ID: 511823
Sample Name: njw.exe
Cookbook: default.jbs
Time: 17:49:38
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

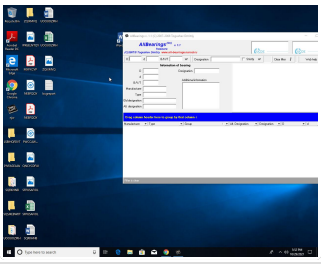
Windows Analysis Report njw.exe

Overview

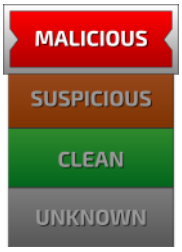
General Information

Sample Name:	njw.exe
Analysis ID:	511823
MD5:	3f91f84924d1db7..
SHA1:	50e790e2b3324c..
SHA256:	a0254e8580186c..
Infos:	

Most interesting Screenshot:



Detection

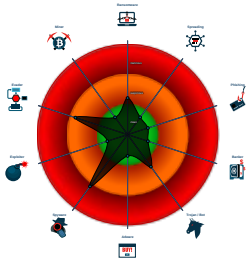


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Tries to steal Mail credentials (via fil…
- Machine Learning detection for samp…
- PE file has nameless sections
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to query locale…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to create guar…
- Found potential string decryption / a…
- Contains functionality to check the p…

Classification



Process Tree

- **System is w10x64**
- njw.exe (PID: 7120 cmdline: 'C:\Users\user\Desktop\njw.exe' MD5: 3F91F84924D1DB7ACE9AD307FCAE35D1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.931984957.000000000401000.00000004.00020000.sdmp	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.njw.exe.400000.0.unpack	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

PE file has nameless sections

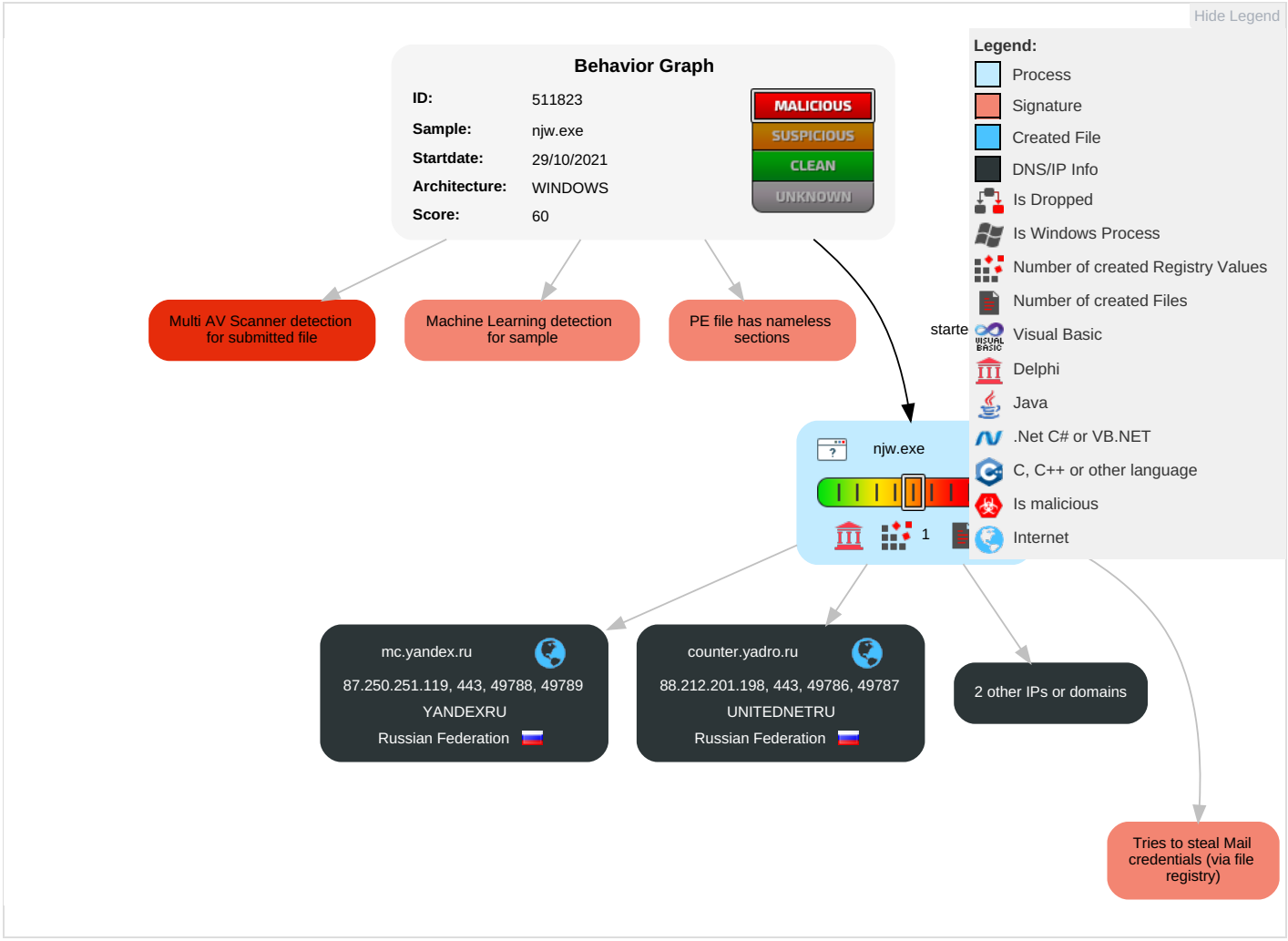
Stealing of Sensitive Information:

Tries to steal Mail credentials (via file registry)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Native API 1	Path Interception	Process Injection 1	Masquerading 1	Input Capture 2	System Time Discovery 1 1	Remote Services	Input Capture 2	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location	Ob De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	Remote System 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 2	DCSync	File and Directory Discovery 1	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	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

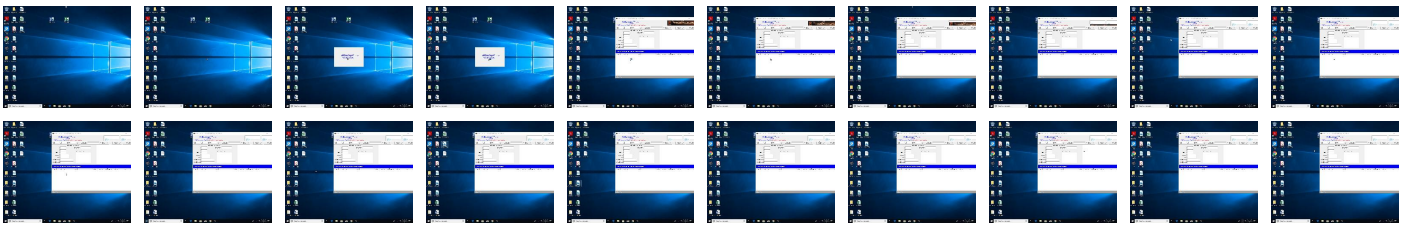
Behavior Graph

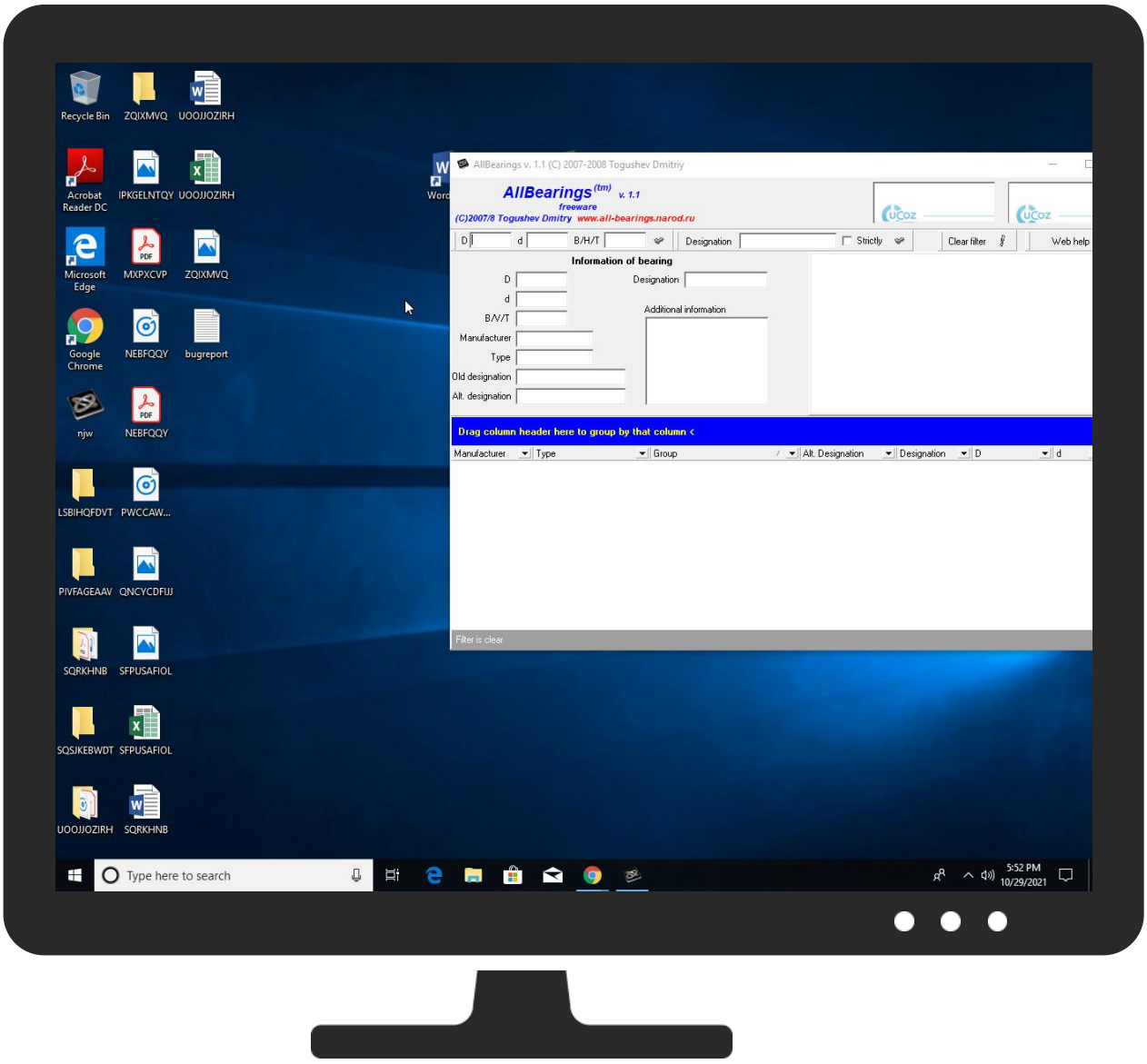


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
njw.exe	11%	Virustotal		Browse
njw.exe	4%	ReversingLabs		
njw.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
counter.yadro.ru	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://counter.yadro.ru/hit;counter1?r	1%	Virustotal		Browse
http://counter.yadro.ru/hit;counter1?r	0%	Avira URL Cloud	safe	
http://www.all-bearings.narod	0%	Avira URL Cloud	safe	
http://counter.yadro.ru/hit;counter1?r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/secondpage.html;0.5443641556055339	0%	Avira URL Cloud	safe	
http://https://counter.yadro.ru/	0%	Avira URL Cloud	safe	
http://https://mc.yandex.	0%	URL Reputation	safe	
http://https://mc.yandex.:	0%	Avira URL Cloud	safe	
http://www.all-bearings.narod.ruc	0%	Avira URL Cloud	safe	
http://www.all-bearings.narod.rud	0%	Avira URL Cloud	safe	
http://https://mc.y	0%	Avira URL Cloud	safe	
http://https://mc.y0	0%	Avira URL Cloud	safe	
http://https://counter.yadro.ru/&	0%	Avira URL Cloud	safe	
http://www.all-bearings.narod.ruopenS	0%	Avira URL Cloud	safe	
http://https://mc.yandex.md/cc	0%	URL Reputation	safe	
http://https://mc.yandex.pK	0%	Avira URL Cloud	safe	
http://https://counter.yadro.ru/hit;counter1?q;r;s1280	0%	Avira URL Cloud	safe	
http://w3.o	0%	Avira URL Cloud	safe	
http://www.remserviss.ruopen	0%	Avira URL Cloud	safe	
http://counter.yadro.ru/hit;counter1?r;s1280	0%	Avira URL Cloud	safe	
http://https://counter.yadro.ru/hit;counter1?q;r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/firstpage.html;0.34476715437082456	0%	Avira URL Cloud	safe	
http://www.remserviss.ru	0%	Avira URL Cloud	safe	
http://https://mc.yandex.md/ccPageView.	0%	Avira URL Cloud	safe	
http://https://iframe-toloka.com/	0%	Avira URL Cloud	safe	
http://www.all-bearings.d	0%	Avira URL Cloud	safe	
http://counter.yadro.ru/	0%	Avira URL Cloud	safe	
http://https://mc.yandex.md/ccba	0%	Avira URL Cloud	safe	
http://www.all-bearings.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mc.yandex.ru	87.250.251.119	true	false		high
counter.yadro.ru	88.212.201.198	true	false	• 3%, Virustotal, Browse	unknown
www-google-analytics.l.google.com	142.250.203.110	true	false		high
www.all-bearings.narod.ru	193.109.247.229	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://counter.yadro.ru/hit;counter1?r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/secondpage.html;0.5443641556055339	false	• Avira URL Cloud: safe	unknown
http://www.all-bearings.narod.ru/.s/img/err/404-arrow.png	false		high
http://https://mc.yandex.ru/watch/14153041?callback=_ymjsp355627947&page-url=http%3A%2F%2Fwww.all-bearings.narod.ru%2Ffirstpage.html&charset=utf-8&browser-info=pv%3A1%3Agdpr%3A14%3Avf%3A9ezyymqkmijljhdjn%3Afp%3A1930%3Afu%3A0%3Aen%3Autf-8%3Ala%3Aen-US%3Av%3A680%3Acn%3A1%3Adp%3A0%3Als%3A732524701665%3Ahid%3A870103866%3Az%3A120%3Ai%3A20210102917512O%3Aet%3A1635522680%3Ac%3A1%3Arn%3A244404675%3Au%3A16355226783226226 28%3Aw%3A148x47%3As%3A1280x1024x32%3Aifr%3A1%3Aj%3A1%3Ans%3A1635522674781%3Ads%3A0%2C0%2C0%2C0%2C0%2C%2C155%2C0%2C2520%2C2521%2C0%2C2520%3Aco%3A0%3Arqnl%3A1%3Ast%3A1635522681%3At%3AHTTP%20404%20Resource%20not%20found&t=gdpr(14)ti(3)&wmode=5	false		high
http://www.all-bearings.narod.ru/.s/img/err/404-logo.png	false		high
http://https://mc.yandex.ru/metrika/advert.gif?t=ti(4)	false		high
http://www.all-bearings.narod.ru/.s/img/err/404.png	false		high
http://www.all-bearings.narod.ru/.s/img/err/404-header-line.gif	false		high
http://mc.yandex.ru/metrika/watch.js	false		high
http://www.all-bearings.narod.ru/.s/img/err/button.png	false		high
http://https://counter.yadro.ru/hit;counter1?q;r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/firstpage.html;0.34476715437082456	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.212.201.198	counter.yadro.ru	Russian Federation		39134	UNITEDNETRU	false
87.250.251.119	mc.yandex.ru	Russian Federation		13238	YANDEXRU	false
193.109.247.229	www.all-bearings.narod.ru	Virgin Islands (BRITISH)		204343	COMPUBYTE-ASRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	511823
Start date:	29.10.2021
Start time:	17:49:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	njw.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
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:	mal60.spyw.winEXE@1/17@4/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 5% (good quality ratio 4.6%) • Quality average: 68.6% • Quality standard deviation: 30.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:51:14	API Interceptor	956x Sleep call for process: njw.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
88.212.201.198	bEzxgfoo6O.rtf	Get hash	malicious	Browse	
	http://3ladies.su	Get hash	malicious	Browse	
	http://https://u.to/r9nvGQ	Get hash	malicious	Browse	
	http://videomytube.cf	Get hash	malicious	Browse	
	http://https://u.to/ofqqGA	Get hash	malicious	Browse	
	http://https://xurl.es/bz56k	Get hash	malicious	Browse	
	http://https://u.to/MM3SFw	Get hash	malicious	Browse	
	http://https://u.to/SBTlFg	Get hash	malicious	Browse	
	http://https://u.to/JGK-Fg	Get hash	malicious	Browse	
	http://https://u.to/YxOpFg&umid=a2728f18-d3ff-4aef-921f-5b5203212a15&auth=0bf7e98084f3624f56880a7a00d412c1d514f34b-95e09708099e407ce94156c8921315b6f95a718e	Get hash	malicious	Browse	
87.250.251.119	http://www.cennikiexcel.ru	Get hash	malicious	Browse	• mc.yandex.ru/metrika/watch.js
	http://An-Crimea.ru	Get hash	malicious	Browse	• mc.yandex.ru/metrika/watch.js
	http://./Documents/2019-01	Get hash	malicious	Browse	• mc.yandex.ru/metrika/watch.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mc.yandex.ru	Open B024L128 .xhtml	Get hash	malicious	Browse	• 87.250.251.119
	uFvG6DlSUpNCq_0a0Y3vNrYQ.exe	Get hash	malicious	Browse	• 93.158.134.119
	MYUNG IN QUotation request.docx	Get hash	malicious	Browse	• 77.88.21.119
	t37BGZn2O1.msi	Get hash	malicious	Browse	• 87.250.250.119
	Elon Musk Site CI6501 .htm	Get hash	malicious	Browse	• 87.250.251.119
	Elon Musk Invite EZ2375 .htm	Get hash	malicious	Browse	• 77.88.21.119
	28jJSvNzXz.exe	Get hash	malicious	Browse	• 87.250.251.119
	Elon Musk Club - 024705 .htm	Get hash	malicious	Browse	• 87.250.251.119
	Bonus Bitcoin - 065540 .htm	Get hash	malicious	Browse	• 87.250.250.119
	DriverPack-17-Online_749652650.1631058953__eqiqpdyx4midqk9.exe	Get hash	malicious	Browse	• 87.250.250.119
	qB6P2WfUjb.exe	Get hash	malicious	Browse	• 87.250.251.119
	IDWCH2.exe	Get hash	malicious	Browse	• 93.158.134.119
	LJSFz5iuuf.exe	Get hash	malicious	Browse	• 93.158.134.119
	OPEN AO-8820 .html	Get hash	malicious	Browse	• 93.158.134.119
	DriverPack-17-Online_174007544.1629221836__itapkqvv6k3n1w8.exe	Get hash	malicious	Browse	• 87.250.250.119
	lo3H2fUlKG.exe	Get hash	malicious	Browse	• 87.250.251.119
	Setup.exe	Get hash	malicious	Browse	• 87.250.251.119
	YWBLA3LR.htm	Get hash	malicious	Browse	• 93.158.134.119
	J7yWiSGmFh.exe	Get hash	malicious	Browse	• 87.250.250.119
	GIJ0V7s4DG.doc	Get hash	malicious	Browse	• 77.88.21.119
counter.yadro.ru	Elon Musk Club - 024705 .htm	Get hash	malicious	Browse	• 88.212.201.204
	Bonus Bitcoin - 065540 .htm	Get hash	malicious	Browse	• 88.212.201.210
	zw0w9vn3tl.exe	Get hash	malicious	Browse	• 88.212.201.216
	bEzxgfoo6O.rtf	Get hash	malicious	Browse	• 88.212.201.198
	bEzxgfoo6O.rtf	Get hash	malicious	Browse	• 88.212.201.204
	iqKNGLP6PS.exe	Get hash	malicious	Browse	• 88.212.201.216
	Ve8rhkTls5.exe	Get hash	malicious	Browse	• 88.212.201.216
	dPWf8DPe5x.exe	Get hash	malicious	Browse	• 88.212.201.216
	http://browsermine.com	Get hash	malicious	Browse	• 88.212.201.210
	http://https://bajashpna.site/Koyo-Oil-Seal-Cross-Reference-Chart/doc	Get hash	malicious	Browse	• 88.212.201.216
	http://https://ofd.beeline.ru/check-order/oxjsoinmq	Get hash	malicious	Browse	• 88.212.201.210
	http://barddistocor.com/mozglue.dll	Get hash	malicious	Browse	• 88.212.201.210
	http://www.2926659.ru/	Get hash	malicious	Browse	• 88.212.201.216
	http://www.emergys.com.mx	Get hash	malicious	Browse	• 88.212.201.216

