ID: 526326
Sample Name: 2zTgaLRFkL.dll
Cookbook: default.jbs
Time: 14:27:45
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

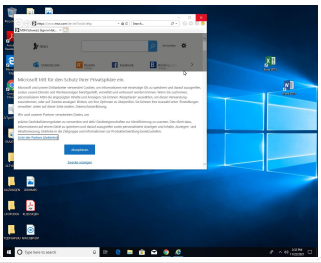
Windows Analysis Report 2zTgaLRFkL.dll

Overview

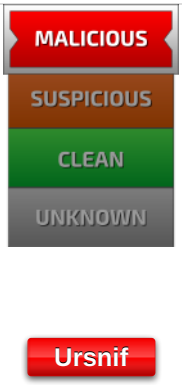
General Information

Sample Name:	2zTgaLRFkL.dll
Analysis ID:	526326
MD5:	096d27e730a166..
SHA1:	880a73f218d5b4b.
SHA256:	5bbba6d13c8222..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection



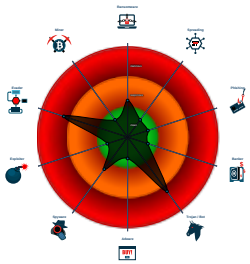
Ursnif

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Tries to detect virtualization through…
- Potentially malicious time measurem…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Tries to load missing DLLs
- Contains functionality to check if a d…
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Detected potential crypto function
- Contains functionality to query CPU …
- Registers a DLL
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5092 cmdline: loaddll32.exe "C:\Users\user\Desktop\2zTgaLRFkL.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 2244 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\2zTgaLRFkL.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4888 cmdline: rundll32.exe "C:\Users\user\Desktop\2zTgaLRFkL.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 2076 cmdline: regsvr32.exe /s C:\Users\user\Desktop\2zTgaLRFkL.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 764 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 5164 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:764 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 5132 cmdline: rundll32.exe C:\Users\user\Desktop\2zTgaLRFkL.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4380 cmdline: rundll32.exe C:\Users\user\Desktop\2zTgaLRFkL.dll,abetfoehywujav MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6004 cmdline: rundll32.exe C:\Users\user\Desktop\2zTgaLRFkL.dll,abjqkqaxstop MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"v1wySnSj0/Qezkq1+zqVG7OQdnxYD8ELZYNPMCkM69BOSUxuoiK8V9jGPFM/rZ9NhfGzVodUM3YW0nB89rcH84RZYG8DLN6HQCkubhXRasaUA7K7h+3lZamvjyookCKgwBWzlu6vCX1eURNonlpROKDMQKBVqofzDshoxJHbAdjZcKqCfEt5vgt07jQB8OABEnd9fROXGjobZcsdaOkEjTvELBFteszn3jqJa1HvAPkpE5gs00qstYhkLp1L+MgFUoKXEL4WViIcGGNpbyyXZKBlebQs4TypEMrC0SUg0PsB7mmSQ4ESN3oL02+qpL14r8rTcWPMVTQH9/bLARbe3XOvj+AriFcBjSRm8ai2Vy0=",
  "c2_domain": [
    "microsoft.com/windowsdisabler",
    "https://technoshoper.com",
    "https://avolebukoneh.website",
    "http://technoshoper.com",
    "http://avolebukoneh.website"
  ],
  "botnet": "8899",
  "server": "12",
  "serpent_key": "56473871MNTYAIDA",
  "sleep_time": "10",
  "CONF_TIMEOUT": "10",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.911757798.0000000004620000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000002.911635582.0000000004600000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000005.00000002.911557435.0000000002ED0000.00000040.00000010.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000005.00000002.911406171.0000000002EB0000.00000004.00000010.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.2ed0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.regsvr32.exe.4620000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.2eb0000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.regsvr32.exe.4620000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.regsvr32.exe.4600000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 1 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Potentially malicious time measurement code found

Stealing of Sensitive Information:

Yara detected Ursnif

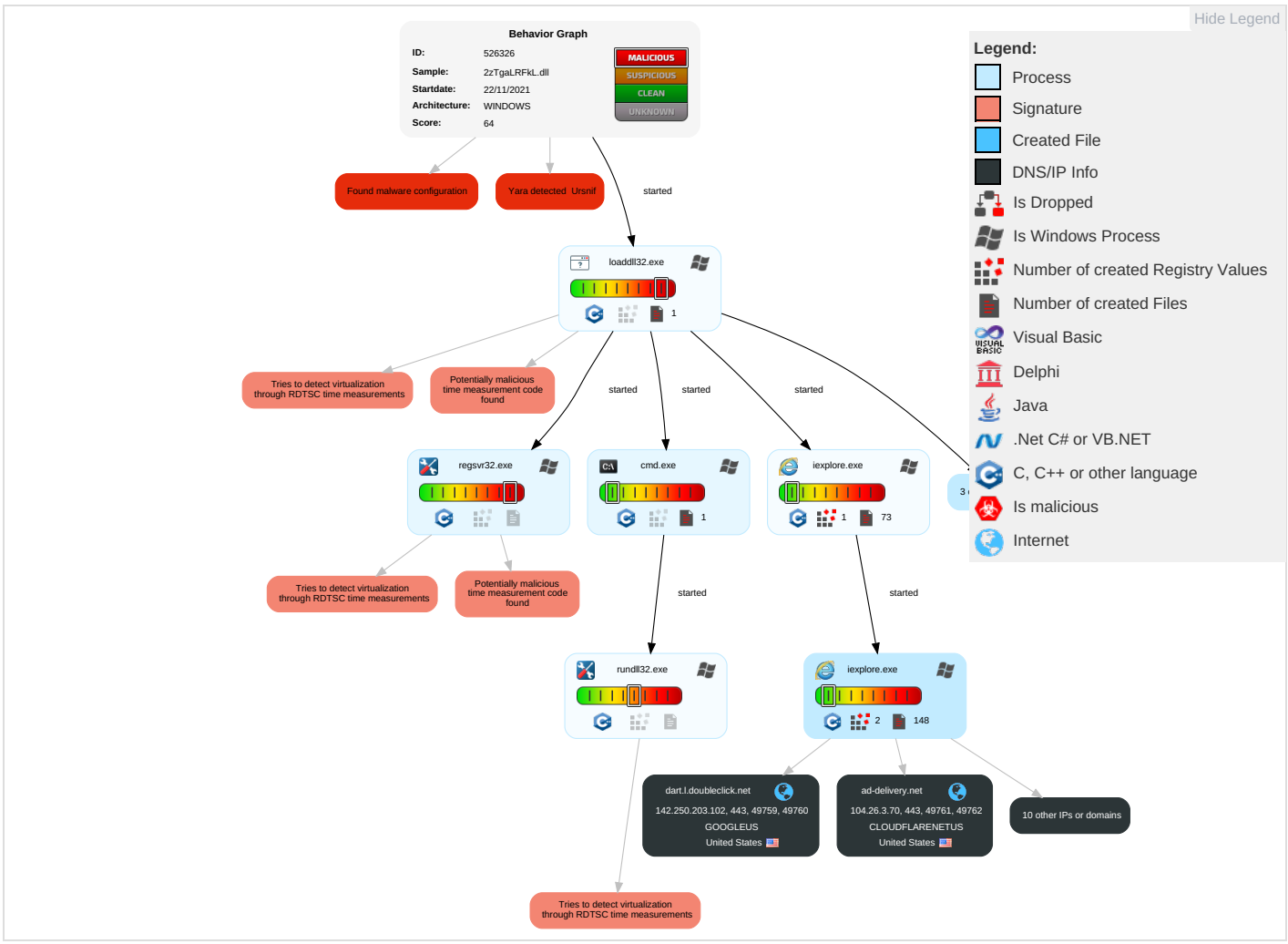
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Rem Serv Effe
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 2	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication	Rem Trac With Auth
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 2	LSASS Memory	Security Software Discovery 1 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Rem Wipe With Auth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obta Devi Clou Back
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Regsvr32 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