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://xmastertrk.com:443	Get hash	malicious	Browse	• 88.212.201.204
	http://3ladies.su	Get hash	malicious	Browse	• 88.212.201.198
	http://https://loptrk.com	Get hash	malicious	Browse	• 88.212.201.204
	http://https://u.to/r9nvGQ	Get hash	malicious	Browse	• 88.212.201.198
	http://https://pdfdocdownloadspanel.site/c6092ba97dfbd305a5bbf77d7de3d86e/Assurant-Trade-In-Value-Phone/doc/capxqjxzbj	Get hash	malicious	Browse	• 88.212.201.216
	http://https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.google.com/url?q%253Dhttps%25253A%25252F%25252Ffree-porno.site%25252Fsestra-porno-komiks-incest%2526sa%253DD%2526sntz%253D1%2526usg%253DAFQjCNH31NWj_BM8nKT1IECA8pWwYU8jkQ%26amp;sa%3DD%26amp;ust%3D1600094899031000%26amp;usg%3DAOvVaw07fZ2B1xkNEovI70NLM1Sd&sa=D&ust=1600094899044000&usg=AFQjCNFDsSWFDQJ9fjo9ZnFaOp1n4lUx9g	Get hash	malicious	Browse	• 88.212.201.216

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNITEDNETRU	zCS6X4TGYb	Get hash	malicious	Browse	• 88.212.199.3
	Elon Musk Club - 024705 .htm	Get hash	malicious	Browse	• 88.212.201.204
	Bonus Bitcoin - 065540 .htm	Get hash	malicious	Browse	• 88.212.201.210
	zw0w9vn3tl.exe	Get hash	malicious	Browse	• 88.212.201.216
	bEzxgfoo6O.rtf	Get hash	malicious	Browse	• 88.212.201.198
	bEzxgfoo6O.rtf	Get hash	malicious	Browse	• 88.212.201.204
	iqKNGLP6PS.exe	Get hash	malicious	Browse	• 88.212.201.216
	http://browsermine.com	Get hash	malicious	Browse	• 88.212.201.210
	http://https://bajashpna.site/Koyo-Oil-Seal-Cross-Reference-Chart/doc	Get hash	malicious	Browse	• 88.212.201.216
	http://https://ofd.beeline.ru/check-order/oxjsoinmq	Get hash	malicious	Browse	• 88.212.201.210
	http://coronavir-novosti.ru	Get hash	malicious	Browse	• 88.212.201.210
	http://barddistocor.com/mozglue.dll	Get hash	malicious	Browse	• 88.212.201.210
	http://www.2926659.ru/	Get hash	malicious	Browse	• 88.212.201.216
	http://www.emergys.com.mx	Get hash	malicious	Browse	• 88.212.201.216
	http://https://xmastertrk.com:443	Get hash	malicious	Browse	• 88.212.201.204
	http://3ladies.su	Get hash	malicious	Browse	• 88.212.201.198
	http://https://loptrk.com	Get hash	malicious	Browse	• 88.212.201.204
	http://https://u.to/r9nvGQ	Get hash	malicious	Browse	• 88.212.201.198
	http://https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.google.com/url?q%253Dhttps%25253A%25252F%25252Ffree-porno.site%25252Fsestra-porno-komiks-incest%2526sa%253DD%2526sntz%253D1%2526usg%253DAFQjCNH31NWj_BM8nKT1IECA8pWwYU8jkQ%26amp;sa%3DD%26amp;ust%3D1600094899031000%26amp;usg%3DAOvVaw07fZ2B1xkNEovI70NLM1Sd&sa=D&ust=1600094899044000&usg=AFQjCNFDsSWFDQJ9fjo9ZnFaOp1n4lUx9g	Get hash	malicious	Browse	• 88.212.201.216
	http://videomytube.cf	Get hash	malicious	Browse	• 88.212.201.198
YANDEXRU	SecuriteInfo.com.Trojan.GenericKD.47272401.17364.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Gen.Variant.Nemesis.1785.13723.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO 407274.doc	Get hash	malicious	Browse	• 77.88.21.158
	PO 407274.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	PO.08996.exe	Get hash	malicious	Browse	• 77.88.21.158
	New Purchase Order.exe	Get hash	malicious	Browse	• 77.88.21.158
	Swift USD PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	Open B024L128 .xhtml	Get hash	malicious	Browse	• 87.250.251.119
	Payment PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	uFvG6DlSUpNCq_0a0Y3vNrYQ.exe	Get hash	malicious	Browse	• 87.250.251.119
	MYUNG IN QUotation request.docx	Get hash	malicious	Browse	• 77.88.21.119
	kutipan langsung.14.10.2021.xlxs.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Suspicious.Win32.Save.a.20932.exe	Get hash	malicious	Browse	• 77.88.21.158
	sora.x86	Get hash	malicious	Browse	• 95.108.149.15
	sora.arm	Get hash	malicious	Browse	• 100.43.91.162
	Petikan segera.12.10.2021.xlxs.exe	Get hash	malicious	Browse	• 77.88.21.158
	Purchase_Order_QBO6814_from_Salvona_Technologies.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ-117404.doc	Get hash	malicious	Browse	• 77.88.21.158
	Petikan segera.08.10.2021.xlxs.exe	Get hash	malicious	Browse	• 77.88.21.158

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	t37BGZn2O1.msi	Get hash	malicious	Browse	• 77.88.21.119

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	jWuh2gZyOs.exe	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	SEMqjw.exe	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	New Fax Message from 120283803.html	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	fax45367876545678.exe	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	gemfs.co.uk (1).html	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	instruction.dll	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	stash-9131480.xls	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	oCN3rc0FzJ.exe	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	cjzu7hTifh.exe	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	e0PXyEbkUg.exe	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	#Ud83d#Udd0a VM 9193407174.wav.html	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	PL5m30TFgh.exe	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	Hgny9xwmj6.exe	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	Pv9fSenm0V.exe	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	stash-1675061873.xls	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	stash-1822309505.xls	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	stash-1817904387.xls	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	stash-1675061873.xls	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	Casting Invite.-06503_20211027.xlsb	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198
	0x000500000001abb1-152.exe	Get hash	malicious	Browse	• 87.250.251.119 • 88.212.201.198

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\www.all-bearings.narod[1].xml	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\www.all-bearings.narod[1].xml	
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\404-arrow[1].png	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	PNG image data, 6 x 9, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1169
Entropy (8bit):	6.375857124482774
Encrypted:	false
SSDEEP:	24:zS1he91Wwh82lYSKw7+H1V/uT3cyJ3V2r7hGQ9/9mekJ:MqQvnL8q1durJ3Gh5/Y5J
MD5:	F491D002C601CED0C0BC19994B89CDDC
SHA1:	65B26746EC3BF706DFED1CA6D81BEF6211D15FEF
SHA-256:	BA146CE6FB6E788B50E02B45B72835450B513EC744B2F8DE1DD85589B42F8F05
SHA-512:	0E96575D89DFDE823A577EAF6D4CB4EFAB56C37875B7E5955F7F9FF759B67805FF0013DEDC1C98A73616F7C55CEEBBD5222C0A1EF2F17A936CAE36425E1298 7
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....].....tEXtSoftware.Adobe ImageReadyq.e<...diTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:9A714C550974E111987BC97C16A991C4" xmpMM:DocumentID="xmp.did:8F1EEDA87F2611E18D85EF20DD25A302" xmpMM:InstanceID="xmp.iid:8F1EEDA77F2611E18D85EF20DD25A302" xmp:CreatorTool="Adobe Photoshop CS4 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:92ED5C9A097FE111BC73B13FF08B8A3F" stRef:documentID="xmp.did:9A714C550974E111987BC97C16A991C4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...r....IDATx.b..t.r..G....g.b..f..aW8.....w\.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\404[1].png	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	PNG image data, 155 x 66, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4451
Entropy (8bit):	7.815188084249031
Encrypted:	false
SSDEEP:	48:mqQvnL8QsrJ3GhrwUC5CY1s7P5ShGRQvQCfCWzSWAnXmeQkzkCgDoSbKVRVbGeLG:XQoL0hrYg9yXvjdSWAWeQlFCXukVaa16
MD5:	9684186972F20E829835912A9FF55F3A
SHA1:	ACA5BF4DE51319525F1DB749DC0825CA8E1C06C1
SHA-256:	389267599E2B30CDA3F0091BCDAA856C39E38543038A52955EBA5B048E915742
SHA-512:	31BBD89B9801E09EA5BFA25FDA51FFFDD765C8BEA4BD7FFC80C89750220F99AC35616BDB8146044F69E948424468C3E8691871D6AA2E5C0C27730BFC6AE8AE 0
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....B.....@P.k....tEXtSoftware.Adobe ImageReadyq.e<...diTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:9A714C550974E111987BC97C16A991C4" xmpMM:DocumentID="xmp.did:A2E971A17F2C11E19D72841B70F96071" xmpMM:InstanceID="xmp.iid:A2E971A07F2C11E19D72841B70F96071" xmp:CreatorTool="Adobe Photoshop CS4 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:92ED5C9A097FE111BC73B13FF08B8A3F" stRef:documentID="xmp.did:9A714C550974E111987BC97C16A991C4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>*N.....IDATx..].r.....f...[..*.<@..G.....J...V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ga[1].js	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	46274
Entropy (8bit):	5.48786904450865
Encrypted:	false
SSDEEP:	768:aqNVrKn0VGhn+K7U1r2p/Y60fyy3/g3OMZht1z1prkfw1+9NZ5VA:RHrLVGhnpIwp/Y7cnz1RkLL5m
MD5:	E9372F0EBBCF71F851E3D321EF2A8E5A
SHA1:	2C7D19D1AF7D97085C977D1B69DCB8B84483D87C
SHA-256:	1259EA99BD76596239BFD3102C679EB0A5052578DC526B0452F4D42F8BCDD45F
SHA-512:	C3A1C74AC968FC2FA366D9C25442162773DB9AF1289ADFB165FC71E7750A7E62BD22F424F241730F3C2427AFFF8A540C214B3B97219A360A231D4875E6DDEE6
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ga[1].js	
Preview:	(function(){var E;var g=window,n=document,p=function(a){var b=g._gaUserPrefs;if(b&&b.ioo&&b.ioo()||a&&!0===g["ga-disable-"+a])return!0;try{var c=g.external;if(c &&c._gaUserPrefs&&"oo"==c._gaUserPrefs)return!0}catch(f){}a=[];b=n.cookie.split(";");c=/^\s*AMP_TOKEN=\s*(.*?)\s*$/;for(var d=0;d<b.length;d++){var e=b[d].match (c);e&&a.push(e[1])}for(b=0;b<a.length;b++)if("$OPT_OUT"==decodeURIComponent(a[b]))return!0;return!1};var q=function(a){return encodeURIComponent?enco deURIComponent(a).replace(/\(/g,"%28").replace(/\)/g,"%29"):a},r=/^(www\.)?google(\.com?)?(\.[a-z]{2})?$/,u=/(^\|\.)doubleclick\.net$/i;function Aa(a,b){switch(b){case 0:r eturn""+a;case 1:return 1*a;case 2:return!!a;case 3:return 1E3*a}return a}function Ba(a){return"function"==typeof a}function Ca(a){return void 0!=a&&-1<(a.constructor+"") .indexOf("String")}function F(a,b){return void 0==a||"-"==a&&!b||""==a}function Da(a){if(!a||""==a)return"";for(;a&&-1<" \n\r\t".indexOf(a.charAt(0));)a=a.substring(1);for(;a&&- 1<" \n\r\t".i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ga[2].js	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	46274
Entropy (8bit):	5.48786904450865
Encrypted:	false
SSDEEP:	768:aqNVrKn0VGhn+K7U1r2p/Y60fyy3/g3OMZht1z1prkfw1+9NZ5VA:RHrLVGhnpIwp/Y7cnz1RkLL5m
MD5:	E9372F0EBBCF71F851E3D321EF2A8E5A
SHA1:	2C7D19D1AF7D97085C977D1B69DCB8B84483D87C
SHA-256:	1259EA99BD76596239BFD3102C679EB0A5052578DC526B0452F4D42F8BCDD45F
SHA-512:	C3A1C74AC968FC2FA366D9C25442162773DB9AF1289ADFB165FC71E7750A7E62BD22F424F241730F3C2427AFFF8A540C214B3B97219A360A231D4875E6DDEE6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	(function(){var E;var g=window,n=document,p=function(a){var b=g._gaUserPrefs;if(b&&b.ioo&&b.ioo()||a&&!0===g["ga-disable-"+a])return!0;try{var c=g.external;if(c &&c._gaUserPrefs&&"oo"==c._gaUserPrefs)return!0}catch(f){}a=[];b=n.cookie.split(";");c=/^\s*AMP_TOKEN=\s*(.*?)\s*$/;for(var d=0;d<b.length;d++){var e=b[d].match (c);e&&a.push(e[1])}for(b=0;b<a.length;b++)if("$OPT_OUT"==decodeURIComponent(a[b]))return!0;return!1};var q=function(a){return encodeURIComponent?enco deURIComponent(a).replace(/\(/g,"%28").replace(/\)/g,"%29"):a},r=/^(www\.)?google(\.com?)?(\.[a-z]{2})?$/,u=/(^\|\.)doubleclick\.net$/i;function Aa(a,b){switch(b){case 0:r eturn""+a;case 1:return 1*a;case 2:return!!a;case 3:return 1E3*a}return a}function Ba(a){return"function"==typeof a}function Ca(a){return void 0!=a&&-1<(a.constructor+"") .indexOf("String")}function F(a,b){return void 0==a||"-"==a&&!b||""==a}function Da(a){if(!a||""==a)return"";for(;a&&-1<" \n\r\t".indexOf(a.charAt(0));)a=a.substring(1);for(;a&&- 1<" \n\r\t".i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\advert[1].gif	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\404-arrow[1].png	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	PNG image data, 6 x 9, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1169
Entropy (8bit):	6.375857124482774
Encrypted:	false
SSDEEP:	24:zS1he91Wwh82lYSKw7+H1V/uT3cyJ3V2r7hGQ9/9mekJ:MqQvnL8q1durJ3Gh5/Y5J
MD5:	F491D002C601CED0C0BC19994B89CDDC
SHA1:	65B26746EC3BF706DFED1CA6D81BEF6211D15FEF
SHA-256:	BA146CE6FB6E788B50E02B45B72835450B513EC744B2F8DE1DD85589B42F8F05
SHA-512:	0E96575D89DFDE823A577EAF6D4CB4EFAB56C37875B7E5955F7F9FF759B67805FF0013DEDC1C98A73616F7C55CEEBBD5222C0A1EF2F17A936CAE36425E1298 7
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\404-arrow[1].png	
Preview:	.PNG.....IHDR.....].....tEXtSoftware.Adobe ImageReadyq.e<...diTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:9A714C550974E111987BC97C16A991C4" xmpMM:DocumentID="xmp.did:8F1EEDA87F2611E18D85EF20DD25A302" xmpMM:InstanceID="xmp.iid:8F1EEDA77F2611E18D85EF20DD25A302" xmp:CreatorTool="Adobe Photoshop CS4 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:92ED5C9A097FE111BC73B13FF08B8A3F" stRef:documentID="xmp.did:9A714C550974E111987BC97C16A991C4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...r....IDATx.b..t.r..G....g.b..f..aW8.....w\.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\404-header-line[1].gif	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	1161
Entropy (8bit):	6.66123176440527
Encrypted:	false
SSDEEP:	24:4al1he91Wwh82lYSKw7+AVRT3cyJ3V2r7hGY8D:RqQvnL8rjrJ3GhL8D
MD5:	5B4E842D2F840996ECB19B6AE635E873
SHA1:	EE82D94636E4393AAF6E97931793975950A82CA6
SHA-256:	AC9C14376FAC0CD59069AEEF8D7667E6A85DAD3BA0379DC2A6026A20DB18DF1A
SHA-512:	8E0061925AF72421F8F003F22FC51D284B7F97FBCA3D4A5525CB3411485946CC0738066AE0A88B9D2BA8C4252DB20A69F64E9748BE03FF97AAB7EE2347C4A88D
Malicious:	false
Preview:	GIF89a.....!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:9A714C550974E111987BC97C16A991C4" xmpMM:DocumentID="xmp.did:4C014FE07F2611E19F57DEAD3C227423" xmpMM:InstanceID="xmp.iid:4C014FDF7F2611E19F57DEAD3C227423" xmp:CreatorTool="Adobe Photoshop CS4 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:92ED5C9A097FE111BC73B13FF08B8A3F" stRef:documentID="xmp.did:9A714C550974E111987BC97C16A991C4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\404-header-line[2].gif	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	1161
Entropy (8bit):	6.66123176440527
Encrypted:	false
SSDEEP:	24:4al1he91Wwh82lYSKw7+AVRT3cyJ3V2r7hGY8D:RqQvnL8rjrJ3GhL8D
MD5:	5B4E842D2F840996ECB19B6AE635E873
SHA1:	EE82D94636E4393AAF6E97931793975950A82CA6
SHA-256:	AC9C14376FAC0CD59069AEEF8D7667E6A85DAD3BA0379DC2A6026A20DB18DF1A
SHA-512:	8E0061925AF72421F8F003F22FC51D284B7F97FBCA3D4A5525CB3411485946CC0738066AE0A88B9D2BA8C4252DB20A69F64E9748BE03FF97AAB7EE2347C4A88D
Malicious:	false
Preview:	GIF89a.....!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:9A714C550974E111987BC97C16A991C4" xmpMM:DocumentID="xmp.did:4C014FE07F2611E19F57DEAD3C227423" xmpMM:InstanceID="xmp.iid:4C014FDF7F2611E19F57DEAD3C227423" xmp:CreatorTool="Adobe Photoshop CS4 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:92ED5C9A097FE111BC73B13FF08B8A3F" stRef:documentID="xmp.did:9A714C550974E111987BC97C16A991C4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\404-logo[1].png	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	PNG image data, 43 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2152
Entropy (8bit):	7.4508196985650255
Encrypted:	false
SSDEEP:	48:4wqQvnL8HZ3rJ3Gh0NNeqNwzja90uVfAZO6UE:4BQot0h0rSja90uFAhP
MD5:	62A569EF932D3AA5B44BBC515DF09653
SHA1:	E910390D6A312FA9F4B222AEEA3226C1F7EA7FA0
SHA-256:	0945354CAD56584EB978AFC9800BC9BD8D24DF25FBFE063573A0511AF5138E8B
SHA-512:	5FD5A2236ACF1E1BB72A12C74FB00C6FB8A3B8D084F513867EA8FAAC1E76027A7CE342A0054B0F873440B7B083551A218324012E021EE343F2FC0CDE03DF94F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\404-logo[1].png	
Preview:	.PNG.....IHDR...+.....'vm....tEXtSoftware.Adobe ImageReadyq.e<...diTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:9A714C550974E111987BC97C16A991C4" xmpMM:DocumentID="xmp.did:6A7BBACF7F2611E19F01EE589B08C430" xmpMM:InstanceID="xmp.iid:6A7BBACE7F2611E19F01EE589B08C430" xmp:CreatorTool="Adobe Photoshop CS4 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:92ED5C9A097FE111BC73B13FF08B8A3F" stRef:documentID="xmp.did:9A714C550974E111987BC97C16A991C4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.O.....IDATx..{ITE....EZjC....j..h.....b..!b*/.c...W

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\404-logo[2].png	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	PNG image data, 43 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2152
Entropy (8bit):	7.4508196985650255
Encrypted:	false
SSDEEP:	48:4wqQvnL8HZ3rJ3Gh0NNeqNwzja90uVfAZO6UE:4BQot0h0rSja90uFAhP
MD5:	62A569EF932D3AA5B44BBC515DF09653
SHA1:	E910390D6A312FA9F4B222AEEA3226C1F7EA7FA0
SHA-256:	0945354CAD56584EB978AFC9800BC9BD8D24DF25FBFE063573A0511AF5138E8B
SHA-512:	5FD5A2236ACF1E1BB72A12C74FB00C6FB8A3B8D084F513867EA8FAAC1E76027A7CE342A0054B0F873440B7B083551A218324012E021EE343F2FC0CDE03DF94F
Malicious:	false
Preview:	.PNG.....IHDR...+.....'vm....tEXtSoftware.Adobe ImageReadyq.e<...diTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:9A714C550974E111987BC97C16A991C4" xmpMM:DocumentID="xmp.did:6A7BBACF7F2611E19F01EE589B08C430" xmpMM:InstanceID="xmp.iid:6A7BBACE7F2611E19F01EE589B08C430" xmp:CreatorTool="Adobe Photoshop CS4 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:92ED5C9A097FE111BC73B13FF08B8A3F" stRef:documentID="xmp.did:9A714C550974E111987BC97C16A991C4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.O.....IDATx..{ITE....EZjC....j..h.....b..!b*/.c...W

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\404[1].png	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	PNG image data, 155 x 66, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4451
Entropy (8bit):	7.815188084249031
Encrypted:	false
SSDEEP:	48:mqQvnL8QsrJ3GhrwUC5CY1s7P5ShGRQvQCfCWzSWAnXmeQkzkCgDoSbKVRVbGeLG:XQoL0hrYg9yXvjdSWAWeQlFCXukVaa16
MD5:	9684186972F20E829835912A9FF55F3A
SHA1:	ACA5BF4DE51319525F1DB749DC0825CA8E1C06C1
SHA-256:	389267599E2B30CDA3F0091BCDAA856C39E38543038A52955EBA5B048E915742
SHA-512:	31BBD89B9801E09EA5BFA25FDA51FFFDD765C8BEA4BD7FFC80C89750220F99AC35616BDB8146044F69E948424468C3E8691871D6AA2E5C0C27730BFC6AE8AE0
Malicious:	false
Preview:	.PNG.....IHDR.....B.....@P.k....tEXtSoftware.Adobe ImageReadyq.e<...diTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:9A714C550974E111987BC97C16A991C4" xmpMM:DocumentID="xmp.did:A2E971A17F2C11E19D72841B70F96071" xmpMM:InstanceID="xmp.iid:A2E971A07F2C11E19D72841B70F96071" xmp:CreatorTool="Adobe Photoshop CS4 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:92ED5C9A097FE111BC73B13FF08B8A3F" stRef:documentID="xmp.did:9A714C550974E111987BC97C16A991C4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>*N.....IDATx..].r.....f...[..*.<@..G.....J...V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\button[2].png	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	PNG image data, 1 x 20, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1036
Entropy (8bit):	6.003417494129505
Encrypted:	false
SSDEEP:	24:PQJ1he91Wwh82lYSKw7+AzVvT3cyJ3V2r7hGAOK7:qqQvnL83RrJ3GhOQ
MD5:	20ECCCF80B7CCE904C2EE06F65007306
SHA1:	951474262705F3D4C58E3E937DAF03A9D0BFC7FA
SHA-256:	DB06224375A1362DE84DA041DB7BD476C60267D1E7D24A8569F967CE0C07EF05
SHA-512:	692DDE2E59BBB0DE8411E46787DDCDE95156F0E15994219194105CFE3CBDA9A666FAC512DD059297BD5560B6117D0D15DFCC657A431187161F887A525821AE9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\button[2].png	
Preview:	.PNG.....IHDR.....l.....tEXtSoftware.Adobe ImageReadyq.e<...diTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:9A714C550974E111987BC97C16A991C4" xmpMM:DocumentID="xmp.did:3331FF467FCD11E18838E5F708B7572B" xmpMM:InstanceID="xmp.iid:3331FF457FCD11E18838E5F708B7572B" xmp:CreatorTool="Adobe Photoshop CS4 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:92ED5C9A097FE111BC73B13FF08B8A3F" stRef:documentID="xmp.did:9A714C550974E111987BC97C16A991C4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>..L....>IDATx.l....!.....KS...P"..70.{.*.9..L".....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\watch[1].js	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	dropped
Size (bytes):	132911
Entropy (8bit):	5.575537014376501
Encrypted:	false
SSDEEP:	1536:gSYWWEU3rdOKg7spQAFdmxdoxUxZ2mCeEo/sS8r7kuuDvWvzODHIbkZUQ1mOTMnF:g5WWboAnmxYztM4cMpNO5K
MD5:	ECA5C7083EF9B406373D0C3399A909DF
SHA1:	186F214942A03FAEBAEE065A9AD6C44509FD595C
SHA-256:	D583F0408C31E539635F93EA833DA6D7FFF4707B3B17679A16B16FD24D639864
SHA-512:	4B63B57801F39D330626588816E5550619EDE8611E1CB22013EA8DB79BA6F643383BB69D57D0168BD2946F7B88DA048E60719B2E7648D201643DF5094DDB5059
Malicious:	false
Preview:	.(function(){try{(function(Jc){function Hi(a){return a.replace(Ii,function(b,c,d,e){return""+c+e})}function Kc(a,b){if(!b)return!1;var c=M(a);return(new RegExp(b)).test(" "+c.pathname+c.hash+c.search)}function Ji(a,b){return Da(a,b,function(c){var d=n(c,"settings.dr");return{rc:Ki(a,d),isEnabled:n(c,"settings.auto_goals")}})}function Li(a,b){function c(){var m=l+"0",p=l+"1";h[m]?h[p]?(l=l.slice(0,-1),--k):(g[p]=e(8),h[p]=1):(g[m]=e(8),h[m]=1)}function d(){var m=l+"1";h[l+"0"]?h[m]?(l=l.slice(0,-1),--k):(l+="1",.h[l]=1):(l+="0",h[l]=1)}function e(m){void 0===m&&(m=1);var p=f.slice(k,k+m);k+=m;return p}for(var f=Ye(a,b,""),g={},h={},k=1,l="";k<f.length-1;)("0"===e()?d:c)();return g}function Mi(a,b,c,d,e){c=Dd(a,a.document.body,c);d=Dd(a,a.document.body,d);N(e.target,[c,d])&&Ed(a,b)}function Ze(a,b,c,d){(c=Ni(a,d,c))&&Ed(a,b,c)}function $e(a,b){var c=af(a,b);return Oi(a,c)}function af(a,b){var c=Dd(a,a.document.body,b);return c?Pi(a,c):""}function Ed(a,b,c){(b=Ea(a,b))&&b.params(cc(["__y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\watch[2].js	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	dropped
Size (bytes):	132911
Entropy (8bit):	5.575537014376501
Encrypted:	false
SSDEEP:	1536:gSYWWEU3rdOKg7spQAFdmxdoxUxZ2mCeEo/sS8r7kuuDvWvzODHIbkZUQ1mOTMnF:g5WWboAnmxYztM4cMpNO5K
MD5:	ECA5C7083EF9B406373D0C3399A909DF
SHA1:	186F214942A03FAEBAEE065A9AD6C44509FD595C
SHA-256:	D583F0408C31E539635F93EA833DA6D7FFF4707B3B17679A16B16FD24D639864
SHA-512:	4B63B57801F39D330626588816E5550619EDE8611E1CB22013EA8DB79BA6F643383BB69D57D0168BD2946F7B88DA048E60719B2E7648D201643DF5094DDB5059
Malicious:	false
Preview:	.(function(){try{(function(Jc){function Hi(a){return a.replace(Ii,function(b,c,d,e){return""+c+e})}function Kc(a,b){if(!b)return!1;var c=M(a);return(new RegExp(b)).test(" "+c.pathname+c.hash+c.search)}function Ji(a,b){return Da(a,b,function(c){var d=n(c,"settings.dr");return{rc:Ki(a,d),isEnabled:n(c,"settings.auto_goals")}})}function Li(a,b){function c(){var m=l+"0",p=l+"1";h[m]?h[p]?(l=l.slice(0,-1),--k):(g[p]=e(8),h[p]=1):(g[m]=e(8),h[m]=1)}function d(){var m=l+"1";h[l+"0"]?h[m]?(l=l.slice(0,-1),--k):(l+="1",.h[l]=1):(l+="0",h[l]=1)}function e(m){void 0===m&&(m=1);var p=f.slice(k,k+m);k+=m;return p}for(var f=Ye(a,b,""),g={},h={},k=1,l="";k<f.length-1;)("0"===e()?d:c)();return g}function Mi(a,b,c,d,e){c=Dd(a,a.document.body,c);d=Dd(a,a.document.body,d);N(e.target,[c,d])&&Ed(a,b)}function Ze(a,b,c,d){(c=Ni(a,d,c))&&Ed(a,b,c)}function $e(a,b){var c=af(a,b);return Oi(a,c)}function af(a,b){var c=Dd(a,a.document.body,b);return c?Pi(a,c):""}function Ed(a,b,c){(b=Ea(a,b))&&b.params(cc(["__y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\advert[1].gif	
Process:	C:\Users\user\Desktop\njw.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F56701
Malicious:	false
Preview:	GIF89a.....l.....,.....D..;

C:\Users\user\Desktop\bugreport.txt	
Process:	C:\Users\user\Desktop\njw.exe

C:\Users\user\Desktop\bugreport.txt	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	18164
Entropy (8bit):	4.9882772544962215
Encrypted:	false
SSDEEP:	384:f9rMWwQN3CxK+8T6zPtw1c5bgrwuBG5bgqO4pPQCAK3JEaKmI6xYVGnbYWEdOaCN:JwQN3Cg+8T6zPu1c5bgrwuBG5bgqO4pZ
MD5:	C1757ECB255B635D6BA341EF72AF480D
SHA1:	87D16FC44477F4F06640B02D27674BBD228614CA
SHA-256:	7A96B64D191CF08F88C8C21DAE04C0A925E7893D8919BD94CCD14AA7527963AC
SHA-512:	2005270175A3C936A9AB9D17265AAF63C629287ED634E581E0F9DA56200174401B31DC3D03EBBF0A7F44CA20C322A2B62AA4E3257863D274A32F5434EFA64E0D
Malicious:	false
Preview:	date/time : 2021-10-29, 17:51:08, 31ms..computer name : 114127..user name : user <admin>..operating system : Windows NT New build 9200..system language : English..system up time : 1 hour 43 minutes..program up time : 5 seconds..processors : 2x Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..physical memory : 2743/8191 MB (free/total)..free disk space : (C:) 79.99 GB..display mode : 1280x1024, 32 bit..process id : $1bd0..allocated memory : 39.16 MB..executable : njw.exe..exec. date/time : 2021-10-29 17:50..madExcept version : 3.0b..callstack crc : $1a0983a1, $6b1df792, $6b1df792..exception number : 1..exception class : EDatabaseError..exception message : Cannot open file bearingdb.tdb.....main thread ($1bd4):..004ca780 +074 njw.exe DB DatabaseError ..004ca7e9 +031 njw.exe DB DatabaseErrorFmt..004f0e72 +06e njw.exe TinyDB 6042 +9 TTinyDBFileIO.Open..004f79ba +07e njw.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Entropy (8bit):	7.935591299650064
TrID:	• Win32 Executable (generic) a (10002005/4) 99.81% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	njw.exe
File size:	1694802
MD5:	3f91f84924d1db7ace9ad307fcae35d1
SHA1:	50e790e2b3324c1b3805916c5a3c323ed8a7305f
SHA256:	a0254e8580186ca146fcc6082a6110888ac0cc3c7f733e760ad7a655bd2a0503
SHA512:	fda6aeccba43b923567ca1e662f31526a5458dc74df356f077116b0a6300f2e7ac0ce3af8ae81a18064048279c1a231d94c2f5a6c66e5dd210363e6bcf734218
SSDEEP:	49152:iOv9gx8KFwoDGqqO3XG00ASL6/PaSm9eMqDsnF0v:i8GxP+qquXGtLsXaeMqDUF2
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	6860d1e434cc7c80

Static PE Info

General

Entrypoint:	0x68861c
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, DEBUG_STRIPPED, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]

General

TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	09240fdb1ba0c5773dfe515581b453b6

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x1000	0x1f8a34	0xf6200	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x1fa000	0xba1c	0x5a00	False	0.982118055556	data	7.98180899146	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x206000	0x2489	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x209000	0x32e2	0x1400	False	0.93984375	data	7.89313292742	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x20d000	0x51	0x200	False	0.193359375	data	3.96131250875	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x20e000	0xf0	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x20f000	0x18	0x200	False	0.048828125	data	0.19667565744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x210000	0x26d28	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x237000	0x5061c	0x50800	False	0.749223602484	data	7.33188771893	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x288000	0xab9c	0x7200	False	0.985094572368	data	7.97472353809	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
	0x293000	0xe2c	0x1000	False	0.3603515625	data	4.53691628835	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x294000	0x615a	0x1400	False	1.0021484375	data	7.96644681101	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/29/21-17:51:14.924932	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
10/29/21-17:51:15.851555	TCP	2925	INFO web bug 0x0 gif attempt	80	49782	193.109.247.229	192.168.2.4
10/29/21-17:51:16.067758	TCP	2925	INFO web bug 0x0 gif attempt	80	49782	193.109.247.229	192.168.2.4
10/29/21-17:51:16.429861	TCP	2925	INFO web bug 0x0 gif attempt	80	49784	142.250.203.110	192.168.2.4
10/29/21-17:51:16.523030	TCP	2925	INFO web bug 0x0 gif attempt	80	49784	142.250.203.110	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 29, 2021 17:51:13.816387892 CEST	192.168.2.4	8.8.8.8	0xc22c	Standard query (0)	www.all-bearings.narod.ru	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:14.822130919 CEST	192.168.2.4	8.8.8.8	0xc22c	Standard query (0)	www.all-bearings.narod.ru	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:15.343087912 CEST	192.168.2.4	8.8.8.8	0x6b57	Standard query (0)	counter.yadro.ru	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:15.362785101 CEST	192.168.2.4	8.8.8.8	0xe7f9	Standard query (0)	mc.yandex.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 17:51:14.890239954 CEST	8.8.8.8	192.168.2.4	0xc22c	No error (0)	www.all-bearings.narod.ru		193.109.247.229	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:14.924814939 CEST	8.8.8.8	192.168.2.4	0xc22c	No error (0)	www.all-bearings.narod.ru		193.109.247.229	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:15.347728014 CEST	8.8.8.8	192.168.2.4	0x2fe6	No error (0)	www-google-analytics.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:15.362226963 CEST	8.8.8.8	192.168.2.4	0x6b57	No error (0)	counter.yadro.ru		88.212.201.198	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:15.362226963 CEST	8.8.8.8	192.168.2.4	0x6b57	No error (0)	counter.yadro.ru		88.212.201.210	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:15.362226963 CEST	8.8.8.8	192.168.2.4	0x6b57	No error (0)	counter.yadro.ru		88.212.201.216	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:15.362226963 CEST	8.8.8.8	192.168.2.4	0x6b57	No error (0)	counter.yadro.ru		88.212.201.204	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:15.381855965 CEST	8.8.8.8	192.168.2.4	0xe7f9	No error (0)	mc.yandex.ru		87.250.251.119	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:15.381855965 CEST	8.8.8.8	192.168.2.4	0xe7f9	No error (0)	mc.yandex.ru		87.250.250.119	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 17:51:15.381855965 CEST	8.8.8.8	192.168.2.4	0xe7f9	No error (0)	mc.yandex.ru		77.88.21.119	A (IP address)	IN (0x0001)
Oct 29, 2021 17:51:15.381855965 CEST	8.8.8.8	192.168.2.4	0xe7f9	No error (0)	mc.yandex.ru		93.158.134.119	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.all-bearings.narod.ru
  - mc.yandex.ru
  - counter.yadro.ru

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49790	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49792	88.212.201.198	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49800	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49801	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49782	193.109.247.229	80	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:14.979448080 CEST	1390	OUT	GET /secondpage.html HTTP/1.1 Accept: */* Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.045492887 CEST	1391	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 29 Oct 2021 15:51:16 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=15 ETag: W/"611e66ad-1ad5" Content-Encoding: gzip Data Raw: 61 30 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 9d 59 fb 6f db 38 12 fe 3d 7f 05 ab e0 60 bb 89 25 bf 92 a6 7e 15 6d da c5 2e 90 6e 7b bb e9 1d 8a a2 28 68 89 b6 d8 48 a2 4a 52 71 bc d9 fc ef 37 43 ea 65 5b 4e ba 67 a1 91 c4 c7 70 e6 9b 99 8f 43 75 fa ec ed 87 cb eb cf 1f df 91 50 c7 d1 fc 68 5a dc 18 0d e6 47 04 7e d3 98 69 0a bd 3a ed b2 1f 19 bf 9d 39 be 48 34 4b 74 57 6f 52 e6 90 fc 6d e6 68 76 a7 3d 9c 3e 21 7e 48 a5 62 7a 96 e9 65 f7 c2 21 5e 2e 49 73 1d b1 f9 af d7 d7 1f c9 a8 37 22 7f 30 25 32 e9 33 92 08 4d 96 22 4b 82 a9 67 87 1c 4d 95 de 44 8c e0 0a b9 60 5f 29 67 7e b4 10 c1 86 dc c7 54 ae 78 32 26 bd 09 49 69 10 f0 64 65 9e 17 d4 bf 59 49 94 33 26 c7 cb e5 72 02 42 13 3d 26 fd 41 7a e7 0d e0 0f 69 fd 87 c9 80 26 b4 05 2a 8a 48 48 18 77 7e 81 d7 e4 c1 8a a6 e4 be e8 18 0e e8 c0 07 19 b8 7a 37 60 be 90 54 73 01 ab 82 7c 26 23 9e b0 72 d2 38 14 b7 4c 92 fb bd a1 89 30 a3 74 70 4a 78 92 66 fa 94 28 16 31 1f ee 38 94 4a 06 eb 55 3a 92 a7 95 74 fd 88 51 58 c9 dc c6 64 21 74 68 5a ad 0f c8 fd 9a 07 3a 1c 93 17 c3 b3 f4 6e 42 0a 9c 68 a6 05 0c f3 9e 77 f3 1f 7a 97 49 fb fc dc 3b 3a b6 ef e4 3e 64 7c 15 82 36 67 66 7a 1d cf 4c 46 6d cf 55 1e 8f 57 1e 93 d2 03 ff 15 52 10 0a 77 c5 97 1d 22 59 ca a8 ee de 91 1e f8 17 24 3c 1c 1d 47 62 25 c0 c6 48 50 10 1b b1 a5 ae b4 aa 7b 6f 70 9e e2 ac 1e 36 e6 36 8c 86 a8 43 a1 d1 e0 45 4d 1e a0 16 70 95 46 74 03 10 44 c2 bf a9 c7 01 79 89 f3 0e 0b 21 e8 2b 50 68 3d 26 21 0f 02 96 40 4b a6 d1 88 dc 5f d6 e3 1c bc 8c 8e e9 be 84 df 2e 1a 18 5d 8d 90 a0 7a 6e 9a ac 3a 20 aa 6b e1 20 3e c8 01 70 ed 0d bd a5 b8 66 5d 1f 9c af 59 09 8d 44 0d 2b 6c ea 78 3c 62 ea 99 19 d5 37 de ca e3 a8 8f b1 7e 7e 20 8c 5e f8 3d 36 f8 49 53 a8 94 62 bd 6b 0b 7a 90 f4 ad 6f ab 70 aa ff 20 9c aa 8e 98 f2 a4 d6 71 8c ef e4 be 34 e0 ac 67 f4 3f 33 66 20 32 66 bc 59 63 3b 64 72 6f f6 cf 71 65 eb 1f 1a f1 15 00 55 a1 0a 7a 0b 69 e8 a3 cc a9 0b c4 62 d4 8c c5 0b b6 18 05 83 72 a2 2f 02 56 11 4b df 2a 36 b0 8a 95 cb db b4 28 a2 e9 fc fc 27 92 64 07 40 5c 2f a5 2b 06 8c 67 08 af 54 75 84 aa f6 0e a9 8a d7 de 54 9a 13 8e 96 34 51 4b 21 63 50 20 4d 99 f4 a9 62 4d 76 1a 70 4d 9c 35 a3 3b 7a b9 45 1a 26 fa c8 85 f5 75 7d 72 38 dc 62 e0 1a c7 22 e0 4d 06 0c 86 78 95 62 4a b6 6a 62 82 fe b0 8c fc dd f1 59 54 4d 19 96 91 0f 19 8a 6a d7 37 82 88 2b dd 35 3b 48 49 c1 c7 0a 08 d3 0f c9 3d e6 9f 79 5c 0b 19 94 84 39 7c d1 db 16 42 b6 5c 3d 30 bd c8 11 dd ed a6 1d e6 58 80 4c 06 16 43 12 12 25 22 1e 90 63 7f 89 57 d1 d5 95 34 e0 99 1a 5b f1 40 44 9a fb 34 2a 82 39 06 3e 8a 8c a3 ad 8a 6a 11 3f 1a 20 a5 2e 03 94 56 a0 7d 36 a2 41 b9 71 a9 90 06 48 75 3d a3 13 fe b3 3b 63 cd 52 23 15 37 1e 6b 52 93 0d 43 bc c8 33 1e a7 90 62 34 d1 cd e6 6c d1 0a bb c0 6b 2f 25 16 99 d6 22 b1 59 51 6c 17 a0 7a 26 15 ea 9e 0a 6e d2 79 17 d7 03 40 d5 a8 fc 96 2b be 30 d8 3d 1f 2f b9 04 ff fb 21 8f 82 13 ac 47 48 1d ce c2 bc 5e dd 9c 9f 21 b3 a5 10 ba d8 33 0d 99 d9 86 1a 9d f5 cf 2a d2 ce f1 d1 22 dd 42 32 58 e0 85 1e ce c5 81 d3 9a b3 71 30 72 5f fe 6b 67 60 38 22 f7 5b f9 d9 cf 09 aa c6 fd fd 03 7c 77 76 8e d7 8e 40 cc a8 c6 fd b8 39 89 76 a6 46 1c 66 d7 97 3e 90 fe 17 14 af 9d f9 30 19 08 6c 77 cc 7e b5 d5 b0 34 4e 3d 58 72 d5 ab b3 83 4e 9d 7a c6 30 a8 33 3d 5b e8 4e b1 90 c3 b2 d3 97 3c d5 f5 ba f3 3b bd a5 b6 d5 c1 2a f6 16 aa af 6f 2b fa 83 cc ec Data Ascii: a01Yo8=`%~m.n{(hHJRq7Ce[NgpCuPhZG~i:9H4KtWoRmhv=>!~Hbze!^.Is7"0%23M"KgMD`_)g~Tx2&lideYI3 &rB=&Azi&*HHw~z7`Ts|&#r8L0tpJxf(18JU:tQXd!thZ:nBhwzI;:>d|6gfzLFmUWRw"Y$<Gb%HP{op66CEMpFtDy !+Ph=&!@K_.]zn: k >pf]YD+lx<b7~~ ^=6ISbkzop q4g?3f 2fYc;droqeUzibr/VK*6('d@V+gTuT4QK!cP MbMvpM5;zE& u}r8b"MxbJjbYTMj7+5;HI=y\9|B\=0XLC%"cW4[@D4*9>j? .V}6AqHu=;cR#7kRC3b4Ik/%"YQlz&ny@+0=/!GH^!3*"B2Xq0r _kg`8"[|wv@9vFf>0lw~4N=XrNz03=[N<;*o+
Oct 29, 2021 17:51:15.785819054 CEST	1457	OUT	GET /.s/img/err/404-header-line.gif HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive
Oct 29, 2021 17:51:15.851555109 CEST	1458	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 29 Oct 2021 15:51:17 GMT Content-Type: image/gif Content-Length: 1161 Last-Modified: Mon, 31 Jul 2017 10:32:10 GMT Connection: keep-alive Keep-Alive: timeout=15 ETag: "597f072a-489" Expires: Thu, 18 Nov 2021 15:51:17 GMT Cache-Control: max-age=1728000 Accept-Ranges: bytes
Oct 29, 2021 17:51:15.859746933 CEST	1461	OUT	GET /.s/img/err/404-logo.png HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive
Oct 29, 2021 17:51:15.925540924 CEST	1462	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 29 Oct 2021 15:51:17 GMT Content-Type: image/png Content-Length: 2152 Last-Modified: Mon, 31 Jul 2017 10:32:10 GMT Connection: keep-alive Keep-Alive: timeout=15 ETag: "597f072a-868" Expires: Thu, 18 Nov 2021 15:51:17 GMT Cache-Control: max-age=1728000 Accept-Ranges: bytes