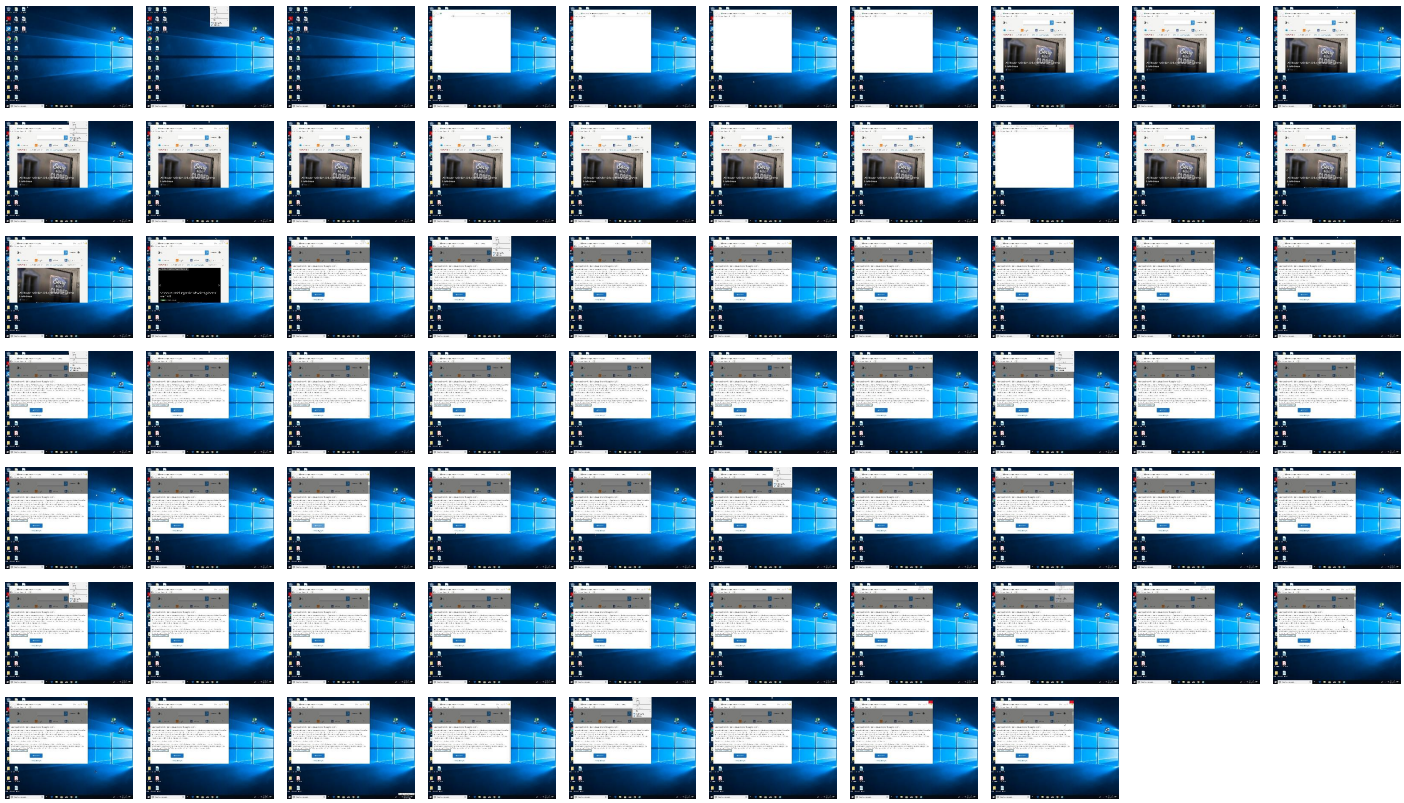
Behavior Graph

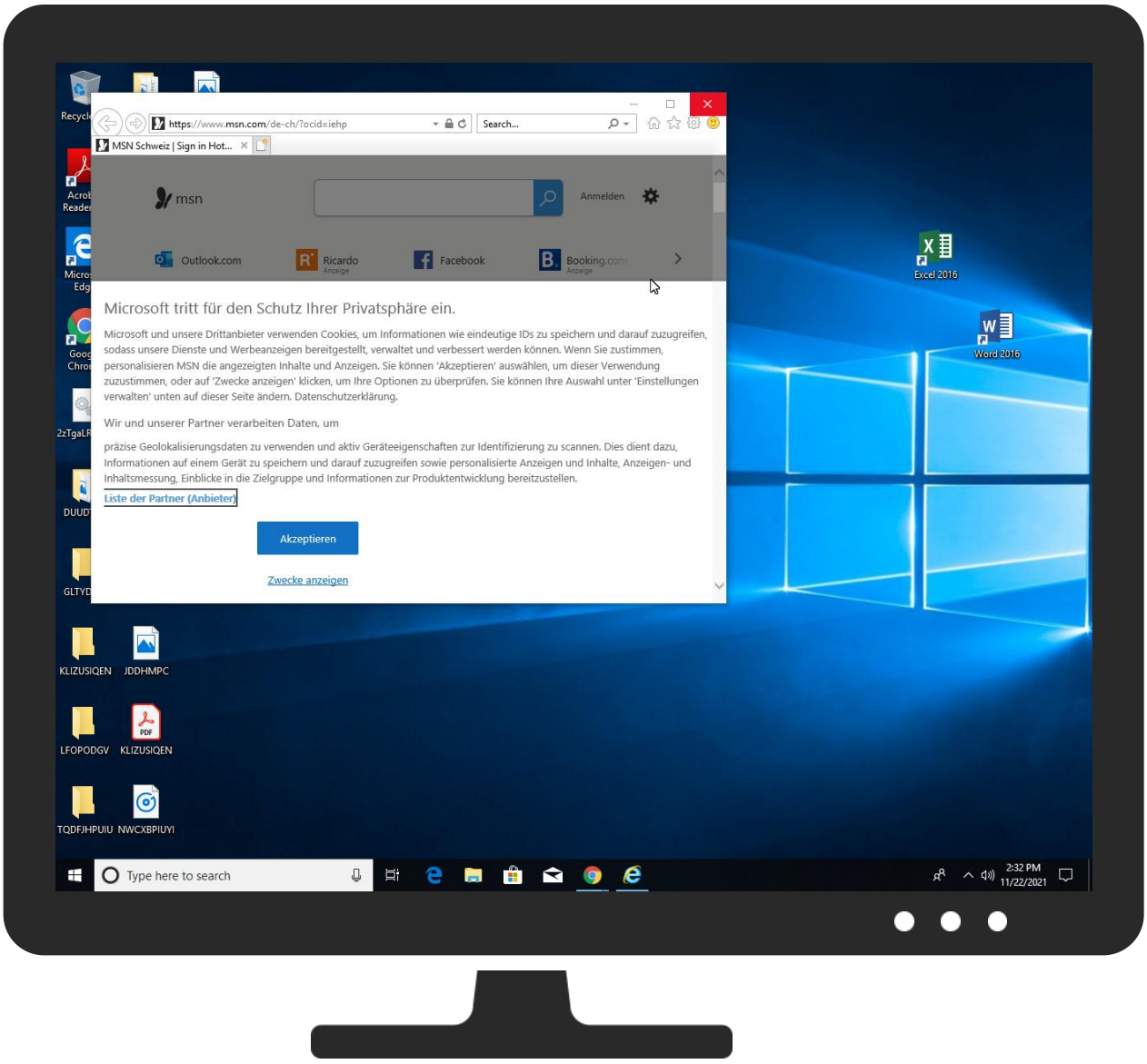


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://https://www.botman.ninja/privacy-policy	0%	Avira URL Cloud	safe	
http://https://www.queryclick.com/privacy-policy	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	
http://https://www.stroeer.de/werben-mit-stroeer/onlinewerbung/programmatic-data/sdi-datenschutz-b2c	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://silvermob.com/privacy	0%	Avira URL Cloud	safe	
http://https://ad-delivery.net/px.gif?ch=1&e=0.4482105559414631	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://doceree.com/.well-known/deviceStorage.json	0%	Avira URL Cloud	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://www.stroeer.de/ssp-datenschutz	0%	Avira URL Cloud	safe	
http://https://optimise-it.de/datenschutz	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	2.18.160.23	true	false		high
dart.l.doubleclick.net	142.250.203.102	true	false		high
hblg.media.net	2.18.160.23	true	false		high
lg3.media.net	2.18.160.23	true	false		high
btloader.com	172.67.70.134	true	false		unknown
ad-delivery.net	104.26.3.70	true	false		unknown
assets.msn.com	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
cvision.media.net	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://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250	false		high
http://https://ad-delivery.net/px.gif?ch=1&e=0.4482105559414631	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.3.70	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
142.250.203.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
172.67.70.134	btloader.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526326
Start date:	22.11.2021
Start time:	14:27:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 38s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	2zTgaLRFkL.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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:	mal64.troj.evad.winDLL@17/115@11/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 92.8%) • Quality average: 82.1% • Quality standard deviation: 29.8%
HCA Information:	• Successful, ratio: 68% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.26.3.70	http://mkklcdnv61.com	Get hash	malicious	Browse	• mkklcdnv61.com/cdn-cgi/styles/main.css
172.67.70.134	0MGLPJiSa5.dll	Get hash	malicious	Browse	
	wMidyLtyIL.dll	Get hash	malicious	Browse	
	delta.dll	Get hash	malicious	Browse	
	5555555.dll	Get hash	malicious	Browse	
	5555555.dll	Get hash	malicious	Browse	
	wsEUOSJMF6.dll	Get hash	malicious	Browse	
	wsEUOSJMF6.dll	Get hash	malicious	Browse	
	X4V4jFmFhO.dll	Get hash	malicious	Browse	
	new.dll	Get hash	malicious	Browse	
	youNextNext.dll	Get hash	malicious	Browse	
	gelfor.dll	Get hash	malicious	Browse	
	bebys10.dll	Get hash	malicious	Browse	
	INV-23373_2.dll	Get hash	malicious	Browse	
	WfLJNUAm.dll	Get hash	malicious	Browse	
	zuroq1.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment 1205_2.dll	Get hash	malicious	Browse	
	girlDowTube.dll	Get hash	malicious	Browse	
	tbConn.dll	Get hash	malicious	Browse	
	RFQ 104RM.dll	Get hash	malicious	Browse	