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.932754993 CEST	1466	OUT	GET /.s/img/err/404.png HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive
Oct 29, 2021 17:51:15.998469114 CEST	1469	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 29 Oct 2021 15:51:17 GMT Content-Type: image/png Content-Length: 4451 Last-Modified: Mon, 31 Jul 2017 10:32:10 GMT Connection: keep-alive Keep-Alive: timeout=15 ETag: "597f072a-1163" Expires: Thu, 18 Nov 2021 15:51:17 GMT Cache-Control: max-age=1728000 Accept-Ranges: bytes
Oct 29, 2021 17:51:16.002221107 CEST	1477	OUT	GET /.s/img/err/404-header-line.gif HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive
Oct 29, 2021 17:51:16.067758083 CEST	1493	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 29 Oct 2021 15:51:17 GMT Content-Type: image/gif Content-Length: 1161 Last-Modified: Mon, 31 Jul 2017 10:32:10 GMT Connection: keep-alive Keep-Alive: timeout=15 ETag: "597f072a-489" Expires: Thu, 18 Nov 2021 15:51:17 GMT Cache-Control: max-age=1728000 Accept-Ranges: bytes
Oct 29, 2021 17:51:16.070837975 CEST	1498	OUT	GET /.s/img/err/404-arrow.png HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive
Oct 29, 2021 17:51:16.136607885 CEST	1664	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 29 Oct 2021 15:51:17 GMT Content-Type: image/png Content-Length: 1169 Last-Modified: Mon, 31 Jul 2017 10:32:10 GMT Connection: keep-alive Keep-Alive: timeout=15 ETag: "597f072a-491" Expires: Thu, 18 Nov 2021 15:51:17 GMT Cache-Control: max-age=1728000 Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49783	193.109.247.229	80	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.015364885 CEST	1390	OUT	GET /firstpage.html HTTP/1.1 Accept: */* Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.082951069 CEST	1395	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 29 Oct 2021 15:51:16 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=15 ETag: W/"611e66ad-1ad5" Content-Encoding: gzip Data Raw: 61 30 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 9d 59 fb 6f db 38 12 fe 3d 7f 05 ab e0 60 bb 89 25 bf 92 a6 7e 15 6d da c5 2e 90 6e 7b bb e9 1d 8a a2 28 68 89 b6 d8 48 a2 4a 52 71 bc d9 fc ef 37 43 ea 65 5b 4e ba 67 a1 91 c4 c7 70 e6 9b 99 8f 43 75 fa ec ed 87 cb eb cf 1f df 91 50 c7 d1 fc 68 5a dc 18 0d e6 47 04 7e d3 98 69 0a bd 3a ed b2 1f 19 bf 9d 39 be 48 34 4b 74 57 6f 52 e6 90 fc 6d e6 68 76 a7 3d 9c 3e 21 7e 48 a5 62 7a 96 e9 65 f7 c2 21 5e 2e 49 73 1d b1 f9 af d7 d7 1f c9 a8 37 22 7f 30 25 32 e9 33 92 08 4d 96 22 4b 82 a9 67 87 1c 4d 95 de 44 8c e0 0a b9 60 5f 29 67 7e b4 10 c1 86 dc c7 54 ae 78 32 26 bd 09 49 69 10 f0 64 65 9e 17 d4 bf 59 49 94 33 26 c7 cb e5 72 02 42 13 3d 26 fd 41 7a e7 0d e0 0f 69 fd 87 c9 80 26 b4 05 2a 8a 48 48 18 77 7e 81 d7 e4 c1 8a a6 e4 be e8 18 0e e8 c0 07 19 b8 7a 37 60 be 90 54 73 01 ab 82 7c 26 23 9e b0 72 d2 38 14 b7 4c 92 fb bd a1 89 30 a3 74 70 4a 78 92 66 fa 94 28 16 31 1f ee 38 94 4a 06 eb 55 3a 92 a7 95 74 fd 88 51 58 c9 dc c6 64 21 74 68 5a ad 0f c8 fd 9a 07 3a 1c 93 17 c3 b3 f4 6e 42 0a 9c 68 a6 05 0c f3 9e 77 f3 1f 7a 97 49 fb fc dc 3b 3a b6 ef e4 3e 64 7c 15 82 36 67 66 7a 1d cf 4c 46 6d cf 55 1e 8f 57 1e 93 d2 03 ff 15 52 10 0a 77 c5 97 1d 22 59 ca a8 ee de 91 1e f8 17 24 3c 1c 1d 47 62 25 c0 c6 48 50 10 1b b1 a5 ae b4 aa 7b 6f 70 9e e2 ac 1e 36 e6 36 8c 86 a8 43 a1 d1 e0 45 4d 1e a0 16 70 95 46 74 03 10 44 c2 bf a9 c7 01 79 89 f3 0e 0b 21 e8 2b 50 68 3d 26 21 0f 02 96 40 4b a6 d1 88 dc 5f d6 e3 1c bc 8c 8e e9 be 84 df 2e 1a 18 5d 8d 90 a0 7a 6e 9a ac 3a 20 aa 6b e1 20 3e c8 01 70 ed 0d bd a5 b8 66 5d 1f 9c af 59 09 8d 44 0d 2b 6c ea 78 3c 62 ea 99 19 d5 37 de ca e3 a8 8f b1 7e 7e 20 8c 5e f8 3d 36 f8 49 53 a8 94 62 bd 6b 0b 7a 90 f4 ad 6f ab 70 aa ff 20 9c aa 8e 98 f2 a4 d6 71 8c ef e4 be 34 e0 ac 67 f4 3f 33 66 20 32 66 bc 59 63 3b 64 72 6f f6 cf 71 65 eb 1f 1a f1 15 00 55 a1 0a 7a 0b 69 e8 a3 cc a9 0b c4 62 d4 8c c5 0b b6 18 05 83 72 a2 2f 02 56 11 4b df 2a 36 b0 8a 95 cb db b4 28 a2 e9 fc fc 27 92 64 07 40 5c 2f a5 2b 06 8c 67 08 af 54 75 84 aa f6 0e a9 8a d7 de 54 9a 13 8e 96 34 51 4b 21 63 50 20 4d 99 f4 a9 62 4d 76 1a 70 4d 9c 35 a3 3b 7a b9 45 1a 26 fa c8 85 f5 75 7d 72 38 dc 62 e0 1a c7 22 e0 4d 06 0c 86 78 95 62 4a b6 6a 62 82 fe b0 8c fc dd f1 59 54 4d 19 96 91 0f 19 8a 6a d7 37 82 88 2b dd 35 3b 48 49 c1 c7 0a 08 d3 0f c9 3d e6 9f 79 5c 0b 19 94 84 39 7c d1 db 16 42 b6 5c 3d 30 bd c8 11 dd ed a6 1d e6 58 80 4c 06 16 43 12 12 25 22 1e 90 63 7f 89 57 d1 d5 95 34 e0 99 1a 5b f1 40 44 9a fb 34 2a 82 39 06 3e 8a 8c a3 ad 8a 6a 11 3f 1a 20 a5 2e 03 94 56 a0 7d 36 a2 41 b9 71 a9 90 06 48 75 3d a3 13 fe b3 3b 63 cd 52 23 15 37 1e 6b 52 93 0d 43 bc c8 33 1e a7 90 62 34 d1 cd e6 6c d1 0a bb c0 6b 2f 25 16 99 d6 22 b1 59 51 6c 17 a0 7a 26 15 ea 9e 0a 6e d2 79 17 d7 03 40 d5 a8 fc 96 2b be 30 d8 3d 1f 2f b9 04 ff fb 21 8f 82 13 ac 47 48 1d ce c2 bc 5e dd 9c 9f 21 b3 a5 10 ba d8 33 0d 99 d9 86 1a 9d f5 cf 2a d2 ce f1 d1 22 dd 42 32 58 e0 85 1e ce c5 81 d3 9a b3 71 30 72 5f fe 6b 67 60 38 22 f7 5b f9 d9 cf 09 aa c6 fd fd 03 7c 77 76 8e d7 8e 40 cc a8 c6 fd b8 39 89 76 a6 46 1c 66 d7 97 3e 90 fe 17 14 af 9d f9 30 19 08 6c 77 cc 7e b5 d5 b0 34 4e 3d 58 72 d5 ab b3 83 4e 9d 7a c6 30 a8 33 3d 5b e8 4e b1 90 c3 b2 d3 97 3c d5 f5 ba f3 3b bd a5 b6 d5 c1 2a f6 16 aa af 6f 2b fa 83 cc ec Data Ascii: a01Yo8=`%~m.n{(hHJRq7Ce[NgpCuPhZG~i:9H4KtWoRmhv=>!~Hbze!^.Is7"0%23M"KgMD`_)g~Tx2&lideYI3 &rB=&Azi&*HHw~z7`Ts|&#r8L0tpJxf(18JU:tQXd!thZ:nBhwzI;:>d|6gfzLFmUWRw"Y$<Gb%HP{op66CEMpFtDy !+Ph=&!@K_.]zn: k >pf]YD+lx<b7~~ ^=6ISbkzop q4g?3f 2fYc;droqeUzibr/VK*6('d@V+gTuT4QK!cP MbMvpM5;zE& u}r8b"MxbJjbYTMj7+5;HI=y\9|B\=0XLC%"cW4[@D4*9>j? .V}6AqHu=;cR#7kRC3b4Ik/%"YQlz&ny@+0=/!GH^!3*"B2Xq0r _kg`8"[|wv@9vFf>0lw~4N=XrNz03=[N<;*o+
Oct 29, 2021 17:51:15.785171032 CEST	1457	OUT	GET /.s/img/err/button.png HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive
Oct 29, 2021 17:51:15.852315903 CEST	1459	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 29 Oct 2021 15:51:17 GMT Content-Type: image/png Content-Length: 1036 Last-Modified: Mon, 31 Jul 2017 10:32:10 GMT Connection: keep-alive Keep-Alive: timeout=15 ETag: "597f072a-40c" Expires: Thu, 18 Nov 2021 15:51:17 GMT Cache-Control: max-age=1728000 Accept-Ranges: bytes
Oct 29, 2021 17:51:15.858786106 CEST	1461	OUT	GET /.s/img/err/404-arrow.png HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive
Oct 29, 2021 17:51:15.925990105 CEST	1464	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 29 Oct 2021 15:51:17 GMT Content-Type: image/png Content-Length: 1169 Last-Modified: Mon, 31 Jul 2017 10:32:10 GMT Connection: keep-alive Keep-Alive: timeout=15 ETag: "597f072a-491" Expires: Thu, 18 Nov 2021 15:51:17 GMT Cache-Control: max-age=1728000 Accept-Ranges: bytes

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.933043003 CEST	1467	OUT	GET /.s/img/err/button.png HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive
Oct 29, 2021 17:51:16.000112057 CEST	1474	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 29 Oct 2021 15:51:17 GMT Content-Type: image/png Content-Length: 1036 Last-Modified: Mon, 31 Jul 2017 10:32:10 GMT Connection: keep-alive Keep-Alive: timeout=15 ETag: "597f072a-40c" Expires: Thu, 18 Nov 2021 15:51:17 GMT Cache-Control: max-age=1728000 Accept-Ranges: bytes
Oct 29, 2021 17:51:16.003344059 CEST	1478	OUT	GET /.s/img/err/404-logo.png HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive
Oct 29, 2021 17:51:16.070466995 CEST	1495	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 29 Oct 2021 15:51:17 GMT Content-Type: image/png Content-Length: 2152 Last-Modified: Mon, 31 Jul 2017 10:32:10 GMT Connection: keep-alive Keep-Alive: timeout=15 ETag: "597f072a-868" Expires: Thu, 18 Nov 2021 15:51:17 GMT Cache-Control: max-age=1728000 Accept-Ranges: bytes
Oct 29, 2021 17:51:16.074219942 CEST	1499	OUT	GET /.s/img/err/404.png HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.all-bearings.narod.ru Connection: Keep-Alive
Oct 29, 2021 17:51:16.141700029 CEST	1666	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 29 Oct 2021 15:51:17 GMT Content-Type: image/png Content-Length: 4451 Last-Modified: Mon, 31 Jul 2017 10:32:10 GMT Connection: keep-alive Keep-Alive: timeout=15 ETag: "597f072a-1163" Expires: Thu, 18 Nov 2021 15:51:17 GMT Cache-Control: max-age=1728000 Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49787	88.212.201.198	80	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.440135956 CEST	1437	OUT	GET /hit;counter1?r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/firstpage.html;0.34476715437082456 HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: counter.yadro.ru Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.499608040 CEST	1439	IN	HTTP/1.1 302 Moved Temporarily Date: Fri, 29 Oct 2021 15:51:23 GMT Server: 0W/0.8c Content-Type: text/html Location: https://counter.yadro.ru/hit;counter1?r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/firstpage.html;0.34476715437082456 Content-Length: 32 Expires: Wed, 28 Oct 2020 21:00:00 GMT Pragma: no-cache Cache-control: no-cache Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 4d 6f 76 65 64 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body>Moved</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49788	87.250.251.119	80	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.440211058 CEST	1437	OUT	GET /metrika/watch.js HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: mc.yandex.ru Connection: Keep-Alive
Oct 29, 2021 17:51:15.481770992 CEST	1438	IN	HTTP/1.1 302 Moved temporarily Content-Length: 0 Location: https://mc.yandex.ru/metrika/watch.js

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49789	87.250.251.119	80	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.440260887 CEST	1438	OUT	GET /metrika/watch.js HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: mc.yandex.ru Connection: Keep-Alive
Oct 29, 2021 17:51:15.482186079 CEST	1439	IN	HTTP/1.1 302 Moved temporarily Content-Length: 0 Location: https://mc.yandex.ru/metrika/watch.js