	RFQ 5mn00.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
contextual.media.net	tebdXHvUhB.dll	Get hash	malicious	Browse	• 2.18.160.23
	619b721d39f71.dll	Get hash	malicious	Browse	• 2.18.160.23
	619b721d39f71.dll	Get hash	malicious	Browse	• 2.18.160.23
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 2.18.160.23
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 2.18.160.23
	malware.dll	Get hash	malicious	Browse	• 2.18.160.23
	kZ45hWt9ul.dll	Get hash	malicious	Browse	• 2.18.160.23
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 23.211.6.95
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 23.211.6.95
	loveTubeLike.dll	Get hash	malicious	Browse	• 104.76.200.23
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 23.211.6.95
	data.dll	Get hash	malicious	Browse	• 2.18.160.23
	Kathleen.xz.0.dll	Get hash	malicious	Browse	• 2.18.160.23
	delta.dll	Get hash	malicious	Browse	• 23.211.6.95
	2021-11-15-DLL-returned-from-softwareupdatechecking.at.dll	Get hash	malicious	Browse	• 23.211.6.95
	delta.dll	Get hash	malicious	Browse	• 23.211.6.95
	5555555.dll	Get hash	malicious	Browse	• 23.211.6.95
	5555555.dll	Get hash	malicious	Browse	• 23.211.6.95
	5555555.dll	Get hash	malicious	Browse	• 2.18.160.23
	5555555.dll	Get hash	malicious	Browse	• 2.18.160.23

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	zMvP34LhcZ.exe	Get hash	malicious	Browse	• 162.159.133.233
	tebdXHvUhB.dll	Get hash	malicious	Browse	• 104.26.6.139
	Payment Swift Copy Of #U00a362,271.03.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment Advice...pdf....exe	Get hash	malicious	Browse	• 162.159.130.233
	new order.docx	Get hash	malicious	Browse	• 104.21.71.149
	BANK DETAILS.doc	Get hash	malicious	Browse	• 172.67.171.239
	VESSEL SAILING SCHEDULE FOR WEEK __ 48.ppam	Get hash	malicious	Browse	• 104.16.203.237
	DHL_AWB_NO#907853880911.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment Advice 001-22112021.ppam	Get hash	malicious	Browse	• 104.16.203.237
	^^att-DHL 20180904153201117119330^PDF.exe	Get hash	malicious	Browse	• 172.67.200.96
	Almunif Pipes Purchase order_04212021.exe	Get hash	malicious	Browse	• 104.21.19.200
	ZiraatBankasi-20212211.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase_order.exe	Get hash	malicious	Browse	• 104.21.19.200
	New Order 000112221.exe	Get hash	malicious	Browse	• 104.21.59.22
	Payment Advice...pdf....exe	Get hash	malicious	Browse	• 162.159.133.233
	619b721d39f71.dll	Get hash	malicious	Browse	• 104.26.3.70
	619b721d39f71.dll	Get hash	malicious	Browse	• 104.26.7.139
	Play_VM_582497.htm	Get hash	malicious	Browse	• 104.18.11.207
	TEVRKPBK.EXE	Get hash	malicious	Browse	• 162.159.133.233
	PO.NX-48940.xlsx	Get hash	malicious	Browse	• 23.227.38.74
CLOUDFLARENETUS	zMvP34LhcZ.exe	Get hash	malicious	Browse	• 162.159.133.233
	tebdXHvUhB.dll	Get hash	malicious	Browse	• 104.26.6.139
	Payment Swift Copy Of #U00a362,271.03.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment Advice...pdf....exe	Get hash	malicious	Browse	• 162.159.130.233
	new order.docx	Get hash	malicious	Browse	• 104.21.71.149
	BANK DETAILS.doc	Get hash	malicious	Browse	• 172.67.171.239
	VESSEL SAILING SCHEDULE FOR WEEK __ 48.ppam	Get hash	malicious	Browse	• 104.16.203.237