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49786	88.212.201.198	80	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.440336943 CEST	1438	OUT	GET /hit;counter1?r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/secondpage.html;0.5443641556055339 HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: counter.yadro.ru Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 29, 2021 17:51:15.503304958 CEST	1440	IN	HTTP/1.1 302 Moved Temporarily Date: Fri, 29 Oct 2021 15:51:23 GMT Server: 0W/0.8c Content-Type: text/html Location: https://counter.yadro.ru/hit;counter1?r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/secondpage.html;0.5443641556055339 Content-Length: 32 Expires: Wed, 28 Oct 2020 21:00:00 GMT Pragma: no-cache Cache-control: no-cache Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 4d 6f 76 65 64 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body>Moved</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49791	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49793	88.212.201.198	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49795	88.212.201.198	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49794	88.212.201.198	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49796	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49797	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49798	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49799	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49790	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:15 UTC	0	OUT	GET /metrika/watch.js HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Connection: Keep-Alive Host: mc.yandex.ru
2021-10-29 15:51:16 UTC	1	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Cache-Control: max-age=3600 Connection: Close Content-Length: 132911 Content-Type: application/javascript Date: Fri, 29 Oct 2021 15:51:16 GMT ETag: "617677e6-2072f" Expires: Fri, 29 Oct 2021 16:51:16 GMT Last-Modified: Mon, 25 Oct 2021 12:24:54 GMT Strict-Transport-Security: max-age=31536000
2021-10-29 15:51:16 UTC	1	IN	Data Raw: ef bb bf 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 28 66 75 6e 63 74 69 6f 6e 28 4a 63 29 7b 66 75 6e 63 74 69 6f 6e 20 48 69 28 61 29 7b 72 65 74 75 72 6e 20 61 2e 72 65 70 6c 61 63 65 28 49 69 2c 66 75 6e 63 74 69 6f 6e 28 62 2c 63 2c 64 2c 65 29 7b 72 65 74 75 72 6e 22 22 2b 63 2b 65 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 4b 63 28 61 2c 62 29 7b 69 66 28 21 62 29 72 65 74 75 72 6e 21 31 3b 76 61 72 20 63 3d 4d 28 61 29 3b 72 65 74 75 72 6e 28 6e 65 77 20 52 65 67 45 78 70 28 62 29 29 2e 74 65 73 74 28 22 22 2b 63 2e 70 61 74 68 6e 61 6d 65 2b 63 2e 68 61 73 68 2b 63 2e 73 65 61 72 63 68 29 7d 66 75 6e 63 74 69 6f 6e 20 4a 69 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 44 61 28 61 2c 62 2c 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d 6e 28 63 2c Data Ascii: (function(){try{(function(Jc){function Hi(a){return a.replace(Ii,function(b,c,d,e){return""+c+e})}function Kc(a,b){if(!b)return!1;var c=M(a);return(new RegExp(b)).test(""+c.pathname+c.hash+c.search)}function Ji(a,b){return Da(a,b,function(c){var d=n(c,
2021-10-29 15:51:16 UTC	14	IN	Data Raw: 74 61 26 26 28 64 3d 30 3c 61 2e 77 68 65 65 6c 44 65 6c 74 61 3f 32 3a 30 3e 61 2e 77 68 65 65 6c 44 65 6c 74 61 3f 31 3a 30 29 3b 69 66 28 64 29 7b 76 61 72 20 65 3d 4d 63 28 62 2c 61 29 3b 61 3d 64 62 28 62 2c 63 29 3b 62 3d 74 61 28 62 29 3b 65 3d 5b 65 2e 78 2c 65 2e 79 5d 3b 63 3d 63 5b 6d 61 5d 3b 69 66 28 21 63 7c 7c 30 3e 63 29 63 3d 5b 5d 3b 65 6c 73 65 7b 76 61 72 20 66 3d 5b 5d 3b 75 61 28 66 2c 33 31 29 3b 7a 28 66 2c 62 29 3b 7a 28 66 2c 63 29 3b 7a 28 66 2c 65 5b 30 5d 29 3b 7a 28 66 2c 65 5b 31 5d 29 3b 75 61 28 66 2c 30 29 3b 75 61 28 66 2c 30 29 3b 75 61 28 66 2c 64 29 3b 63 3d 66 7d 72 65 74 75 72 6e 20 50 28 61 2c 63 29 7d 7d 7d 66 75 6e 63 74 69 6f 6e 20 6d 66 28 61 29 7b 76 61 72 20 62 3d 61 2e 6f 3b 61 3d 4c 64 28 62 29 3b 76 61 72 Data Ascii: ta&&(d=0<a.wheelDelta?2:0>a.wheelDelta?1:0);if(d){var e=Mc(b,a);a=db(b,c);b=ta(b);e=[e.x,e.y];c=c[ma];if(!c||0>c)c=[];else{var f=[];ua(f,31);z(f,b);z(f,c);z(f,e[0]);z(f,e[1]);ua(f,0);ua(f,0);ua(f,d);c=f}return P(a,c)}}}function mf(a){var b=a.o;a=Ld(b);var
2021-10-29 15:51:16 UTC	22	IN	Data Raw: 2b 63 2b 22 2e 22 29 3b 47 64 28 61 2c 62 2c 22 62 74 6e 22 2c 64 29 28 63 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 4b 6a 28 61 2c 62 29 7b 76 61 72 20 63 3d 41 61 28 61 29 3b 69 66 28 22 22 21 3d 3d 63 2e 62 28 22 63 63 22 29 29 72 65 74 75 72 6e 20 30 3b 76 61 72 20 64 3d 76 28 22 63 63 22 2c 63 2e 6c 29 3b 64 28 30 29 3b 76 61 72 20 65 3d 57 28 61 29 2c 66 3d 4c 28 61 29 3b 66 3d 71 28 54 28 57 61 28 7b 44 61 3a 31 7d 29 2b 22 2e 63 22 29 2c 4d 62 28 66 75 6e 63 74 69 6f 6e 28 67 29 7b 64 28 67 2b 22 26 22 2b 65 28 58 61 29 29 7d 29 2c 76 28 22 63 63 22 2c 66 2e 6c 29 29 3b 64 61 28 61 2c 22 36 22 2c 62 29 28 7b 7d 29 2e 74 68 65 6e 28 66 29 5b 22 63 61 74 63 68 22 5d 28 71 28 4d 62 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 67 3d 65 28 58 61 29 3b 63 Data Ascii: +c+".");Gd(a,b,"btn",d)(c)}}function Kj(a,b){var c=Aa(a);if(""!==c.b(""cc""))return 0;var d=v(""cc"",c.l);d(0);var e=W(a),f=L(a);f=q(T(Wa({Da:1})+".c"),Mb(function(g){d(g+"&"+e(Xa))}),v(""cc"",f.l));da(a,"6",b){}).then(f)[""catch""](q(Mb(function(){var g=e(Xa);c
2021-10-29 15:51:16 UTC	30	IN	Data Raw: 75 72 6e 20 53 28 66 75 6e 63 74 69 6f 6e 28 64 2c 65 29 7b 64 5b 65 5d 3d 63 28 22 28 22 2b 65 2b 22 29 22 29 3b 72 65 74 75 72 6e 20 64 7d 2c 7b 7d 2c 6e 6b 29 7d 66 75 6e 63 74 69 6f 6e 20 56 69 28 61 29 7b 61 3d 65 62 28 61 29 3b 69 66 28 21 61 29 72 65 74 75 72 6e 22 22 3b 61 3d 61 28 22 76 69 64 65 6f 22 29 3b 74 72 79 7b 76 61 72 20 62 3d 63 61 28 22 63 61 6e 50 6c 61 79 54 79 70 65 22 2c 61 29 2c 63 3d 76 62 28 66 75 6e 63 74 69 6f 6e 28 64 29 7b 72 65 74 75 72 6e 20 49 28 71 28 4b 2c 63 61 28 22 63 63 22 2c 64 2b 22 3b 20 63 6f 64 65 63 73 3d 22 29 2c 6f 6b 29 7d 2c 61 67 29 3b 72 65 74 75 72 6e 20 49 28 62 2c 5b 5d 2e 63 6f 6e 63 61 74 28 61 67 2c 63 29 29 7d 63 61 74 63 68 28 64 29 7b 72 65 74 75 72 6e 22 63 61 6e 50 6c 61 79 54 Data Ascii: urn S(function(d,e){d[e]=c("("+e+")");return d},{},nk)}function Vi(a){a=eb(a);if(!a)return"";a=a("video");try{var b=ca("canPlayType",a),c=vb(function(d){return I(q(K,ca("concat",d+"; codecs=")),ok)},ag);return I(b,[].concat(ag,c))}catch(d){return"canPlayT
2021-10-29 15:51:16 UTC	38	IN	Data Raw: 74 75 72 6e 20 64 26 26 21 65 3f 66 3a 67 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 24 6b 28 61 2c 62 2c 63 2c 64 29 7b 62 3d 64 2e 62 28 22 63 63 22 29 3b 64 3d 47 28 5b 22 63 63 22 2c 22 22 5d 2c 64 2e 6c 29 3b 69 66 28 62 29 7b 76 61 72 20 65 3d 62 2e 73 70 6c 69 74 28 22 26 22 29 3b 62 3d 65 5b 30 5d 3b 69 66 28 28 65 3d 62 3d 65 5b 31 5d 29 26 26 70 61 72 73 65 49 6e 74 28 65 2c 31 30 29 29 26 26 31 34 34 30 3c 57 28 61 29 28 58 61 29 2d 65 29 72 65 74 74 75 72 6e 20 64 28 29 3b 63 2e 6c 28 22 63 63 22 2c 62 29 7d 65 6c 73 65 20 73 61 28 30 29 28 62 29 7c 7c 64 28 29 7d 66 75 6e 63 74 69 6f 6e 20 61 6c 28 61 2c 62 2c 63 2c 64 29 7b 72 65 74 75 72 6e 20 44 61 28 61 2c 62 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 69 66 28 22 30 22 3d 3d 3d 6e 28 65 2c 22 73 65 Data Ascii: turn d&&!e?f:g})}function $k(a,b,c,d){b=d.b("cc");d=G(["cc",""],d.l);if(b){var e=b.split("&");b=e[0];if((e=(e=e[1])&&parseInt(e,10))&&1440<W(a)(Xa)-e)return d();c.l("cc",b)}else sa(0)(b)||d()}function al(a,b,c,d){return Da(a,b,function(e){if("0"===n(e,"se

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:16 UTC	78	IN	Data Raw: 20 76 61 28 66 75 6e 63 74 69 6f 6e 28 62 2c 63 29 7b 63 28 61 29 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 77 6b 28 61 29 7b 72 65 74 75 72 6e 20 76 61 28 66 75 6e 63 74 69 6f 6e 28 62 2c 63 29 7b 61 2e 74 68 65 6e 28 63 2c 62 29 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 76 6b 28 61 29 7b 76 61 72 20 62 3d 5b 5d 2c 63 3d 21 31 3b 72 65 74 75 72 6e 20 76 61 28 66 75 6e 63 74 69 6f 6e 28 64 2c 65 29 7b 66 75 6e 63 74 69 6f 6e 20 66 28 67 29 7b 62 2e 70 75 73 68 28 67 29 3d 3d 3d 61 2e 6c 65 6e 67 74 68 26 26 64 28 62 29 7d 44 28 66 75 6e 63 74 69 6f 6e 28 67 29 7b 67 28 50 63 28 66 2c 66 75 6e 63 74 69 6f 6e 28 68 29 7b 69 66 28 21 63 29 74 72 79 7b 65 28 68 29 2c 63 3d 21 30 7d 63 61 74 63 68 28 6b 29 7b 66 28 6b 29 7d 7d 29 29 7d 2c 61 29 7d 29 7d 66 75 6e 63 74 69 Data Ascii: va(function(b,c){c(a)})}function wk(a){return va(function(b,c){a.then(c,b)})}function vk(a){var b=[],c=!1;return va(function(d,e){function f(g){b.push(g)===a.length&&d(b)}D(function(g){g(Pc(f,function(h){if(!c)try{e(h),c=!0}catch(k){f(k)}}))},a)})}functi
2021-10-29 15:51:16 UTC	86	IN	Data Raw: 3b 29 64 2b 3d 65 5b 66 5d 7c 7c 22 2a 22 2c 64 2b 3d 6b 68 28 61 2c 62 2c 63 29 7c 7c 22 22 2c 62 3d 62 2e 70 61 72 65 6e 74 45 6c 65 6d 65 6e 74 2c 66 3d 4c 61 28 62 29 7c 7c 22 2a 22 3b 72 65 74 75 72 6e 20 7a 62 28 64 2c 31 32 38 29 7d 66 75 6e 63 74 69 6f 6e 20 6b 68 28 61 2c 62 2c 63 29 7b 69 66 28 61 3d 64 28 61 2c 62 29 29 7b 61 3d 61 2e 63 68 69 6c 64 4e 6f 64 65 73 3b 66 6f 72 28 76 61 72 20 64 3d 62 26 26 62 2e 6e 6f 64 65 4e 61 6d 65 2c 65 3d 30 2c 66 3d 30 3b 66 3c 61 2e 6c 65 6e 67 74 68 3b 66 2b 3d 31 29 69 66 28 64 3d 3d 3d 28 61 5b 66 5d 26 26 61 5b 66 5d 2e 6e 6f 64 65 4e 61 6d 65 29 29 7b 69 66 28 62 3d 3d 61 5b 66 5d 29 72 65 74 75 72 6e 20 65 3b 63 26 26 61 5b 66 5d 3d 3d 3d 63 7c 7c 28 65 2b 3d 31 29 7d 7d 72 65 74 75 72 6e 20 Data Ascii: ;)d+=e[f]||"*",d+=kh(a,b,c)||"",b=b.parentElement,f=La(b)||"*";return zb(d,128)}function kh(a,b,c){if(a=dd(a,b)){a=a.childNodes;for(var d=b&&b.nodeName,e=0,f=0;f<a.length;f+=1)if(d===(a[f]&&a[f].nodeName)){if(b===a[f])return e;c&&a[f]===c||(e+=1)}}return
2021-10-29 15:51:16 UTC	94	IN	Data Raw: 20 78 68 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 7a 63 28 66 75 6e 63 74 69 6f 6e 28 63 2c 64 2c 65 29 7b 61 28 64 2c 65 29 26 26 63 2e 70 75 73 68 28 64 29 3b 72 65 74 75 72 6e 20 63 7d 2c 5b 5d 2c 62 29 7d 66 75 6e 63 74 69 6f 6e 20 6e 63 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 42 61 28 61 29 7b 69 66 28 41 63 28 61 29 7b 69 66 28 41 63 3d 71 61 28 41 72 72 61 79 2e 69 73 41 72 72 61 79 2c 22 69 73 41 72 72 61 79 22 29 29 7c 7c 28 41 63 3d 6d 6d 29 3b 72 65 74 75 72 6e 20 41 63 28 61 29 7d 66 75 6e 63 74 69 6f 6e 20 49 61 28 61 29 7b 69 66 28 41 63 29 72 65 74 75 72 6e 20 41 63 28 61 29 3b 28 41 63 3d 71 61 28 41 72 72 61 79 2e 69 73 41 72 72 61 79 2c 22 69 73 41 72 72 61 79 22 29 29 7c 7c 28 41 63 3d 6d 6d 29 3b 72 65 74 75 72 6e 20 71 28 29 7b 76 61 72 20 61 3d 6e 61 28 61 72 67 75 6d 65 6e 74 73 29 2c 62 3d 61 2e 73 68 69 66 74 28 29 3b 72 65 74 75 72 6e Data Ascii: xh(a,b){return zc(function(c,d,e){a(d,e)&&c.push(d);return c},[],b)}function nc(a,b){return Ba(a)?!1:Ce.call(a,b)}function Ia(a){if(Ac)return Ac(a);(Ac=qa(Array.isArray,"isArray"))||(Ac=mm);return Ac(a)}function q(){var a=na(arguments),b=a.shift();return
2021-10-29 15:51:16 UTC	102	IN	Data Raw: 70 3d 59 28 70 2c 4d 61 28 5b 30 2c 63 2e 63 68 61 72 43 6f 64 65 41 74 28 6c 2b 31 30 29 5d 2c 31 36 29 29 3b 63 61 73 65 20 31 30 3a 70 3d 59 28 70 2c 4d 61 28 5b 30 2c 63 2e 63 68 61 72 43 6f 64 65 41 74 28 6c 2b 39 29 5d 2c 38 29 29 3b 63 61 73 65 20 39 3a 70 3d 59 28 70 2c 5b 30 2c 63 2e 63 68 61 72 43 6f 64 65 41 74 28 6c 2b 38 29 5d 29 2c 70 3d 50 61 28 70 2c 6b 29 2c 70 3d 58 62 28 70 2c 33 33 29 2c 70 3d 50 61 28 70 2c 68 29 2c 64 3d 59 28 64 2c 70 29 3b 63 61 73 65 20 38 3a 6d 3d 59 28 6d 2c 4d 61 28 5b 30 2c 63 2e 63 68 61 72 43 6f 64 65 41 74 28 6c 2b 37 29 5d 2c 35 36 29 29 3b 63 61 73 65 20 37 3a 6d 3d 59 28 6d 2c 4d 61 28 5b 30 2c 63 2e 63 68 61 72 43 6f 64 65 41 74 28 6c 2b 36 29 5d 2c 34 38 29 29 3b 63 61 73 65 20 36 3a 6d 3d 59 28 6d 2c Data Ascii: p=Y(p,Ma([0,c.charCodeAt(l+10)],16));case 10:p=Y(p,Ma([0,c.charCodeAt(l+9)],8));case 9:p=Y(p,[0,c.charCodeAt(l+8)]),p=Pa(p,k),p=Xb(p,33),p=Pa(p,h),d=Y(d,p);case 8:m=Y(m,Ma([0,c.charCodeAt(l+7)],56));case 7:m=Y(m,Ma([0,c.charCodeAt(l+6)],48));case 6:m=Y(m,
2021-10-29 15:51:16 UTC	110	IN	Data Raw: 3d 4c 61 28 61 29 26 26 62 28 29 7d 66 75 6e 63 74 69 6f 6e 20 70 64 28 61 2c 62 2c 63 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 64 3d 45 61 28 61 2c 62 29 2c 65 3d 6e 61 28 61 72 67 75 6d 65 6e 74 73 29 3b 69 66 28 64 29 72 65 74 75 72 6e 20 63 2e 61 70 70 6c 79 28 76 6f 69 64 20 30 2c 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 51 6d 28 61 2c 62 2c 63 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 64 3d 45 61 28 61 2c 62 29 2c 65 3d 6e 61 28 61 72 67 75 6d 65 6e 74 73 29 3b 63 2e 61 70 70 6c 79 28 76 6f 69 64 20 30 2c 65 29 3b 72 65 74 75 72 6e 20 64 7d 7d 66 75 6e 63 74 69 6f 6e 20 52 6d 28 61 2c 62 2c 63 2c 64 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 66 6f 72 28 76 61 72 20 65 3d 5b Data Ascii: =La(a)&&b()}function pd(a,b,c){return function(){var d=Ea(a,b),e=na(arguments);if(d)return c.apply(void 0,e)}}function Qm(a,b,c){return function(){var d=Ea(a,b),e=na(arguments);c.apply(void 0,e);return d}}function Rm(a,b,c,d){return function(){for(var e=[
2021-10-29 15:51:16 UTC	118	IN	Data Raw: 73 6b 7c 2e 2a 5c 2e 79 61 6e 64 65 78 7c 74 75 72 62 6f 70 61 67 65 73 5c 2e 6f 72 67 7c 74 75 72 62 6f 5c 2e 73 69 74 65 29 24 2f 2c 0a 74 6b 3d 74 28 66 75 6e 63 74 69 6f 6e 28 61 29 7b 61 3d 4d 28 61 29 2e 68 6f 73 74 6e 61 6d 65 3b 76 61 72 20 62 3d 21 31 3b 61 26 26 28 62 3d 2d 31 21 3d 3d 61 2e 73 65 61 72 63 68 28 68 6e 29 29 3b 72 65 74 75 72 6e 20 62 7d 29 2c 6a 6e 3d 2f 28 3f 3a 5e 7c 5c 2e 29 28 3f 3a 79 61 7c 79 61 6e 64 65 78 29 5c 2e 28 3f 3a 5c 77 2b 7c 63 6f 6d 3f 5c 2e 5c 77 2b 29 24 2f 2c 6b 6e 3d 74 28 66 75 6e 63 74 69 6f 6e 28 61 29 7b 61 3d 4d 28 61 29 2e 68 6f 73 74 6e 61 6d 65 3b 76 61 72 20 62 3d 21 31 3b 61 26 26 28 62 3d 2d 31 21 3d 3d 61 2e 73 65 61 72 63 68 28 6a 6e 29 29 3b 72 65 74 75 72 6e 20 62 7d 29 2c 74 6d 3d 74 28 66 Data Ascii: sk|.*\.yandex|turbopages\.org|turbo\.site)$/,tk=t(function(a){a=M(a).hostname;var b=!1;a&&(b=-1!==a.search(hn));return b}),jn=/(?:^|\.)(?:ya|yandex)\.(?:\w+|com?\.\w+)$/,kn=t(function(a){a=M(a).hostname;var b=!1;a&&(b=-1!==a.search(jn));return b}),tm=t(f
2021-10-29 15:51:16 UTC	174	IN	Data Raw: 22 3a 22 2a 22 2c 22 2f 22 3a 22 2d 22 2c 22 3d 22 3a 22 5f 22 7d 2c 45 63 3d 74 28 66 75 6e 63 74 69 6f 6e 28 61 29 7b 61 3d 6e 28 61 2c 22 63 6f 6e 73 6f 6c 65 22 29 3b 76 61 72 20 62 3d 6e 28 61 2c 22 6c 6f 67 22 29 3b 62 3d 6e 64 28 22 6c 6f 67 22 2c 62 29 3f 45 28 62 2c 61 29 3a 43 3b 76 61 72 20 63 3d 6e 28 61 2c 22 77 61 72 6e 22 29 3b 3d 6e 64 28 22 77 61 72 6e 22 2c 63 29 3f 45 28 63 2c 61 29 3a 62 3b 76 61 72 20 64 3d 6e 28 61 2c 22 65 72 72 6f 72 22 29 3b 61 3d 6e 64 28 22 65 72 72 6f 72 22 2c 64 29 3f 45 28 64 2c 61 29 3a 62 3b 72 65 74 75 72 6e 7b 6c 6f 67 3a 62 2c 65 72 72 6f 72 3a 61 2c 77 61 72 6e 3a 63 7d 7d 29 2c 78 6e 3d 41 28 22 70 2e 63 64 22 2c 66 75 6e 63 74 69 6f 6e 28 61 29 7b 69 66 28 68 64 28 61)||Ae(a)) Data Ascii: ":"*","/":"-","=":"_"},Ec=t(function(a){a=n(a,"console");var b=n(a,"log");b=nd("log",b)?E(b,a):C;var c=n(a,"warn");c=nd("warn",c)?E(c,a):b;var d=n(a,"error");a=nd("error",d)?E(d,a):b;return{log:b,error:a,warn:c}}),xn=A("p.cd",function(a){if(hd(a)||Ae(a))
2021-10-29 15:51:16 UTC	182	IN	Data Raw: 75 72 6e 20 6e 75 6c 6c 3b 64 3d 64 2e 63 61 6c 6c 28 61 2e 64 6f 63 75 6d 65 6e 74 2c 0a 22 69 66 72 61 6d 65 22 29 3b 66 3d 28 63 3d 7b 7d 2c 63 2e 63 6f 75 6e 74 65 72 49 64 3d 62 2e 69 64 2c 63 2e 68 69 64 3d 22 22 2b 51 62 28 61 29 2c 63 29 3b 6a 6c 28 61 2c 67 29 3b 63 3d 4c 6e 28 61 2c 66 29 3b 76 61 72 20 6b 3d 4e 6e 28 61 2c 6c 29 3b 74 72 79 7b 6d 3d 6c 2e 63 6f 6e 74 65 6e 74 57 69 6e 64 6f 77 7d 63 61 74 63 68 28 70 29 7b 7d 6d 26 26 6b 28 6d 2c 7b 74 79 70 65 3a 22 69 6e 69 74 54 6f 43 68 69 6c 64 22 7d 2c 66 75 6e 63 74 69 6f 6e 28 70 2c 75 29 7b 67 2e 4a 28 22 69 6e 69 74 54 6f 50 61 72 65 6e 74 22 2c 5b 70 2c 75 5d 29 7d 29 7d 2c 64 29 3b 48 62 28 61 29 Data Ascii: urn null;d=d.call(a.document,"iframe");f=(c={},c.counterId=b.id,c.hid=""+Qb(a),c);jl(a,g);c=Ln(a,f);var k=Nn(a,c([]));D(function(l){var m=null;try{m=l.contentWindow}catch(p){}m&&k(m,{type:"initToChild"},function(p,u){g.J("initToParent",[p,u])})},d);Hb(a)