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_AWB_NO#907853880911.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment Advice 001-22112021.ppam	Get hash	malicious	Browse	• 104.16.203.237
	^^att-DHL 20180904153201117119330^PDF.exe	Get hash	malicious	Browse	• 172.67.200.96
	Almunif Pipes Purchase order_04212021.exe	Get hash	malicious	Browse	• 104.21.19.200
	ZiraatBankasi-20212211.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase_order.exe	Get hash	malicious	Browse	• 104.21.19.200
	New Order 000112221.exe	Get hash	malicious	Browse	• 104.21.59.22
	Payment Advice...pdf....exe	Get hash	malicious	Browse	• 162.159.133.233
	619b721d39f71.dll	Get hash	malicious	Browse	• 104.26.3.70
	619b721d39f71.dll	Get hash	malicious	Browse	• 104.26.7.139
	Play_VM_582497.htm	Get hash	malicious	Browse	• 104.18.11.207
	TEVRKPBK.EXE	Get hash	malicious	Browse	• 162.159.133.233
	PO.NX-48940.xlsx	Get hash	malicious	Browse	• 23.227.38.74

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	619b721d39f71.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	619b721d39f71.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	AP_Remittance_SWT130003815_0.html	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	Order Enquiry_CRM07540001965-pdf(109KB).exe	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	malware.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	kZ45hWt9ul.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	loveTubeLike.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	ATT00330.HTM	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	data.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TELEFAX_Davidson-techOLX831OLX23AY2AY.HTM	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	Receipt_INV_460Kbps fdp.htm	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	MrBfVHgunq.exe	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	Kathleen.xz.0.dll	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	TELEFAX_SaccountyZNT142ZNT08YN8YN.HTM	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134
	Remittance-11162021.html	Get hash	malicious	Browse	• 104.26.3.70 • 142.250.203.102 • 172.67.70.134

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.msn[2].xml

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	139
Entropy (8bit):	5.239434861799844
Encrypted:	false
SSDEEP:	3:D9yRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAekKWLFdAqSmoA0aKb:JUFkduqswEkIXH40AAekKhskb
MD5:	C7A2F0B6DB20F2AEBC3CD94FC7533C0D
SHA1:	4377F1679EED282D8258818758CB39CCEFBDE616
SHA-256:	410410F76F7E95DEE831CEE4516AFEF95EEC20608F8E3569477A8C2A4E03ABB0
SHA-512:	D77005E2334813460A4E23ED00FF90B9CBDC18EFEA198EC21557B9F1BF320471E5D21F9A42AFC74B39B26B70B59B1F3D38E6D9CE753DD92F34BB5722311CC89
Malicious:	false
Preview:	<root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="1855895936" htime="30924784" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\contextual.media[1].xml

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	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\Recovery\High\Active\RecoveryStore.{8D788003-4BE3-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{8D788003-4BE3-11EC-90E5-ECF4BB570DC9}.dat	
Size (bytes):	5120
Entropy (8bit):	1.9004012448977132
Encrypted:	false
SSDEEP:	12:rl0YmGFIMOrEgm2p+IaCyQZI/GgCF+ULrEgm2p+IaCyQZI/GeFoyZI0G77xyZI0a:rNOGW/3yPULGW/3yjoyyLyy69lW8C6
MD5:	61F789A54984C2C7D2FEA842CFD89FA2
SHA1:	B7DBCCF3B52C31C80D1DFED9C4370D99A55B0FEC
SHA-256:	3D250A2F46C7E6CFCFD09076A67299E2E3E75977E284F66F349BD367173DFD2F
SHA-512:	ADD1889F3942CB9E20DDAD617D15CD30F6D2E0A71086E056DF3475C8035C7F6823BB946B65D0175FB99E5A6EFF9967F85F8CE5B2195E774A233DC336CC8F99E
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....l.[.....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.B.I.B.4.j.e.N.L.7.B.G.Q.5.e.z.0.u.1.c.N.y.Q.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8D788005-4BE3-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	329728
Entropy (8bit):	3.6032894448710744
Encrypted:	false
SSDEEP:	3072:jZ/2Bfcdmu5kgTzGtZZ/2Bfc+mu5kgTzGtQZ/2Bfcdmu5kgTzGtnZ/2Bfc+mu5kn:K264
MD5:	E5841DAE433F6E9F14A9BA72507F3F98
SHA1:	9ADF8D939A5B1D5F5CE40B6D1BEE8C6F6266376E
SHA-256:	849B3389B88864732DF0216C858284186127F8904F41189350ECF2FC6AE5AC6B
SHA-512:	352BCEDC25D671732A5FDC5C4E3E040819DFA3FBE0B618238293F50447ACF74C1859F51ECB2FADE0C8CDF1E17477286A2C96A5EB0DC00987E7271DBB62648EA
Malicious:	false
Preview:	.....>.....D...E...F...G..... .....R.o.o.t. . E.n.t.r.y.....0..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.....4. .....T.r.a.v.e.l.L.o.g.....T.L.0.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.087980626813176
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc41EEad7dB/TD90/QL3WIZK0QhPPFVDHkEtMjwu:TMHdNMNxOEEa5LnWimI00ONVbkEtMb
MD5:	C0F0E696BD531C1501C17A572896704B
SHA1:	59FEA2CB8FBECFE55D03FDF3162F1438E3275D49
SHA-256:	9AC46141AA72BD128297500017A1EC5A7B2E8228F7E191A76148735E6ABE9EDD
SHA-512:	7F129AE4C9D6C38B619D6114AB34DA86C6476DB95340592628099D93A43E4A184570F1B468C162C203E8F078B0A154455C1301076E3B5470E327CAACC47FA863
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x88561c8b,0x01d7dff0</date><accdate>0x8b868e13,0x01d7dff0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.1080777675483695
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4fLGTkc7EobXUtTD90/QL3WIZK0QhPPFkI5kU5EtMjwu:TMHdNMNxe2kaEAUtnWimI00ONkak6Ety
MD5:	364B28B3C75B6371ED9A7DD4260FAE67
SHA1:	D071A45B3D0DAF7CF5B27C5E2490EBD279489B6D
SHA-256:	37AD92C131D5FDDE96349F14DA6820337D850106147FDAD64C6AF87C00D51D12
SHA-512:	9E92144223BEC553544E62352676E520EC76C9C7EE4C026FE1E4C15939E02A05B7DE0EE9E9A8D12A4FDE7CD0BB8B0FD2E98712463FF8EA359CFB27A86A65BBAE
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x7dc00d46,0x01d7dff0</date><accdate>0x7e622c30,0x01d7dff0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.107736549894857
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4GLeAC+s7VY3TD90/QL3WIZK0QhPPFyhBcEEtMjwu:TMHdNMNxvLpCF+3nWimI00ONmZEtMb
MD5:	B4C0790285C93FA5D5DF269910A4A56C
SHA1:	C017F46E08CA8DF5AD65D6D68C99406EFDE40981
SHA-256:	1F3CC4A673277C0DBDD8B3D098669E1A02E043CB221B08AF0A0FD295863F96C7
SHA-512:	0B71268043C2C9FEA922968DAE000833439E9D5B7AC4B82D38FAA4D4EF0816F4552C3489ADEE579AA8DA03DF44331853126FEAC7AF65DBBC915F763124F4A84
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x8bc22a28,0x01d7dff0</date><accdate>0x8be1275f,0x01d7dff0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.123837759095399
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4JIGW33VUBE+KTD90/QL3WIZK0QhPPFgE5EtMjwu:TMHdNMNxiIBH+E+KnWimI00ONd5EtMb
MD5:	AE0113131C820EBB6FD102DA2ED87FCD
SHA1:	DC4E51CFC295EE47F8153DD3D7F7D3A7D10A2BDA
SHA-256:	1235C4B2508343299CBA5A2915AAD0FD93E09A49E31AA2FB11BFCB8500A4C8C6
SHA-512:	D39B0F4112E0DB5083D2313F67F8519638750E87C586AE49857931AAFBA7BE5D2AC91A2DFD9BEABF51524302A87426C46994408C3A28382F2ADFE6BDAF58104
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x8456391f,0x01d7dff0</date><accdate>0x84ac0c82,0x01d7dff0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.111605618384957
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4UxGweLBAY3TD90/QL3WIZK0QhPPF8K0QU5EtMjwu:TMHdNMNxhGwgAY3nWimI00ON8K075Ety
MD5:	F78B5C40A51FE94816CBB21F5FB94787
SHA1:	CA9D366C70F0A1C35AF62483E42281B2FD99477A
SHA-256:	C16A1B76E0B0FACA1E9DDD2DA79FB0E61B8C9C34FA2F540A97D27911AE06DAEC
SHA-512:	FE049AF6FCB73E3A0C44A5F63B3F6C3506454539969E3268EC65D78A688E00DAC98BFAE17F3721AB47CAB592A086CEDB1D7CF25A6E06C12D460585F095A7FE46
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x8bf8fed4,0x01d7dff0</date><accdate>0x8c159c3d,0x01d7dff0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.117285021147419
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4QunKMdqGXTD90/QL3WIZK0QhPPFAkEtMjwu:TMHdNMNx0nd3nWimI00ONxEtMb