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:16 UTC	190	IN	Data Raw: 3d 0a 64 7d 61 2e 70 72 6f 74 6f 74 79 70 65 2e 51 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 70 61 28 74 68 69 73 2e 6f 2c 71 28 45 28 74 68 69 73 2e 66 6c 75 73 68 2c 74 68 69 73 29 2c 45 28 74 68 69 73 2e 51 62 2c 74 68 69 73 29 29 2c 74 68 69 73 2e 6c 62 2c 22 62 2e 66 22 29 7d 3b 61 2e 70 72 6f 74 6f 74 79 70 65 2e 73 65 6e 64 3d 66 75 6e 63 74 69 6f 6e 28 62 2c 63 29 7b 74 68 69 73 2e 55 63 28 62 2c 63 7c 7c 5b 5d 2c 74 68 69 73 2e 56 61 29 3b 74 68 69 73 2e 56 61 2b 3d 31 7d 3b 61 2e 70 72 6f 74 6f 74 79 70 65 2e 70 75 73 68 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 3b 61 2e 70 72 6f 74 6f 74 79 70 65 2e 66 6c 75 73 68 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 3b 72 65 74 75 72 6e 20 61 7d 28 29 2c 67 67 3d 61 61 28 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b Data Ascii: =d}a.prototype.Qb=function(){pa(this.o,q(E(this.flush,this),E(this.Qb,this)),this.lb,"b.f")};a.prototype.send=function(b,c){this.Uc(b,c||[],this.Va);this.Va+=1};a.prototype.push=function(){};a.prototype.flush=function(){};return a}(),gg=aa(function(a,b){
2021-10-29 15:51:16 UTC	198	IN	Data Raw: 5b 5d 3b 63 2e 24 62 3d 37 35 30 30 3b 63 2e 6c 62 3d 33 45 34 3b 63 2e 51 62 28 29 3b 72 65 74 75 72 6e 20 63 7d 70 6d 28 62 2c 61 29 3b 62 2e 70 72 6f 74 6f 74 79 70 65 2e 70 75 73 68 3d 66 75 6e 63 74 69 6f 6e 28 63 2c 64 29 7b 76 61 72 20 65 3d 74 68 69 73 2e 4f 62 2e 4e 62 28 63 2c 64 29 3b 4a 61 28 74 68 69 73 2e 62 75 66 66 65 72 2c 65 29 3b 74 68 69 73 2e 4f 62 2e 7a 63 28 74 68 69 73 2e 62 75 66 66 65 72 29 3e 74 68 69 73 2e 24 62 26 26 74 68 69 73 2e 66 6c 75 73 68 28 29 7d 3b 62 2e 70 72 6f 74 6f 74 79 70 65 2e 66 6c 75 73 68 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 63 3d 74 68 69 73 2e 62 75 66 66 65 72 3b 63 2e 6c 65 6e 67 74 68 26 26 28 74 68 69 73 2e 73 65 6e 64 28 63 29 2c 74 68 69 73 2e 62 75 66 66 65 72 3d 5b 5d 29 7d 3b 72 65 74 Data Ascii: [];c.$b=7500;c.lb=3E4;c.Qb();return c}pm(b,a);b.prototype.push=function(c,d){var e=this.Ob.Nb(c,d);Ja(this.buffer,e);this.Ob.zc(this.buffer)>this.$b&&this.flush()};b.prototype.flush=function(){var c=this.buffer;c.length&&(this.send(c),this.buffer=[])};ret
2021-10-29 15:51:16 UTC	206	IN	Data Raw: 6e 28 65 29 7b 65 2e 43 28 64 29 7d 29 7d 7d 29 2c 49 6f 3d 41 28 22 66 69 64 22 2c 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 2c 63 3d 43 3b 69 66 28 21 4f 28 61 2e 50 65 72 66 6f 72 6d 61 6e 63 65 4f 62 73 65 72 76 65 72 29 29 72 65 74 75 72 6e 20 63 3b 76 61 72 20 64 3d 4c 28 61 29 3b 69 66 28 64 2e 62 28 22 66 69 64 6f 22 29 29 72 65 74 75 72 6e 20 63 3b 64 2e 6c 28 22 66 69 64 6f 22 2c 21 30 29 3b 76 61 72 20 65 3d 6e 65 77 20 61 2e 50 65 72 66 6f 72 6d 61 6e 63 65 4f 62 73 65 72 76 65 72 28 78 28 61 2c 22 66 69 64 22 2c 66 75 6e 63 74 69 6f 6e 28 66 29 7b 66 3d 66 2e 67 65 74 45 6e 74 72 69 65 73 28 29 5b 30 5d 3b 64 2e 6c 28 22 66 69 64 22 2c 61 2e 4d 61 74 68 2e 72 6f 75 6e 64 28 31 30 30 2a 28 66 2e 70 72 6f 63 65 73 73 69 6e 67 53 74 61 Data Ascii: n(e){e.C(d)}}}),Io=A("fid",function(a){var b,c=C;if(!O(a.PerformanceObserver))return c;var d=L(a);if(d.b("fido"))return c;d.l("fido",!0);var e=new a.PerformanceObserver(x(a,"fid",function(f){f=f.getEntries()[0];d.l("fid",a.Math.round(100*(f.processingSta
2021-10-29 15:51:16 UTC	214	IN	Data Raw: 63 5b 31 5d 2c 65 3d 63 5b 32 5d 2c 66 3d 63 2e 73 6c 69 63 65 28 33 29 3b 63 3d 70 61 72 73 65 49 6e 74 28 63 5b 30 5d 2c 32 29 3b 69 66 28 31 3d 3d 3d 63 29 63 3d 22 41 54 35 54 36 6b 75 30 36 6b 45 73 58 4b 33 69 79 42 52 67 6f 36 6c 6b 38 72 43 74 58 34 4b 6a 66 30 71 70 52 65 37 34 76 74 41 70 6c 4f 6b 6b 70 53 69 38 45 39 46 44 54 42 4a 6c 49 56 36 73 7a 47 75 57 61 77 79 49 4c 72 4c 6c 7a 74 77 6c 34 4b 45 71 73 31 70 4e 46 76 4e 64 74 49 72 59 74 52 4f 42 4e 31 67 53 47 53 31 61 64 70 2b 6d 79 72 7a 6d 5a 4b 6f 71 45 72 74 43 76 32 30 57 79 57 69 52 6c 45 71 5a 51 55 7a 76 56 33 73 52 61 31 6e 53 63 6d 6c 78 70 74 77 4c 4c 59 37 6f 22 3b 65 6c 73 65 20 69 66 28 32 3d 3d 3d 63 29 63 3d 22 43 79 32 46 63 72 65 4c 4a 4c 70 59 58 57 33 42 58 46 4a 71 Data Ascii: c[1],e=c[2],f=c.slice(3);c=parseInt(c[0],2);if(1===c)c="AT5T6ku06kEsXK3iyBRgo6lk8rCtX4Kjf0qpRe74vtAplOkkpSi8E9FDTBJlIV6szGuWawyILrLlztwl4KEqs1pNFvNdtIrYtROBN1gSGS1adp+myrzmZKoqErtCv20WyWiRlEqZQUzvV3sRa1nScmlxptwLLY7o";else if(2===c)c="Cy2FcreLJLpYXW3BXFJq

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49792	88.212.201.198	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:15 UTC	0	OUT	GET /hit;counter1?r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/secondpage.html;0.5443641556055339 HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Connection: Keep-Alive Host: counter.yadro.ru
2021-10-29 15:51:16 UTC	13	IN	HTTP/1.1 302 Moved Temporarily Server: nginx/1.17.9 Date: Fri, 29 Oct 2021 15:51:24 GMT Content-Type: text/html Content-Length: 32 Connection: close Location: https://counter.yadro.ru/hit;counter1?q;r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/secondpage.html;0.5443641556055339 Expires: Wed, 28 Oct 2020 21:00:00 GMT Pragma: no-cache Cache-control: no-cache P3P: policyref="/w3c/p3p.xml", CP="UNI" Set-Cookie: FTID=1XV1Xy3Wb9uB1XV1Xy001Ei9; path=/; expires=Fri, 28 Oct 2022 21:00:00 GMT; HttpOnly; Secure; SameSite=None; domain=.yadro.ru Strict-Transport-Security: max-age=86400
2021-10-29 15:51:16 UTC	13	IN	Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 4d 6f 76 65 64 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body>Moved</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49800	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:21 UTC	272	OUT	GET /watch/14153041/1?callback=_ymjsp355627947&page-url=http%3A%2F%2Fwww.all-bearings.narod.ru%2Ffirstpage.html&charset=utf-8&browser-info=pv%3A1%3Agdpr%3A14%3Avf%3A9ezyymqkmijljhdjn%3Afp%3A1930%3Afu%3A0%3Aen%3Autf-8%3Ala%3Aen-US%3Av%3A680%3Acn%3A1%3Adp%3A0%3Als%3A732524701665%3Ahid%3A87010386%3Az%3A120%3Ai%3A20210102917512O%3Aet%3A1635522680%3Ac%3A1%3Arn%3A244404675%3Au%3A16355226783226226 28%3Aw%3A148x47%3As%3A1280x1024x32%3Aifr%3A1%3Aj%3A1%3Ans%3A1635522674781%3Ads%3A0%2C0%2C0%2C0%2C0%2C%2C155%2C0%2C2520%2C2521%2C0%2C2520%3Aco%3A0%3Arqnl%3A1%3Ast%3A1635522681%3At%3AHTTP%20404%20Resource%20not%20found&t=gdpr%2814%29ti%283%29&wmode=5 HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: mc.yandex.ru Connection: Keep-Alive Cookie: yandexuid=3723159021635522681; i=yROKAQCkQEDp/MhTCtujtSWzFSx7PgG/2QZgPGeQuaYkCYGk4Lr5g33sdF0NzFWf3pPBk9Yj1OF7cHnVzZMM+SWO+Mc=; ymex=1667058681.yrts.1635522681#1667058681.yrtsi.1635522681; yabs-sid=702787781635522681
2021-10-29 15:51:21 UTC	273	IN	HTTP/1.1 200 Ok Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Connection: Close Content-Length: 343 Content-Type: application/javascript Date: Fri, 29 Oct 2021 15:51:21 GMT Expires: Fri, 29-Oct-2021 15:51:21 GMT Last-Modified: Fri, 29-Oct-2021 15:51:21 GMT Pragma: no-cache Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
2021-10-29 15:51:21 UTC	274	IN	Data Raw: 2f 2a 2a 2f 74 72 79 7b 5f 79 6d 6a 73 70 33 35 35 36 32 37 39 34 37 28 7b 22 61 75 74 6f 5f 67 6f 61 6c 73 22 3a 30 2c 22 62 75 74 74 6f 6e 5f 67 6f 61 6c 73 22 3a 30 2c 22 63 5f 72 65 63 70 22 3a 22 31 2e 30 30 30 30 30 22 2c 22 66 6f 72 6d 5f 67 6f 61 6c 73 22 3a 30 2c 22 70 63 73 22 3a 22 31 22 2c 22 77 65 62 76 69 73 6f 72 22 3a 7b 22 61 72 63 68 5f 74 79 70 65 22 3a 22 6e 6f 6e 65 22 2c 22 64 61 74 65 22 3a 22 32 30 32 30 2d 30 39 2d 30 34 20 32 30 3a 33 32 3a 32 31 22 2c 22 66 6f 72 6d 73 22 3a 31 2c 22 72 65 63 70 22 3a 22 31 2e 30 30 30 30 30 22 7d 2c 22 73 62 70 22 3a 20 7b 22 61 22 3a 22 57 70 33 42 63 78 52 52 36 46 46 48 63 78 42 45 79 39 43 33 36 5a 7a 76 49 70 51 55 54 41 39 68 68 4f 68 75 44 70 42 46 30 6b 5a 37 45 2f 4e 73 6d 53 62 5a 54 Data Ascii: /**/try{_ymjsp355627947({"auto_goals":0,"button_goals":0,"c_recp":"1.00000","form_goals":0,"pcs":"1","webvisor":{"arch_type":"none","date":"2020-09-04 20:32:21","forms":1,"recp":"1.00000"},"sbp": {"a":"Wp3BcxRR6FFHcxBEy9C36ZzvlpQUTA9hhOhuDpBF0kZ7E/NsmSbZT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49801	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:21 UTC	274	OUT	GET /metrika/advert.gif?t=ti(4) HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: mc.yandex.ru Connection: Keep-Alive
2021-10-29 15:51:21 UTC	275	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Cache-Control: max-age=3600 Connection: Close Content-Length: 43 Content-Type: image/gif Date: Fri, 29 Oct 2021 15:51:21 GMT ETag: "617677e6-2b" Expires: Fri, 29 Oct 2021 16:51:21 GMT Last-Modified: Mon, 25 Oct 2021 12:24:54 GMT Strict-Transport-Security: max-age=31536000
2021-10-29 15:51:21 UTC	275	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 00 00 00 00 00 00 00 00 21 f9 04 01 00 00 00 00 2c 00 00 00 00 01 00 01 00 00 02 02 44 01 00 3b Data Ascii: GIF89a!,D;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49791	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:15 UTC	0	OUT	GET /metrika/watch.js HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Connection: Keep-Alive Host: mc.yandex.ru
2021-10-29 15:51:16 UTC	8	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Cache-Control: max-age=3600 Connection: Close Content-Length: 132911 Content-Type: application/javascript Date: Fri, 29 Oct 2021 15:51:16 GMT ETag: "617677e6-2072f" Expires: Fri, 29 Oct 2021 16:51:16 GMT Last-Modified: Mon, 25 Oct 2021 12:24:54 GMT Strict-Transport-Security: max-age=31536000
2021-10-29 15:51:16 UTC	8	IN	Data Raw: ef bb bf 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 28 66 75 6e 63 74 69 6f 6e 28 4a 63 29 7b 66 75 6e 63 74 69 6f 6e 20 48 69 28 61 29 7b 72 65 74 75 72 6e 20 61 2e 72 65 70 6c 61 63 65 28 49 69 2c 66 75 6e 63 74 69 6f 6e 28 62 2c 63 2c 64 2c 65 29 7b 72 65 74 75 72 6e 22 22 2b 63 2b 65 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 4b 63 28 61 2c 62 29 7b 69 66 28 21 62 29 72 65 74 75 72 6e 21 31 3b 76 61 72 20 63 3d 4d 28 61 29 3b 72 65 74 75 72 6e 28 6e 65 77 20 52 65 67 45 78 70 28 62 29 29 2e 74 65 73 74 28 22 22 2b 63 2e 70 61 74 68 6e 61 6d 65 2b 63 2e 68 61 73 68 2b 63 2e 73 65 61 72 63 68 29 7d 66 75 6e 63 74 69 6f 6e 20 4a 69 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 44 61 28 61 2c 62 2c 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d 6e 28 63 2c Data Ascii: (function(){try{(function(Jc){function Hi(a){return a.replace(Ii,function(b,c,d,e){return""+c+e})}function Kc(a,b){if(!b)return!1;var c=M(a);return(new RegExp(b)).test(""+c.pathname+c.hash+c.search)}function Ji(a,b){return Da(a,b,function(c){var d=n(c,
2021-10-29 15:51:16 UTC	46	IN	Data Raw: 6b 20 61 7d 7d 63 61 74 63 68 28 48 29 7b 7d 79 3d 7b 7d 7d 49 64 28 64 2c 79 29 3b 69 66 28 21 63 2e 67 65 74 53 68 61 64 65 72 50 72 65 63 69 73 69 6f 6e 46 6f 72 6d 61 74 29 72 65 74 75 72 6e 20 42 28 22 7e 22 2c 64 29 3b 49 64 28 64 2c 66 6a 28 63 29 29 3b 72 65 74 75 72 6e 20 42 28 22 7e 22 2c 64 29 7d 66 75 6e 63 74 69 6f 6e 20 49 64 28 61 2c 62 2c 63 29 7b 76 6f 69 64 20 30 3d 3d 3d 63 26 26 28 63 3d 22 3a 22 29 3b 44 28 66 75 6e 63 74 69 6f 6e 28 64 29 7b 72 65 74 75 72 6e 20 61 2e 70 75 73 68 28 22 22 2b 0a 64 5b 30 5d 2b 63 2b 64 5b 31 5d 29 7d 2c 4e 61 28 62 29 29 7d 66 75 6e 63 74 69 6f 6e 20 67 6a 28 61 29 7b 76 61 72 20 62 3d 68 6a 28 61 29 3b 72 65 74 75 72 6e 20 62 3f 53 28 66 75 6e 63 74 69 6f 6e 28 63 2c 64 2c 65 29 7b 64 3d 22 22 2b 28 Data Ascii: k a}}catch(H){}y={}}ld(d,y);if(!c.getShaderPrecisionFormat)return B("~",d);ld(d,fj(c));return B("~",d)}function ld(a,b,c){void 0===c&&(c=":");D(function(d){return a.push(""+d[0]+c+d[1])},Na(b))}function gj(a){var b=hj(a);return b?S(function(c,d,e){d=""+(
2021-10-29 15:51:16 UTC	54	IN	Data Raw: 65 74 75 72 6e 20 63 7d 2c 7b 7d 2c 61 29 3b 72 65 74 75 72 6e 20 79 61 28 61 29 2e 6c 65 6e 67 74 68 3f 61 3a 76 6f 69 64 20 30 7d 66 75 6e 63 74 69 6f 6e 20 47 6a 28 61 2c 62 2c 63 29 7b 76 61 72 20 64 3d 21 31 2c 65 3d 22 22 3b 69 66 28 21 69 63 28 62 29 29 72 65 74 75 72 6e 20 4c 62 28 63 2c 22 45 63 6f 6d 6d 65 72 63 65 20 64 61 74 61 20 73 68 6f 75 6c 64 20 62 65 20 61 6e 20 6f 62 6a 65 63 74 22 29 2c 64 3b 76 61 72 20 66 3d 62 2e 67 6f 6f 64 73 3b 0a 73 77 69 74 63 68 28 61 29 7b 63 61 73 65 20 22 64 65 74 61 69 6c 22 3a 63 61 73 65 20 22 61 64 64 22 3a 63 61 73 65 20 22 72 65 6d 6f 76 65 22 3a 49 61 28 66 29 26 26 66 2e 6c 65 6e 67 74 68 3f 28 64 3d 52 64 28 66 75 6e 63 74 69 6f 6e 28 67 29 7b 72 65 74 75 72 6e 20 69 63 28 67 29 26 26 28 56 61 28 Data Ascii: eturn c},{},a);return ya(a).length?a:void 0}function Gj(a,b,c){var d=!1,e="";if(!ic(b))return Lb(c,"Ecommerce data should be an object"),d;var f=b.goods;switch(a){case "detail":case "add":case "remove":Ia(f)&&f.length?(d=Rd(function(g){return ic(g)&&(Va(
2021-10-29 15:51:16 UTC	62	IN	Data Raw: 52 41 59 5f 42 55 46 46 45 52 2c 64 2c 62 2e 53 54 41 54 49 43 5f 44 52 41 57 29 3b 63 2e 45 63 3d 33 3b 63 2e 4b 63 3d 33 3b 64 3d 62 2e 63 72 65 61 74 65 50 72 6f 67 72 61 6d 28 29 3b 76 61 72 20 65 3d 62 2e 63 72 65 61 74 65 53 68 61 64 65 72 28 62 2e 56 45 52 54 45 58 5f 53 48 41 44 45 52 29 3b 69 66 28 21 64 7c 7c 21 65 29 72 65 74 75 72 6e 22 22 3b 62 2e 73 68 61 64 65 72 53 6f 75 72 63 65 28 65 2c 22 61 74 74 72 69 62 75 74 65 20 76 65 63 32 20 61 74 74 72 56 65 72 74 65 78 3b 76 61 72 79 69 6e 67 20 76 65 63 32 20 76 61 72 79 69 6e 54 65 78 43 6f 6f 72 64 69 6e 61 74 65 3b 75 6e 69 66 6f 72 6d 20 76 65 63 32 20 75 6e 69 66 6f 72 6d 4f 66 66 73 65 74 3b 76 6f 69 64 20 6d 61 69 6e 28 29 7b 76 61 72 79 69 6e 54 65 78 43 6f 6f 72 64 69 6e 61 74 65 3d Data Ascii: RAY_BUFFER,d,b.STATIC_DRAW);c.Ec=3;c.Kc=3;d=b.createProgram();var e=b.createShader(b.VERTEX_SHADER);if(!d||!e)return"";b.shaderSource(e,"attribute vec2 attrVertex;varying vec2 varyinTexCoordinate;uniform vec2 uniformOffset;void main(){varyinTexCoordinate=
2021-10-29 15:51:16 UTC	70	IN	Data Raw: 20 4a 28 66 75 6e 63 74 69 6f 6e 28 6c 2c 6d 29 7b 63 2e 5a 61 28 68 2c 6b 2c 66 75 6e 63 74 69 6f 6e 28 70 2c 75 29 7b 6c 28 5b 70 2c 75 5d 29 7d 29 3b 70 61 28 61 2c 76 28 6a 62 28 29 2c 6d 29 2c 35 31 30 30 2c 22 69 73 2e 6f 22 29 7d 29 7d 2c 4b 62 3a 66 75 6e 63 74 69 6f 6e 28 68 29 7b 76 61 72 20 6b 3d 7b 4d 62 3a 5b 5d 2c 68 62 3a 5b 5d 2c 64 61 74 61 3a 68 7d 3b 64 2e 70 75 73 68 28 6b 29 3b 72 65 74 75 72 6e 20 66 28 63 2e 66 61 2c 6b 2c 68 29 7d 2c 4c 62 3a 66 75 6e 63 74 69 6f 6e 28 68 29 7b 76 61 72 20 6b 3d 7b 4d 62 3a 5b 5d 2c 68 62 3a 5b 5d 2c 64 61 74 61 3a 68 7d 3b 65 2e 70 75 73 68 28 6b 29 3b 72 65 74 75 72 6e 20 66 28 63 2e 6a 61 2c 6b 2c 68 29 7d 7d 7d 66 75 6e 63 74 69 6f 6e 20 67 65 28 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 Data Ascii: J(function(l,m){c.Za(h,k,function(p,u){l([p,u])});pa(a,v(jb(),m),5100,"is.o")})},Kb:function(h){var k={Mb:[],hb:[],data:h};d.push(k);return f(c.fa,k,h)},Lb:function(h){var k={Mb:[],hb:[],data:h};e.push(k);return f(c.ja,k,h)}}}function ge(){return functio
2021-10-29 15:51:16 UTC	126	IN	Data Raw: 69 6f 6e 28 6b 29 7b 65 2e 53 63 3d 6b 2e 44 61 3b 72 65 74 75 72 6e 20 6e 65 28 61 2c 63 2c 65 29 2e 74 68 65 6e 28 76 28 6b 2e 44 61 2c 4b 29 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 72 6c 28 61 29 7b 76 61 72 20 62 3d 22 6d 63 2e 79 61 6e 64 65 78 2e 72 75 22 2c 63 3d 6e 28 61 2c 22 64 6f 63 75 6d 65 6e 74 2e 72 65 66 65 72 72 65 72 22 29 3b 69 66 28 21 63 29 72 65 74 75 72 6e 20 62 3b 28 61 3d 59 64 28 61 2c 63 29 2e 68 6f 73 74 2e 6d 61 74 63 68 28 2f 28 3f 3a 5e 7c 5c 2e 29 28 3f 3a 79 61 7c 79 61 6e 64 65 78 29 5c 2e 28 3f 3a 5c 77 2b 7c 63 6f 6d 3f 5c 2e 5c 77 2b 29 24 2f 29 29 3f 28 61 3d 61 5b 30 5d 2e 73 70 6c 69 74 28 22 79 61 6e 64 65 78 22 29 2e 72 65 76 65 72 73 65 28 29 5b 30 5d 2e 73 75 62 73 74 72 69 6e 67 28 31 29 2c 61 3d 4e 28 61 2c Data Ascii: ion(k){e.Sc=k.Da;return ne(a,c,e).then(v(k.Da,K))}}}function rl(a){var b="mc.yandex.ru",c=n(a,"document.referrer");if(!c)return b;(a=Yd(a,c).host.match(/(?:^|\.)(?:ya|yandex)\.(?:\w+|com?\.\w+)$/))?(a=a[0].split("yandex").reverse()[0].substring(1),a=N(a,