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
MD5:	E4129AC6CD14BA5B7B0B557EB42EB32E
SHA1:	339CF5430D8E309B204C3A4D33978A4C978B4BC9
SHA-256:	3E90667EF2A7CEA0D637903B421F807F286D35159CE856D7F2E196B239025557
SHA-512:	B7EF2E27B29981CA97265FD10F5948F8442E4C808FD7603BA4C275ECE4457BB88C0A10B8E0E57E19CC3965618E1832A496FF06A1E68AA4E3A4BA35084C51F8CI
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x86298479,0x01d7dff0</date><a ccdate>0x863efa71,0x01d7dff0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Re ddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.147761772632051
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4oTfn/unTD90/QL3WIZK0QhPPF6Kq5EtMjwu:TMHdNMNxxfknWimI00ON6Kq5EtMb
MD5:	878FAD2B0A259C67E1BCCF419F487B8B
SHA1:	A35B4F055BB56A4692EE454B6360B502438EE748
SHA-256:	9BFB9FCE57F0825317FC385757999194E8F7B0B981C7EC8C2776391C1804CF46
SHA-512:	F1FF7DE0FEB206A6858FFEFDDB40CC68A75D12892CB814E0D38BB9E8DAA7DDFE9DC5658F1ABC22086433F2C14081B806913E48892591D26832A9B3D930889E2 8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x8544a2d3,0x01d7dff0</date>< accdate>0x860a860e,0x01d7dff0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\N YTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.133498009122621
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4YX2nD1Ko8TD90/QL3WIZK0QhPPF02CqEtMjwu:TMHdNMNxcD1Ko8nWimI00ONVEtMb
MD5:	4D502DB193B2B165006E8C7E1277BCD0
SHA1:	7BA677F2F4E7EE9CF3241BD85614CBDDE8EA452A
SHA-256:	F05A5BBF42659E36717FB6C060931BBD9BFF3D749B4BBC8EC6ACCC2E450BAD11
SHA-512:	6A11225B4634F61A4CC8693D9E1D66568C82204A8D88EB0B345CA8902D6150D4DFCDB160AC489EBE3E7041980B68EBB74455DA50C92BCFB296A6E3304662F50
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x81446d26,0x01d7dff0</date> <accdate>0x835a7b73,0x01d7dff0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\ Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.089308135001532
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4Inn3TD90/QL3WIZK0QhPPFiwE5EtMjwu:TMHdNMNxfnn3nWimI00ONe5EtMb
MD5:	947A12ADBB64A9C7E012A033FEFBB6FA
SHA1:	ECE32A47C5919B84129EA839840533058B8B15C8
SHA-256:	A40C7DF308347D2C5124BE52DAC372B8712BC23803E76D49F5E070C1BA9F392F
SHA-512:	CE145D051221660D87FCEC3EE5B698352D7D75AE7B3803A772E3751F0B5D9DC2F586C34EB10EE948F8C07C718A17451164869C682EEB6EE32F4027FFD20564D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x83a82c20,0x01d7dff0</date><a ccdate>0x83bda234,0x01d7dff0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Category:	dropped
Size (bytes):	22330
Entropy (8bit):	4.293002444235518
Encrypted:	false
SSDEEP:	96:eQQQQQ1n9KlyzS29dcBUXqupkE1OwDzXIzS29dcBUXq7E:3n4QzSAcBQpkEgcz4zSAcBa
MD5:	0894D09A4039772AF4591CAB1EC7708E
SHA1:	305F7A49F620B29DF2E4548B77A12F551D0EBBED
SHA-256:	B77E35D329FBEC8421BE32088E1008A79E219AE40D23B00CA20A0896666220DF
SHA-512:	241995A26E040B26A420682C10D3D469C34207983870A7B3B224FA74855CB8BB82C0A44B43321063000E5F9ABD86BC2AD9147AE2EE2F8B7683BE0F0BC8BFCE84
Malicious:	false
Preview:	........%.h.t.t.p.s.:././.w.w.w...m.i.c.r.o.s.o.f.t...c.o.m./.f.a.v.i.c.o.n...i.c.o.~(................h(......(....................(......................................"P.."""""""""""""""""""""" """""""""""""""" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"" ...333333333333333 333333333333333"" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"" """" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"" ...33333333333333333333333333 33333"" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"" ...333 3333333333333333333333333333"" ...3333333333333333333333333333333"""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\264bf325-c7e4-4939-8912-2424a7abe532[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	58885
Entropy (8bit):	7.966441610974613
Encrypted:	false
SSDEEP:	1536:Hj/aV3ggpq9UKGo7EVbG4+FVWC2eXNA6qQYKIp/uzL:Di3gyq9Ue7EVsCjeXuS
MD5:	FFA41B1A288BD24A7FC4F5C52C577099
SHA1:	E1FD1B79CCCD8631949357439834F331043CDD28
SHA-256:	AA29FA56717EA9922C3D85AB4324B6F58502C4CF649C850B1EC432E8E2DB955F
SHA-512:	64750B574FFA44C5FD0456D9A32DD1EF1074BA85D380FD996F2CA45FA2CE48D102961A34682B07BA3B4055690BB3622894F0E170BF2CC727FFCD19DECA7CCB D
Malicious:	false
Preview:	......JFIF............C...C...,.,.."..E.........................!...1."AQ.a q..#2.B.....$Rb...3...C...%&4.r.................................B.........................!1A.."Qa..2q.B.......#..Rr.$3b4....%CDc...........?....]..l;.q.`.e...=..??n.\..)..".[K.W.u('d+.c...;.......R...(... .N.~.J,g...-.....-H.[vI....n!.g......F... ...r..>%..*b.l..."......~7.k..s..r....u...0...)........x........4.(Ik...*EM.S...n4rN.V..88.J..~.....Q.FJ..A.D.-D.tk'?.F.......IY.]......O~=*3.N....rr.u(.....'.h},..... ..3[[...q.....g...&.O.....z...k.n.:~.)-S(..M....:.?(?.2206..g...".S........~.#.........=.....~.<,G............B..\l6..@Jr=...(.....N.....xi.....}...o.:F@$...>.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....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AA7XCQ3[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):	667
Entropy (8bit):	7.561736401445472
Encrypted:	false