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:16 UTC	134	IN	Data Raw: 6c 3b 67 20 69 6e 20 65 68 3f 68 3d 62 2e 67 65 74 41 74 74 72 69 62 75 74 65 26 26 62 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 65 68 5b 67 5d 29 3a 67 20 69 6e 20 55 62 26 26 28 68 3d 22 70 22 3d 3d 3d 67 3f 55 62 5b 67 5d 28 61 2c 62 2c 65 29 3a 22 63 22 3d 3d 3d 67 3f 55 62 5b 67 5d 28 61 2c 62 2c 64 29 3a 55 62 5b 67 5d 28 61 2c 62 29 29 3b 68 26 26 28 68 3d 68 2e 73 6c 69 63 65 28 30 2c 66 68 5b 67 5d 7c 7c 31 30 30 29 2c 66 5b 67 5d 3d 79 65 5b 67 5d 3f 22 22 2b 73 63 28 68 29 3a 68 29 3b 72 65 74 75 72 6e 20 66 7d 2c 7b 7d 2c 63 29 7d 66 75 6e 63 74 69 6f 6e 20 50 66 28 61 2c 62 2c 63 29 7b 69 66 28 61 2e 64 6f 63 75 6d 65 6e 74 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 41 6c 6c 26 26 0a 6b 61 28 22 71 75 65 72 79 53 65 6c 65 63 74 6f 72 41 6c 6c 26 26 0a 6b 61 28 22 71 75 65 72 79 53 65 6c 65 63 74 6f 72 41 6c 6c Data Ascii: l;g in eh?h=b.getAttribute&&b.getAttribute(eh[g]):g in Ub&&(h="p"===g?Ub[g](a,b,e):"c"===g?Ub[g](a,b,d):Ub[g](a,b));h&&(h=h.slice(0,fh[g]||100),f[g]=ye[g]?""+sc(h):h);return f},{},c)}function Pf(a,b,c){if(a.document.querySelectorAll&&ka("querySelectorAll
2021-10-29 15:51:16 UTC	142	IN	Data Raw: 63 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 63 3d 6e 61 28 61 72 67 75 6d 65 6e 74 73 29 2c 64 3d 63 5b 30 5d 3b 63 3d 63 2e 73 6c 69 63 65 28 31 29 3b 76 61 72 20 65 3d 4c 28 64 29 2c 66 3d 65 2e 62 28 22 6d 36 38 30 22 2c 7b 7d 29 2c 67 3d 6e 28 66 2c 61 29 3b 67 7c 7c 28 67 3d 74 28 62 29 2c 66 5b 61 5d 3d 67 2c 65 2e 6c 28 22 6d 36 38 30 22 2c 66 29 29 3b 72 65 74 75 72 6e 20 67 2e 61 70 70 6c 79 28 76 6f 69 64 20 30 2c 50 28 5b 64 5d 2c 63 29 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 7a 61 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 62 3f 61 28 62 29 3a 61 28 29 7d 66 75 6e 63 74 69 6f 6e 20 74 28 61 2c 62 29 7b 76 61 72 20 63 3d 5b 5d 2c 64 3d 5b 5d 3b 76 61 72 20 65 3d 62 3f 62 3a 4b 3b 72 65 74 75 72 6e 20 66 75 6e Data Ascii: c(a,b){return function(){var c=na(arguments),d=c[0];c=c.slice(1);var e=L(d),f=e.b("m680",{}),g=n(f,a);g||(g=t(b),f[a]=g,e.l("m680",f));return g.apply(void 0,P([d],c))}}function za(a,b){return b?a(b):a()}function t(a,b){var c=[],d=[];var e=b?b:K;return fun
2021-10-29 15:51:16 UTC	150	IN	Data Raw: 2d 62 5d 3b 62 2d 3d 33 32 3b 72 65 74 75 72 6e 5b 61 5b 31 5d 3c 3c 62 7c 61 5b 30 5d 3e 3e 3e 33 32 2d 62 2c 61 5b 30 5d 3c 3c 62 7c 61 5b 31 5d 3e 3e 3e 33 32 2d 62 5d 7d 66 75 6e 63 74 69 6f 6e 20 4d 61 28 61 2c 62 29 7b 62 25 3d 36 34 3b 72 65 74 75 72 6e 20 30 3d 3d 3d 62 3f 61 3a 33 32 3e 62 3f 5b 61 5b 30 5d 3c 3c 62 7c 61 5b 31 5d 3e 3e 3e 33 32 2d 62 2c 61 5b 31 5d 3c 3c 62 5d 3a 5b 61 5b 31 5d 3c 3c 62 2d 33 32 2c 30 5d 7d 66 75 6e 63 74 69 6f 6e 20 59 28 61 2c 62 29 7b 72 65 74 75 72 6e 5b 61 5b 30 5d 5e 62 5b 30 5d 2c 61 5b 31 5d 5e 62 5b 31 5d 5d 7d 66 75 6e 63 74 69 6f 6e 20 44 68 28 61 29 7b 61 3d 59 28 61 2c 5b 30 2c 61 5b 30 5d 3e 3e 3e 31 5d 29 3b 61 3d 50 61 28 61 2c 5b 34 32 38 33 35 34 33 35 31 31 2c 33 39 38 31 38 30 36 37 39 37 5d Data Ascii: -b];b-=32;return[a[1]<<b|a[0]>>>32-b,a[0]<<b|a[1]>>>32-b]}function Ma(a,b){b%=64;return 0===b?a:32>b?[a[0]<<b|a[1]>>>32-b,a[1]<<b]:[a[1]<<b-32,0]}function Y(a,b){return[a[0]^b[0],a[1]^b[1]]}function Dh(a){a=Y(a,[0,a[0]>>>1]);a=Pa(a,[4283543511,3981806797]
2021-10-29 15:51:16 UTC	158	IN	Data Raw: 72 65 74 75 72 6e 20 50 28 65 63 28 61 29 2c 4c 6d 28 61 29 7c 7c 5b 5d 29 7d 66 75 6e 63 74 69 6f 6e 20 4e 68 28 61 29 7b 72 65 74 75 72 6e 28 61 2e 73 68 69 66 74 4b 65 79 3f 32 3a 30 29 7c 28 61 2e 63 74 72 6c 4b 65 79 3f 34 3a 30 29 7c 28 61 2e 61 6c 74 4b 65 79 3f 31 3a 30 29 7c 28 61 2e 6d 65 74 61 4b 65 79 3f 38 3a 30 29 7c 28 61 2e 63 74 72 6c 4b 65 79 7c 7c 61 2e 61 6c 74 4b 65 79 3f 31 36 3a 30 29 7d 66 75 6e 63 74 69 6f 6e 20 4f 68 28 61 29 7b 76 61 72 20 62 3d 5b 5d 3b 4d 65 7c 7c 28 4d 65 3d 21 30 2c 4c 65 26 26 62 2e 70 75 73 68 2e 61 70 70 6c 79 28 62 2c 44 6d 28 61 2e 6f 2c 74 61 28 61 2e 6f 29 29 29 2c 0a 49 62 28 61 2e 6f 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 4d 65 3d 21 31 7d 2c 22 66 76 2e 63 22 29 29 3b 72 65 74 75 72 6e 20 62 7d 66 75 Data Ascii: return P(ec(a),Lm(a)||[])}function Nh(a){return(a.shiftKey?2:0)|(a.ctrlKey?4:0)|(a.altKey?1:0)|(a.metaKey?8:0)|(a.ctrlKey||a.altKey?16:0)}function Oh(a){var b=[];Me||(Me=!0,Le&&b.push.apply(b,Dm(a.o,ta(a.o))),Ib(a.o,function(){Me=!1},"fv.c"));return b}fu
2021-10-29 15:51:16 UTC	166	IN	Data Raw: 2e 65 78 70 3d 22 65 78 70 65 72 69 6d 65 6e 74 73 22 3b 77 61 2e 4f 61 3d 22 65 63 6f 6d 6d 65 72 63 65 22 3b 46 62 2e 4f 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 69 66 28 61 29 72 65 74 75 72 6e 21 30 3d 3d 3d 61 3f 22 64 61 74 61 4c 61 79 65 72 22 3a 22 22 2b 61 7d 3b 77 61 2e 48 3d 22 70 61 72 61 6d 73 22 3b 77 61 2e 49 61 3d 22 75 73 65 72 50 61 72 61 6d 73 22 3b 77 61 2e 73 61 3d 22 61 63 63 75 72 61 74 65 54 72 61 63 6b 42 6f 75 6e 63 65 22 3b 77 61 2e 55 62 3d 22 74 72 69 67 67 65 72 45 76 65 6e 74 22 3b 46 62 2e 55 62 3d 42 6f 6f 6c 65 61 6e 3b 77 61 2e 4a 62 3d 22 73 65 6e 64 54 69 74 6c 65 22 3b 46 62 2e 4a 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 21 21 61 7c 7c 56 28 61 29 7d 3b 77 61 2e 67 62 3d 22 74 72 61 63 6b 48 61 73 Data Ascii: .exp="experiments";wa.Oa="ecommerce";Fb.Oa=function(a){if(a)return!0===a?"dataLayer":""+a};wa.H="params";wa.Ia="userParams";wa.sa="accurateTrackBounce";wa.Ub="triggerEvent";Fb.Ub=Boolean;wa.Jb="sendTitle";Fb.Jb=function(a){return!!a||V(a)};wa.gb="trackHas
2021-10-29 15:51:16 UTC	218	IN	Data Raw: 28 63 2c 64 2c 65 29 7b 65 2b 3d 31 3b 32 3c 3d 65 26 26 21 63 26 26 28 65 3d 42 28 22 2e 22 2c 62 2e 73 6c 69 63 65 28 2d 65 29 29 2c 4e 66 28 61 2c 65 29 26 26 28 63 3d 0a 65 29 29 3b 72 65 74 75 72 6e 20 63 7d 2c 22 22 2c 62 29 7d 29 2c 78 62 3d 74 28 66 6f 6e 28 61 29 7b 5a 67 28 61 2c 22 5f 79 6d 42 52 43 22 2c 22 31 22 29 3b 76 61 72 20 62 3d 22 31 22 21 3d 3d 59 67 28 61 2c 22 5f 79 6d 42 52 43 22 29 3b 62 7c 7c 24 67 28 61 2c 22 5f 79 6d 42 52 43 22 29 3b 72 65 74 75 72 6e 20 62 7d 29 2c 41 61 3d 74 28 58 67 29 2c 74 64 3d 74 28 58 67 2c 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 72 65 74 75 72 6e 22 22 2b 62 2b 63 7d 29 2c 57 3d 74 28 44 67 29 2c 56 67 3d 79 63 28 22 72 22 2c 66 75 6e 63 74 69 6f 6e Data Ascii: (c,d,e){e+=1;2<=e&&!c&&(e=B(".",b.slice(-e)),Nf(a,e)&&(c=e));return c},"",b)}),xb=t(fc),Cl=t(function(a){Zg(a,"_ymBRC","1");var b="1"!==Yg(a,"_ymBRC");b||$g(a,"_ymBRC");return b}),Aa=t(Xg),td=t(Xg,function(a,b,c){return""+b+c}),W=t(Dg),Vg=yc("r",function
2021-10-29 15:51:16 UTC	225	IN	Data Raw: 74 69 6f 6e 22 2c 22 6d 6f 7a 52 54 43 50 65 65 72 43 6f 6e 6e 65 63 74 69 6f 6e 22 2c 22 77 65 62 6b 69 74 52 54 43 50 65 65 72 43 6f 6e 6e 65 63 74 69 6f 6e 22 5d 2c 59 63 3d 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 7b 6a 61 3a 7b 7d 2c 70 65 6e 64 69 6e 67 3a 7b 7d 2c 66 61 3a 7b 7d 7d 7d 29 2c 52 65 3d 54 28 22 70 6f 73 74 4d 65 73 73 61 67 65 22 29 2c 4c 6e 3d 61 61 28 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 29 7b 76 61 72 20 65 2c 66 3d 7b 76 61 3a 57 28 61 29 28 55 29 2c 6b 65 79 3a 61 2e 4d 61 74 68 2e 72 61 6e 64 6f 6d 28 29 2c 64 69 72 3a 30 7d 3b 63 2e 6c 65 6e 67 74 68 26 26 28 66 2e 76 61 3d 70 61 72 73 65 49 6e 74 28 63 5b 30 5d 2c 31 30 29 2c 66 2e 6b 65 79 3d 70 61 72 73 65 46 6c 6f 61 74 28 63 5b 31 5d 29 2c 66 2e Data Ascii: tion","mozRTCPeerConnection","webkitRTCPeerConnection"],Yc=t(function(){return{ja:{},pending:{},fa:{}}}),Re=T("postMessage"),Ln=aa(function(a,b,c,d){var e,f={va:W(a)(U),key:a.Math.random(),dir:0};c.length&&(f.va=parseInt(c[0],10),f.key=parseFloat(c[1]),f.
2021-10-29 15:51:16 UTC	233	IN	Data Raw: 3b 63 3d 45 6b 28 61 2c 62 2c 63 29 3b 76 61 72 20 65 3d 62 61 5b 62 5d 2c 66 3d 65 3f 65 28 61 2c 64 2c 63 29 3a 43 61 28 61 2c 64 2c 63 29 3b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 67 3d 6e 61 28 61 72 67 75 6d 65 6e 74 73 29 2c 68 3d 67 2e 73 6c 69 63 65 28 31 29 3b 67 3d 46 28 67 5b 30 5d 2c 7b 57 3a 5b 62 5d 7d 29 3b 72 65 74 75 72 6e 20 66 2e 61 70 70 6c 79 28 76 6f 69 64 20 30 2c 50 28 5b 67 5d 2c 68 29 29 7d 7d 2c 75 69 29 2c 68 67 3d 74 28 71 28 54 28 22 69 64 22 29 2c 6d 62 28 5b 32 36 38 31 32 36 35 33 5d 29 29 2c 51 29 2c 57 6e 3d 41 28 22 64 63 2e 69 6e 69 74 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 62 3d 4d 28 61 29 2c 63 3d 45 63 28 61 29 2c 64 3d 78 62 28 61 29 2c 65 3d 69 67 28 61 29 2c 66 3d 65. Data Ascii: ;c=Ek(a,b,c);var e=ba[b],f=e?e(a,d,c):Ca(a,d,c);return function(){var g=na(arguments),h=g.slice(1);g=F(g[0],{W:[b]});return f.apply(void 0,P([g],h))}},ui),hg=t(q(T("id"),mb([26812653])),Q),Wn=A("dc.init",function(a){var b=M(a),c=Ec(a),d=xb(a),e=ig(a),f=e.