SSDEEP:	12:6v/7TUYRk5V6RwLzZvLk519s0/tWnssyQSKZLsLO7qcNrXlUA3YUz1oK9:STuzZc19skWssyQ5ZsO7qc1Vdf9
MD5:	C9E843CDDAD2F56F8F88B8D6A937B602
SHA1:	EE3382E8031321B266BA31CA47D0667F03C469F8
SHA-256:	D0A577DFBCF142D19E89E5ABC3EEC3020AD0C3A65B9BA6F6534097D0806B2100
SHA-512:	677CDE3738656508AEDBE2DA698B21B5AA15EBA8EDECE60192A5B61004E6CB6A1F718A02066AFF367021C31B9B13D2DDD703976E8F26C22272AE8AADBECC55 ED
Malicious:	false
Preview:	.PNG........IHDR................a....pHYs..........+.....MIDATx...]HSa...n.l;.d..a-HK)..6......"..... ..Gn...E.Q&.EA.y.T....25.K..UT8...M.....>.[u.=.;.y_..../....#.z..w......6.....n!(.k{<... .K..dv..Fm..Ro.NT..Y.N.....;.....$x.....d....p:.?^LR.8k.........7...9.........S<....)...B..#.5:uck...0..0 d..=V.T..ad.{[Z.?.026<..@...R..@.....}.p-..:......Qlo....5$.D...........,..Q".x...c......+./` .f<....._F.&2q.8E........(...%T.}8...=.:...[[...@ ..e...6....Q...?..".q.......p.......j.f........4H\#j.i"@|6_..2.i-.>.j.....)..'*]..r9.[.T5...$l.A.wa-<#.Dt]sPnc9F..Q.8...].....D...f._S...0WG.>b.....t. ~j>.K.h]4~.....Q....BA..?.}.s..;.......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAPFmi4[1].png	
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\4PB7FJMT\AAPQoxX[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):	29573
Entropy (8bit):	7.923714752002336
Encrypted:	false
SSDEEP:	384:INas7fQoYk50HT2pCNRXne+4kfuASiPbTMJgn3ui/VveFKEZS1IdittMjFACj0A1:IzF10HapIdnear3kZSK4ttM8aaqeUHP
MD5:	64A63C14A787834D43C473733FBFFAD6
SHA1:	F364C8E81CFCA303F0A0F658BAF1276943669FCC
SHA-256:	C28A1E76B2CB256E0505676DDF289CDBBD0C9F2CE1553A021CF29D57626DFAD4
SHA-512:	204D9F37932441E64BF8E19AEE91EFFB8077C1CC4EF95A0F28B83254073EFFEF218DCCD4F032412257F3E9AE1764E41495CB96BFA620AF348E39AF54A3B47FE
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..e.[yv..W.t....%...i...TXlL..Ph-.F.Vm.....v#...b..%....M.. .J...[.....q.iB.3.....i.D.....r....'&e.b....ztS..D....u.g(.Z...Y..5.).I.F...OZ. ..L.b..}.....)..#...9.t.)B...l.\'.....J.....I..-,IA..NMjf.#....Y4.....7<..Wm'.....R..f..tk,.AZ{K.....Ukjf.....J.a>e..a..t..!0G.i.`....s.h..HA@.v)...0....4^.!..[.}..yS].kX.>ddA..G".e..].Ww 1J.l'..s.)."..~..]Y>...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQVPm6[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):	2403
Entropy (8bit):	7.807847874907652
Encrypted:	false
SSDEEP:	48:QfAuETAzOifN8pL/nF/TFZoTy7zOWk0ljjGzRi3wWLtWOqO+zgtO:Qf7EwN8tndAW7zI0l0SRnqO+zgtO
MD5:	10BDCE1F28F778B6F7C76D396A88A0A3
SHA1:	705B774818562E65F4C0DC64A08D8D1E38932772
SHA-256:	EB966433ADA42DEA9BE343ECAFA32C13851D1ADAF91734E0697D96AE3B876D0A
SHA-512:	1BD59BED9431C26C14AA4545A6B459680BBDD855E20CE1FE2A5BD4B861DAA793CA9FA6EAF96F353099440E80DD2046E54577DD0B329C45B8EA5FE13CB08B67 D0
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....O.GO.a._+.....f.wF....LBP.LB.....i\[.e.....(?3...t(.jd..3..bj.... uR..z-.7t?.6W..5$[Y..\.P.}*Z.....~..3.f...y.+)9hkN .....=Z0N#..o.uTWFQvg~k..m.&h.."....i..n..#..M\..-]....K..r..y<7SM..[U..|{.....TeqN...h.S# ..fz..o.O....l|.....T.:Z@@..4..[....).EgQ7-..?.c.T.`..k..=2.....7...\.Y.-Q).2{kV.-.... cM!66....Q...Rj.(.d..{...Z.#...Oj.KPI....t.1G?.....j....7Z..Z%.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQW0Fs[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):	2196
Entropy (8bit):	7.799560401503644
Encrypted:	false
SSDEEP:	48:QfAuETAQgh/boT8B8nC/6gVTzeIA8phYvzJrikCr9KJKqm5sLQ:Qf7E2h/MTRC/6mPCZCBKJjOMQ
MD5:	43B1E133700A65EF28BA0599062D2704
SHA1:	B853984965EE3ACB0924580E8A706AA971A8A5EC
SHA-256:	E90243483DCB75142ED2D6CA34804B2F005416AD471F456FC3DF88B2E69083C5
SHA-512:	A78E4743CAE5DA55EB88B19D59363AAF4DAB05E9A210C26D9FAB550276EB86B448F63385486D2A272FAF27F366ED9A78E41B175C69167020E89958645788D193
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQW0Fs[1].jpg	
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..d`....2..F..i..M....H.Fr..,&.nL.\{.L.P..$M..2~.X..u..3.ml1.).b..^.....fU.-.P...".Q.?1.ERFnE.....;E..9%?...:h.K/.....5B".....bu..O....+.Rl.z5...G'.....1M..>.n]~.6.f.5G5._.....*)`....h.g'"..G~"....6:..GNG["..w.flcM/,....+..I/b..T..Xr{z...dth..1..,[..U.c.....4.,...z...6$W....).y..c..f.n.Kj*..K...}k.F....a.....Vu.)...6.....w....{#.1.....q..dw.4..$[T..d....tv..C).n.&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQXXJy[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):	10174
Entropy (8bit):	7.937857195712491
Encrypted:	false
SSDEEP:	192:QovdgprHERH/bhOU+bPxwbgjL5J74qlIIMFLl0ko1uXf6Y/ejuGJlPOcc:bqY/NOXxwbgj/4qlIHl0kooXj/exJlWL
MD5:	49416265B664B6F3A009C607E64E0B83
SHA1:	07C95D7778CA943B6D2E2C7D8E99350F8EFD1DDE
SHA-256:	7C4A388541EE4DBD07BAC67CCDAA43D790797395EB715410C219BBA6C4D178D6
SHA-512:	C614EF9AD0AE944328249060A6A8C24EF4CDDB5C4967F06F5254CEA304E9EAE8DE0474BF7C4F4C22A3662F4A930ED6EA8069B589DFD20BDA4ECEF0D3B585B3E
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..lR(1@.>..s@.4.(.f....!s@.h.s@.h.....I....i...d..{.*9..Y,.-.I.....|.....A..s..Qp.E0...LP.....(.....(.....(.....s@.4.~...xs..o..7...0=Me9_b.m.....RqY...#..a}.9..1s.{. ..zc..=...O....x...Z....&..Z.....-.....;UFd8.t.....Z.G@.1.....R....7..'...R..|...LA@....P.@....P.@..j.v._j..s..;._A.....+..d.%T;.;*.9...{Ks..o?..?SAV(.. ..k..=cq....a..$l.e8.G.$.;\.....?.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQXevg[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):	12126
Entropy (8bit):	7.945197487897491
Encrypted:	false
SSDEEP:	192:QojRJN0D37cpItLy/vhNWN0jOv7QaeDPhM+xbBiKLZHx7bYfKdohw45mxNVv7M6n:bjRJNAjyJEvEj58KNR7whwMmxDMaYU
MD5:	549D7502E6B50302E7B7451DABF61781
SHA1:	87949284AB340C839F895F33BCD7ABE6ED992637
SHA-256:	904790AB667AD93D7F07BE7B90FD02EC0CF09F9194A78C0F52DBFC704FC49C7D
SHA-512:	E68451666915C21C9C8B254B1292D8702F7813D3496251998A7AC2EB5F0403E05A316221EC14F82E2A7A15CF2C58BC26CF94A942DC99B29498237F5291B1107B
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....`W.....Y."O.2@zR...Jv.f}.`..u.P...z...k.F.....}./.vS..ZKc..G@F..R2.|.)...8.....@."......2.6r>...=2hn._..l%g..0..r.C...f=....`..{V.L.Q$7..F.....0t.n.n.Bm.<G../Jw.*E(5'f!.q..P....2..hr$...D.r..N.c{ !r..2....#..i...4.yA.R.. O\P.@..@..7.+....1....C...I .A..bP...+jQ.>.....c..9...Fh..u../b....+..r'..D..x.(.l~\.LE..@.E.....L"G.m<..Ke$A.....>..[*.7.Wl#..y=..C-...M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQXiy5[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):	11110
Entropy (8bit):	7.951242070250693
Encrypted:	false
SSDEEP:	192:QoyguqTHK+zmMmruzI2SfD13AFTBUG7MGZ2I82Gkl9bmI7JWrxBc:b5uqbKVM/5iD1IU+P4Ze9bN7JWk
MD5:	AD09D99AFBFE624D355296FEB417CADA
SHA1:	D30C2607662C519DBF84610C7DEE73A354BBC3E6
SHA-256:	7FFBDDFCBE2938A28B74F91D9137F1846F9ED472E37DA39F7FAB3C058EFFFA8C
SHA-512:	9612B59DE1DA3EAE25ECA39B7E6FB497099AD8ECE9BC82773B843C5A4CCED62C5A4F57E5F6ADD7496771C6F60FC1C2B66A4C6FEAF70BFD8CE5DA19F5434EC1BD
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..Pd.Z.74..L.p9...l~.(i.....#..j..'z@ii..U....f...Q.t....jf.V..GR2....(:#....1.H..5q..j.G...i...t'....;...D.C.dPw...P.p1..%..fM>....+R70n....rk9H..M+....w..Y....!X.,.V.#...pkD.h..m.R2..Hqf[pk.X...ml..j..[:..l,.7.a.k.....y5..i...E..@..Y.d...%.z....[.sr...e...T....\..z.D1.Q. .itM.Y....s....zJN .....V.C.E*...-M...B....Fkh .f.k..7<...v.1..5.e.)....b..ii...Nz..,..m]...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQXrMl[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):	6803
Entropy (8bit):	7.874550187496887
Encrypted:	false
SSDEEP:	96:QfQEmGW//k/bZ46fUvcN68na6HjkKpn7QMqQ0xYp28ZeLJgmUrzG+K453a:QoZJAsRkoSn7QHQ0xYp28QMqD4Na
MD5:	581C3ABB51B6386F4AB06D135AFD6DF6
SHA1:	4705B5EB3A5C42B996E325E93903BCE68B6BD1E4
SHA-256:	49A1528F13453079359F12D1F48DA0CEEE9FA351FD28B0E40D547F8A8AE05C6F
SHA-512:	13EE17508F24E9B3EA721F23AC16DF5222C1EC1F5BD6AFEAB1B7042D35B619D4D135CC70CAE5B7446C4BAA2FE644D2C1CD1852EF42D21E3ED2EE68F675B0AB0E
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..:.Y..KVr..%...@....Z*..:...2..V.c).U....zRe"J..=4&GTH.@...j..vJ0l...4Y.<..FE"...D4H:P4..@.V....i.c.).F:.e.+S.....T.@.v4 1....U..:...2...5h.2.....JL.IPP.*...Q...-!.Ki..H.....1...$.i..e<.R.....L....)..... #pq..H..@....f....q.#.@..41.E..S'.I.M#B....Z3..b.Rc@h.>:L.KPQ..HLj#;..$.7b-sN.K$.....rocD....Nv.....'1.....O..A$g....Wt....W!*T.U)\..j...(.....5.G4.B..+S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQY2pC[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):	2518
Entropy (8bit):	7.800027593302025
Encrypted:	false
SSDEEP:	48:QfAuETAAZivGzxzGqFMl2DeUIIMpITJuKUZikaA4VWDTGhMl/w:Qf7ErZiedzGCMl2eUIIMpPKUZvnGhMxw
MD5:	961CC4ADBC5069D0175B35C59B1BCBFA
SHA1:	DDFC1FFE58001EDFCBA0ABCEEB1FB8A7F5318815
SHA-256:	CF38574DAC879DCD52648A1D8081BAD02C495631B6B60B092551B3EB41C13B6E
SHA-512:	55B41C02D2A1FE1FE9D392F337C9E15D26648DEC761BFC6FC6F15FFE10056BE4E5D072FB39AD1B32704298A7F9798861239239A6F9F14D5627F63F02FCFA67E2
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..21.+..d...nx.$vS+.M.?J.t&.....c..X..Ms..fc....+...ml....1...E...6!.=.....A..p.%..:...?..N.....E..mm..A..K.2~...z...G....%.j.[.c .y.....x.Kv_$...r..C .....''..H9Y.,..q...S.....T!2}..@..).....g..xS....y0.....h..0..?.x..y..u.....d.Rj].@-...G]...pk....+..m$~...''.R...~.....kX.&..eu....''....\.,..l..ta.4.....?..U[l....V....?..3..\....QU....^.?.`m...O...D.,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQYCIb[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):	16645
Entropy (8bit):	7.9220255695429
Encrypted:	false
SSDEEP:	384:Ni6Umro7vaAIzcxsnrYeaCBSNKCNdQ4qux7VN1Jjxl:NPs7vaAlxsrrBScCNdQPuzJ9l
MD5:	32404905482653B1A70065F5B805DD6A
SHA1:	98E1E2AD4CF5154C58E33B2C8EDE940E1A555221
SHA-256:	B793CC41F083DF5D954556B95E0E3504160D09E2D3FBD49D631EB6DC1C522C3A
SHA-512:	BB1755FE604C0B49A6E0BC0035314B553A62683DAB08AAB9D445160B4B964A1927E6097564FBB14AA60129821F9187D03A3C90D96B0C7D79CB248FCAB57D286
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....-...P.@....(.....@....P.P.@..%...S...P.P.@.@..%.....P.P.S.(...P.P.P.P..U@.2..R..21.....rA./xO..G({A....P...P..5_.....4r.9:j6.9r..R.es.A{l....d.....E.s!.....V.h..i...r1Hc<....T.+.....f.B.bn.!.h....1(..A@.@.....P.P.@.@..%...J.(.(.....Qp.....@.....Q....h.@..4.....3.@.}....@..p.'...!....9.....9.....J....U}.h...5<.s.:.T..7nx..~.|Z..%B..N ....m..=?CJ.d8]..5..(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQYUQR[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):	11375
Entropy (8bit):	7.955828129737667