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:16 UTC	241	IN	Data Raw: 75 6c 6c 3b 64 3d 78 28 61 2c 22 63 6c 6d 2e 70 2e 63 22 2c 66 75 6e 63 74 69 6f 6e 28 6c 29 7b 76 61 72 20 6d 3d 67 28 29 3b 69 66 28 6d 29 7b 76 61 72 20 70 3d 22 6f 62 6a 65 63 74 22 3d 3d 3d 74 79 70 65 6f 66 20 6d 3f 6d 3a 7b 7d 2c 75 3d 70 2e 66 69 6c 74 65 72 3b 0a 6d 3d 70 2e 69 73 54 72 61 63 6b 48 61 73 68 7c 7c 21 31 3b 76 61 72 20 72 3d 49 28 66 75 6e 63 74 69 6f 6e 28 79 29 7b 72 65 74 75 72 6e 28 22 22 2b 79 29 2e 74 6f 55 70 70 65 72 43 61 73 65 28 29 7d 2c 70 2e 69 67 6e 6f 72 65 54 61 67 73 7c 7c 5b 5d 29 3b 56 28 68 29 26 26 28 68 3d 70 2e 71 75 6f 74 61 7c 7c 6e 75 6c 6c 29 3b 76 61 72 20 77 3d 21 21 70 2e 71 75 6f 74 61 3b 6c 3d 7b 65 6c 65 6d 65 6e 74 3a 63 6b 28 61 2c 6c 29 2c 70 6f 73 69 74 69 6f 6e 3a 4d 63 28 61 2c 6c 29 2c 62 75 Data Ascii: ull;d=x(a,"clm.p.c",function(l){var m=g();if(m){var p="object"===typeof m?m:{},u=p.filter;m=p.isTrackHash||!1;var r=I(function(y){return(""+y).toUpperCase()},p.ignoreTags||[]);V(h)&&(h=p.quota||null);var w=!!p.quota;l={element:ck(a,l),position:Mc(a,l),bu
2021-10-29 15:51:16 UTC	249	IN	Data Raw: 22 5f 5f 79 6d 22 2c 6d 29 26 26 6c 3b 6d 3d 21 68 67 28 62 29 3b 6c 3d 6c 62 28 61 2c 62 2c 75 3f 22 53 65 74 20 75 73 65 72 20 69 64 20 22 2b 6c 3a 28 70 3f 22 55 73 65 72 20 70 22 3a 22 50 22 29 2b 22 61 72 61 6d 73 2e 20 43 6f 75 6e 74 65 72 20 22 2b 62 2e 69 64 2c 75 3f 76 6f 69 64 20 30 3a 4a 53 4f 4e 2e 73 74 72 69 6e 67 69 66 79 28 66 29 29 3b 68 28 7b 48 3a 66 2c 46 3a 68 61 28 28 63 3d 7b 7d 2c 63 2e 70 61 3d 31 2c 63 2e 61 72 3d 0a 31 2c 63 29 29 2c 44 3a 28 64 3d 7b 7d 2c 64 5b 22 70 61 67 65 2d 75 72 6c 22 5d 3d 6b 7c 7c 4d 28 61 29 2e 68 72 65 66 2c 64 29 7d 2c 62 29 2e 74 68 65 6e 28 6d 3f 6c 3a 43 29 5b 22 63 61 74 63 68 22 5d 28 78 28 61 2c 22 70 2e 73 22 29 29 2e 74 68 65 6e 28 45 28 6f 62 2c 6e 75 6c 6c 2c 61 2c 67 2c 65 29 29 7d 7d 29 Data Ascii: "__ym",m)&&l;m=!hg(b);l=lb(a,b,u?"Set user id "+l:(p?"User p":"P")+"arams. Counter "+b.id,u?void 0:JSON.stringify(f));h({H:f,F:ha((c={},c.pa=1,c.ar=1,c)),D:(d={},d["page-url"]=k||M(a).href,d)},b).then(m?l:C)["catch"](x(a,"p.s")).then(E(ob,null,a,g,e))}})
2021-10-29 15:51:16 UTC	257	IN	Data Raw: 69 73 4e 61 4e 28 63 29 3f 63 3d 30 3a 28 63 3d 4d 61 74 68 2e 6d 69 6e 28 63 2c 64 29 2c 63 3d 4d 61 74 68 2e 6d 61 78 28 63 2c 30 29 29 3b 72 65 74 75 72 6e 20 63 7d 29 2c 6d 70 3d 5b 5b 5b 22 45 55 52 22 2c 22 5c 75 32 30 61 63 22 5d 2c 0a 22 39 37 38 22 5d 2c 5b 5b 22 55 53 44 22 2c 22 5c 75 30 34 32 33 5c 5c 2e 5c 75 30 34 31 35 5c 5c 2e 22 2c 22 5c 5c 24 22 5d 2c 22 38 34 30 22 5d 2c 5b 5b 22 55 41 48 22 2c 22 5c 75 30 34 31 33 5c 75 30 34 32 30 5c 75 30 34 31 64 22 2c 22 5c 75 32 30 62 34 22 5d 2c 22 39 38 30 22 5d 2c 5b 22 5c 75 30 34 32 32 5c 75 30 34 31 33 20 4b 5a 54 20 5c 75 32 30 62 38 20 5c 75 30 34 32 32 5c 75 30 34 61 32 5c 75 30 34 31 33 20 54 45 4e 47 45 20 5c 75 30 34 32 32 5c 75 30 34 31 35 5c 75 30 34 31 64 5c 75 30 34 31 33 5c 75 30 Data Ascii: isNaN(c)?c=0:(c=Math.min(c,d),c=Math.max(c,0));return c}),mp=[[["EUR","\u20ac"],"978"],[["USD","\u0423\\.\u0415\\.","\\$"],"840"],[["UAH","\u0413\u0420\u041d","\u20b4"],"980"],["\u0422\u0413 KZT \u20b8 \u0422\u04a2\u0413 TENGE \u0422\u0415\u041d\u0413\u0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49793	88.212.201.198	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:15 UTC	1	OUT	GET /hit;counter1?r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/firstpage.html;0.34476715437082456 HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Connection: Keep-Alive Host: counter.yadro.ru
2021-10-29 15:51:16 UTC	14	IN	HTTP/1.1 302 Moved Temporarily Server: nginx/1.17.9 Date: Fri, 29 Oct 2021 15:51:24 GMT Content-Type: text/html Content-Length: 32 Connection: close Location: https://counter.yadro.ru/hit;counter1?q;r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/firstpage.html;0.34476715437082456 Expires: Wed, 28 Oct 2020 21:00:00 GMT Pragma: no-cache Cache-control: no-cache P3P: policyref="/w3c/p3p.xml", CP="UNI" Set-Cookie: FTID=1XV1Xy3Wb9uB1XV1Xy001EiW; path=/; expires=Fri, 28 Oct 2022 21:00:00 GMT; HttpOnly; Secure; SameSite=None; domain=.yadro.ru Strict-Transport-Security: max-age=86400
2021-10-29 15:51:16 UTC	14	IN	Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 4d 6f 76 65 64 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body>Moved</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49795	88.212.201.198	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:16 UTC	263	OUT	GET /hit;counter1?q;r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/firstpage.html;0.34476715437082456 HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Connection: Keep-Alive Host: counter.yadro.ru Cookie: FTID=1XV1Xy3Wb9uB1XV1Xy001EiW

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:16 UTC	264	IN	HTTP/1.1 200 OK Server: nginx/1.17.9 Date: Fri, 29 Oct 2021 15:51:24 GMT Content-Type: image/gif Content-Length: 43 Connection: close Expires: Wed, 28 Oct 2020 21:00:00 GMT Pragma: no-cache Cache-control: no-cache P3P: policyref="/w3c/p3p.xml", CP="UNI" Set-Cookie: VID=27k9Bf33T4OB1XV1Xy001PnT; path=/; expires=Fri, 28 Oct 2022 21:00:00 GMT; HttpOnly; Secure; SameSite=None; domain=.yadro.ru Access-Control-Allow-Origin: * Strict-Transport-Security: max-age=86400
2021-10-29 15:51:16 UTC	265	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 ff 00 c0 c0 c0 00 00 00 21 f9 04 01 00 00 00 00 2c 00 00 00 00 01 00 01 00 00 02 02 44 01 00 3b Data Ascii: GIF89a!,D;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49794	88.212.201.198	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:16 UTC	263	OUT	GET /hit;counter1?q;r;s1280*1024*32;uhttp%3A//www.all-bearings.narod.ru/secondpage.html;0.5443641556055339 HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Connection: Keep-Alive Host: counter.yadro.ru Cookie: FTID=1XV1Xy3Wb9uB1XV1Xy001Ei9
2021-10-29 15:51:16 UTC	264	IN	HTTP/1.1 200 OK Server: nginx/1.17.9 Date: Fri, 29 Oct 2021 15:51:24 GMT Content-Type: image/gif Content-Length: 43 Connection: close Expires: Wed, 28 Oct 2020 21:00:00 GMT Pragma: no-cache Cache-control: no-cache P3P: policyref="/w3c/p3p.xml", CP="UNI" Set-Cookie: VID=27k78t1mnSOB1XV1Xy001Exq; path=/; expires=Fri, 28 Oct 2022 21:00:00 GMT; HttpOnly; Secure; SameSite=None; domain=.yadro.ru Access-Control-Allow-Origin: * Strict-Transport-Security: max-age=86400
2021-10-29 15:51:16 UTC	264	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 ff 00 c0 c0 c0 00 00 00 21 f9 04 01 00 00 00 00 2c 00 00 00 00 01 00 01 00 00 02 02 44 01 00 3b Data Ascii: GIF89a!,D;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49796	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:20 UTC	265	OUT	GET /watch/14153041?callback=_ymjsp303195921&page-url=http%3A%2F%2Fwww.all-bearings.narod.ru%2Fsecondpage.html&charset=utf-8&browser-info=pv%3A1%3Agdpr%3A14%3Avf%3A9ezyymqkmijljhdjn%3Afp%3A1976%3Afu%3A0%3Aen%3Autf-8%3Ala%3Aen-US%3Av%3A680%3Acn%3A1%3Adp%3A0%3Als%3A1156845228070%3Ahid%3A271984739%3Az%3A120%3Ai%3A20210102917511 8%3Aet%3A1635522678%3Ac%3A1%3Arn%3A1015963535%3Au%3A16355226783226226 28%3Aw%3A148x55%3As%3A1280x1024x32%3Aifr%3A1%3Aj%3A1%3Ans%3A1635522674734%3Ads%3A0%2C0%2C0%2C0%2C0%2C%2C128%2C0%2C1973%2C1975%2C0%2C1973%3Aco%3A0%3Arqnl%3A1%3Ast%3A1635522680%3At%3AHTTP%20404%20Resource%20not%20found&t=gdpr(14)ti(3)&wmode=5 HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: mc.yandex.ru Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:21 UTC	266	IN	HTTP/1.1 302 Moved temporarily Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Connection: Close Date: Fri, 29 Oct 2021 15:51:20 GMT Expires: Fri, 29-Oct-2021 15:51:20 GMT Last-Modified: Fri, 29-Oct-2021 15:51:20 GMT Location: /watch/14153041/1?callback=_ymjsp303195921&page-url=http%3A%2F%2Fwww.all-bearings.narod.ru%2Fsecondpage.html&charset=utf-8&browser-info=pv%3A1%3Agdpr%3A14%3Avf%3A9ezyymqkmijljhdjn%3Afp%3A1976%3Afu%3A0%3Aen%3Autf-8%3Ala%3Aen-US%3Av%3A680%3Acn%3A1%3Adp%3A0%3Als%3A1156845228070%3Ahid%3A271984739%3Az%3A120%3Ai%3A202101029175118%3Aet%3A1635522678%3Ac%3A1%3Arn%3A1015963535%3Au%3A16355226783226226628%3Aw%3A148x55%3As%3A1280x1024x32%3Aifr%3A1%3Aj%3A1%3Ans%3A16355226747343%3Ads%3A0%2C0%2C0%2C0%2C0%2C%2C128%2C0%2C1973%2C1975%2C0%2C1973%3Aco%3A0%3Arqnl%3A1%3Ast%3A1635522680%3At%3AHTTP%20404%20Resource%20not%20found&t=gdpr%2814%29ti%283%29&wmode=5 Pragma: no-cache Set-Cookie: yandexuid=847304281635522680; Expires=Sat, 29-Oct-2022 15:51:20 GMT; Domain=.yandex.ru; Path=/ Set-Cookie: yabs-sid=2327043721635522680; Path=/ Set-Cookie: i=vL1T7ICVuHRXpyNPzwMzlaKjl/D94ryPalEPO4xIx2pX5AZpVtBfDP0mulercdmDCjCbNqUK2tSOHbHUPiY/6ZY1euA=; Expires=Mon, 27-Oct-2031 15:51:20 GMT; Domain=.yandex.ru; Path=/; Secure; HttpOnly Set-Cookie: ymex=1667058680.yrts.1635522680#1667058680.yrtsi.1635522680; Expires=Sat, 29-Oct-2022 15:51:20 GMT; Domain=.yandex.ru; Path=/ Strict-Transport-Security: max-age=31536000 Transfer-Encoding: chunked X-XSS-Protection: 1; mode=block
2021-10-29 15:51:21 UTC	267	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49797	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:21 UTC	267	OUT	GET /watch/14153041?callback=_ymjsp355627947&page-url=http%3A%2F%2Fwww.all-bearings.narod.ru%2Ffirstpage.html&charset=utf-8&browser-info=pv%3A1%3Agdpr%3A14%3Avf%3A9ezyymqkmijljhdjn%3Afp%3A1930%3Afu%3A0%3Aen%3Autf-8%3Ala%3Aen-US%3Av%3A680%3Acn%3A1%3Adp%3A0%3Als%3A732524701665%3Ahid%3A87010386%3Az%3A120%3Ai%3A202101029175120%3Aet%3A1635522680%3Ac%3A1%3Arn%3A244404675%3Au%3A16355226783226226628%3Aw%3A148x47%3As%3A1280x1024x32%3Aifr%3A1%3Aj%3A1%3Ans%3A1635522674781%3Ads%3A0%2C0%2C0%2C0%2C0%2C%2C155%2C0%2C2520%2C2521%2C0%2C2520%3Aco%3A0%3Arqnl%3A1%3Ast%3A1635522681%3At%3AHTTP%20404%20Resource%20not%20found&t=gdpr(14)ti(3)&wmode=5 HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/firstpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: mc.yandex.ru Connection: Keep-Alive
2021-10-29 15:51:21 UTC	268	IN	HTTP/1.1 302 Moved temporarily Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Connection: Close Date: Fri, 29 Oct 2021 15:51:21 GMT Expires: Fri, 29-Oct-2021 15:51:21 GMT Last-Modified: Fri, 29-Oct-2021 15:51:21 GMT Location: /watch/14153041/1?callback=_ymjsp355627947&page-url=http%3A%2F%2Fwww.all-bearings.narod.ru%2Ffirstpage.html&charset=utf-8&browser-info=pv%3A1%3Agdpr%3A14%3Avf%3A9ezyymqkmijljhdjn%3Afp%3A1930%3Afu%3A0%3Aen%3Autf-8%3Ala%3Aen-US%3Av%3A680%3Acn%3A1%3Adp%3A0%3Als%3A732524701665%3Ahid%3A87010386%3Az%3A120%3Ai%3A202101029175120%3Aet%3A1635522680%3Ac%3A1%3Arn%3A244404675%3Au%3A16355226783226226628%3Aw%3A148x47%3As%3A1280x1024x32%3Aifr%3A1%3Aj%3A1%3Ans%3A1635522674781%3Ads%3A0%2C0%2C0%2C0%2C0%2C%2C155%2C0%2C2520%2C2521%2C0%2C2520%3Aco%3A0%3Arqnl%3A1%3Ast%3A1635522681%3At%3AHTTP%20404%20Resource%20not%20found&t=gdpr%2814%29ti%283%29&wmode=5 Pragma: no-cache Set-Cookie: yandexuid=3723159021635522681; Expires=Sat, 29-Oct-2022 15:51:21 GMT; Domain=.yandex.ru; Path=/ Set-Cookie: yabs-sid=702787781635522681; Path=/ Set-Cookie: i=yROKAQCkQEDp/MhTCtujtSWzFSx7PgG/2QZgPGeQuaYkCYGk4Lr5g33sdF0NzFWf3pPBk9Yj1OF7cHnVzZMM+SWO+Mc=; Expires=Mon, 27-Oct-2031 15:51:14 GMT; Domain=.yandex.ru; Path=/; Secure; HttpOnly Set-Cookie: ymex=1667058681.yrts.1635522681#1667058681.yrtsi.1635522681; Expires=Sat, 29-Oct-2022 15:51:21 GMT; Domain=.yandex.ru; Path=/ Strict-Transport-Security: max-age=31536000 Transfer-Encoding: chunked X-XSS-Protection: 1; mode=block
2021-10-29 15:51:21 UTC	270	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49798	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:21 UTC	270	OUT	GET /metrika/advert.gif?t=ti(4) HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: mc.yandex.ru Connection: Keep-Alive
2021-10-29 15:51:21 UTC	270	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Cache-Control: max-age=3600 Connection: Close Content-Length: 43 Content-Type: image/gif Date: Fri, 29 Oct 2021 15:51:21 GMT ETag: "617677e6-2b" Expires: Fri, 29 Oct 2021 16:51:21 GMT Last-Modified: Mon, 25 Oct 2021 12:24:54 GMT Strict-Transport-Security: max-age=31536000
2021-10-29 15:51:21 UTC	270	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 00 00 00 00 00 00 00 00 21 f9 04 01 00 00 00 00 2c 00 00 00 00 01 00 01 00 00 02 02 44 01 00 3b Data Ascii: GIF89a!,D;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49799	87.250.251.119	443	C:\Users\user\Desktop\njw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:51:21 UTC	270	OUT	GET /watch/14153041/1?callback=_ymjsp303195921&page-url=http%3A%2F%2Fwww.all-bearings.narod.ru%2Fsecondpage.html&charset=utf-8&browser-info=pv%3A1%3Agdpr%3A14%3Avf%3A9ezyymqkmijljhdjn%3Afp%3A1976%3Afu%3A0%3Aen%3Autf-8%3Ala%3Aen-US%3Av%3A680%3Acn%3A1%3Adp%3A0%3Als%3A1156845228070%3Ahid%3A271984739%3Az%3A120%3Ai%3A202101029175118%3Aet%3A1635522678%3Ac%3A1%3Arn%3A1015963535%3Au%3A16355226783226226 28%3Aw%3A148x55%3As%3A1280x1024x32%3Aifr%3A1%3Aj%3A1%3Ans%3A1635522674734%3Ads%3A0%2C0%2C0%2C0%2C0%2C0%2C%2C128%2C0%2C1973%2C1975%2C0%2C1973%3Aco%3A0%3Arqnl%3A1%3Ast%3A1635522680%3At%3AHTTP%20404%20Resource%20not%20found&t=gdpr%2814%29ti%283%29&wmode=5 HTTP/1.1 Accept: */* Referer: http://www.all-bearings.narod.ru/secondpage.html Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: mc.yandex.ru Connection: Keep-Alive Cookie: yandexuid=847304281635522680; i=vL1T7ICVuHRXpyNPzwMzlaKjl/D94ryPalEPO4xIx2pX5AZpVtBfDP0muIercdmDCjCbNqUK2tSOHbHUPiY/6ZY1euA=; ymex=1667058680.yrts.1635522680#1667058680.yrtsi.1635522680; yabs-sid=2327043721635522680
2021-10-29 15:51:21 UTC	273	IN	HTTP/1.1 200 Ok Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Connection: Close Content-Length: 343 Content-Type: application/javascript Date: Fri, 29 Oct 2021 15:51:21 GMT Expires: Fri, 29-Oct-2021 15:51:21 GMT Last-Modified: Fri, 29-Oct-2021 15:51:21 GMT Pragma: no-cache Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
2021-10-29 15:51:21 UTC	273	IN	Data Raw: 2f 2a 2a 2f 74 72 79 7b 5f 79 6d 6a 73 70 33 30 33 31 39 35 39 32 31 28 7b 22 61 75 74 6f 5f 67 6f 61 6c 73 22 3a 30 2c 22 62 75 74 74 6f 6e 5f 67 6f 61 6c 73 22 3a 30 2c 22 63 5f 72 65 63 70 22 3a 22 31 2e 30 30 30 30 30 22 2c 22 66 6f 72 6d 5f 67 6f 61 6c 73 22 3a 30 2c 22 70 63 73 22 3a 22 31 22 2c 22 77 65 62 76 69 73 6f 72 22 3a 7b 22 61 72 63 68 5f 74 79 70 65 22 3a 22 6e 6f 6e 65 22 2c 22 64 61 74 65 22 3a 22 32 30 32 30 2d 30 39 2d 30 34 20 32 30 3a 33 32 3a 32 31 22 2c 22 66 6f 72 6d 73 22 3a 31 2c 22 72 65 63 70 22 3a 22 31 2e 30 30 30 30 30 22 7d 2c 22 73 62 70 22 3a 20 7b 22 61 22 3a 22 64 49 2f 53 48 47 41 4a 56 2b 51 46 38 2b 43 6a 73 68 70 4e 49 6a 41 73 64 6a 58 77 61 4e 53 70 32 70 32 45 74 59 6b 41 78 78 4b 4b 74 63 74 6a 4b 79 2b 69 75 Data Ascii: /**/try{_ymjsp303195921({"auto_goals":0,"button_goals":0,"c_recp":"1.00000","form_goals":0,"pcs":"1","webvisor":{"arch_type":"none","date":"2020-09-04 20:32:21","forms":1,"recp":"1.00000"},"sbp": {"a":"dI/SHGAJV+QF8+CjshpNIjAsdjXwaNSp2p2EtYkAxxKKtctjKy+iu

Code Manipulations

Statistics

System Behavior

Analysis Process: njw.exe PID: 7120 Parent PID: 6120

General

Start time:	17:50:33
Start date:	29/10/2021
Path:	C:\Users\user\Desktop\njw.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\njw.exe'
Imagebase:	0x400000
File size:	1694802 bytes
MD5 hash:	3F91F84924D1DB7ACE9AD307FCAE35D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000000.00000002.931984957.0000000000401000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Disassembly

Code Analysis