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQYUQR[1].jpg	
SSDEEP:	192:QooBASJSgPHYCLUcj8xRltwiQN4eGqAJT9ieCqRfkSPEXkIDsW0n2kEM:bNngg1UdiJ/qiT9JCyk6EXatEM
MD5:	316F6F3F76B391BC23D215A0C5B54EDA
SHA1:	F9FCC03F4BB5E2324496E052084F1B3B224633D1
SHA-256:	EE9267F9A6A2B7C016F3F22E3DE6D9100806D2BEA3E799A6E6B3E1DE4979A251
SHA-512:	9B0B2862F7F47B2ED431985AF9E383A38B1FFD66A030BAEC744D5F7CF7DCD1ACF1AFB56DAD0EABB01D0F242103295CBE6C20F400FE779228447FEAD32F6141 2
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....-.&Zb$....b...M.34.f.....P..D.@Q.z....r[...Xd(l~u.R....fj..H.ok.D.$q....sJO..a....@.....?.t..\|.....f^K7 ..+....^(.....HN..4.V.. v.+...29l_..M.J...EU...j.2J.....[.;.q[Bm.r7.4/..y.:..L...bf..4..h.aT.=E;..(.E.D.LL.P &.#j.a....~4....".LP.[.z+.}2.....x8.....4.+...\|.+f`.....k...I..R...w..n...)l.].[$..Z.NQ>.X....&..H.)..x..D.. ..N.q....zw.h1....W..yw..v.f.3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQYV96[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):	17338
Entropy (8bit):	7.893731201278217
Encrypted:	false
SSDEEP:	384:NtbuXZaE8NBj9JrwXN8l0z9JCX1+N2UpZqP1c7R8o4RBaLGEPt1juetE:NJWJKBj92XNNzOoN2UpY8R83xEXjuJ
MD5:	2FF97BA592E9D23800DC7E7A0ACF4766
SHA1:	ABC540F4692F9376387AA53C4A8A959D6DF9A27B
SHA-256:	3EA36A59A16BBD3D5631810675896B811D491933FC7D90EA89F68E0583556A08
SHA-512:	4E54FCB65106403B5FD3AE2DB1A56063CA646E8EC658A40330194B8804ABCACAD3B5652E14DA61453DEE0060421C5A056F5756B1DD177193905AB71E9537350F
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....q....ICIf9bI.....4.....g.t.b...Z.k.)>.....B.....h.h..p.}.....u..qO.(...&h.9..7.J./.....w.2.".%...5....`....$..E.w-.....\....l.\./.7.. .@.3.@.E,.T.f8...h..|+.u.....y...._....8.|.$k.....;]...[.P6..Rq..3..P...;7O<6.....!...E-.....f.~..GK.x....q.v..ow9....4....Z+...2..{.01..`-..cEE....B.d.nOA...B...Y.u..%F#..z..}i.. \Fb.I5i$"6\.../.L....D.f...K.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQYVTM[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):	7955
Entropy (8bit):	7.901424328402857
Encrypted:	false
SSDEEP:	192:QoLtsDXv+nnAhhafUVnu3iQOwW7tmlv8nat0Hi8l3h2Q:bxsDWnniurXvTGz
MD5:	22E30FA89946E09442BC1F96C58952DE
SHA1:	9B653B0A606F10502F898F230B3CA5B7D4C01D44
SHA-256:	DBEB26E3F9D0BCD30C89DCEE739AEFCE18AB1BA4820EC5E88300113BC9700371
SHA-512:	CF4B24758DFFE360D8FC598313F2FD478038F55330D8E4CBACDA9FF8A29D8CB005C0DF9ECAEDDE7FBBBD894DA5BBBD9E37D5EFE87351F7A5B4959076FE7C 745
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..C.....w..<^. dh$F....q@.w...b..a...|..[m.K5lwV*h..A.;R.t...;...\.Q..n.....`..]...&.T....s.....cOl.,.>.K.].....n}(...E..\..?.5..q 0....].. .4l:.N.#+@..i.....PQqX...N..@..:.....L.;.4...4.;.h.\....).....^?.v.q{..I.....~b....o...j.(O.9..O...xw....)...G.n...?.....YI....}k6.4RLa...0.h.6...#.L.y..p#.`..+"..Jr.....h\....G.O.9;.....4.i!.. :.....X\.....j.1.0z0...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQYvGE[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):	9797
Entropy (8bit):	7.886626214332623
Encrypted:	false
SSDEEP:	192:QtACpQciRVKjnom9jhj51MI1DjRRIl2BAfOmR7VWF+9P:+19omH5GI1DjvDBABxWY9P
MD5:	24332EE9B84419CEBF25BC47D4764597
SHA1:	B4287241284800E9911D49F865CF0A35AC5BE615
SHA-256:	A75D6FD9C924D220D2FA0CFC44BA1CACC2422C9E338997FB09A5D3903C193ADC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQYvGE[1].jpg	
SHA-512:	69B61E3A61E40CF1B92AE4DC070884B5F20DEFA01A62A50CD7E91120CC99026B1966AE316FF2B75F4BD2F59FFC5B62EE26CE713AE40144875EA20CF4DFB58DDF
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....b8P...(....Z.Z.Z.Z.(.h.h.....b....b...Z.(.....(.....J.(.(.(.....@....@.(.h.h.h.h.h.q@...\P...\P...P...(.....%..u&..Q..d.i.....mm....:(.....%qK..+'K.$.$S..)&+2PA.i.(.....J.(.(.....@.@..X...p.....@.(.E.8..\P.....b....\P...@.@..! u4..u...R..I.j..J&E....H]..q.....H.sc...{iT.?8c.....Hc".P.....:R..*..r...?...Dd0.....k..zm...+...6..=P.5...D.....zU....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQZ3BL[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):	2683
Entropy (8bit):	7.843391083264519
Encrypted:	false
SSDEEP:	48:QfAuETADD/FTyLW6VbqT3+Bo0IfW0nkgULrAuMLYoAx+t1ttxF6vY0ZqjQ:Qf7E59qTOBo0IfTkN8uMLYoG+t9xMvYa
MD5:	B99018E40982499D9EF22AD286FF5A40
SHA1:	0F71DC6AE667E0DB2DAC46BE2AE2B5171E7C15AF
SHA-256:	63655C7D65D7BBA8AC738DBE89057517E16D1B841A69FAC9E5377DB245D150B5
SHA-512:	0A504BEA756104D8B93A7408CD457990EC2E5CD9C492ACB194A7EC93C6B178408FA128438365E773E94D30A64AF136B39F7831B2E24DEBC84174721ADC81506
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.}...,I2..V.WW@.....fR...j..6.B....7..NO.l.r.s.b=I.....T.tz\|.....'..4f.....!"(FX....Q+j]..zp%...c.N0.....V.3D.4@/`y..W*0.=.I.....M."...>..m.....on..rVW..>.,.F.\7.{..q....D.2.....`.z-n.....0Ap0.....q.wp..g.jT.b.;.....$.1..0.eH?....A:n..n....].2.FW.#..Fv..4."..K.u%.{H...d...k.....H.c.q.3%}.s.:(ni._ciC.0....ec..r.&X....4.ao.D..H..h.b.}....X... .....>.or..K....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQZ8Vf[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):	14421
Entropy (8bit):	7.950549145259091
Encrypted:	false
SSDEEP:	384:+lNQ9VvBWTS9lNbqg6g+zpxl/hEMogWA1Rd:+l69vWm9lNbqgCzYMogp1Rd
MD5:	4CDF1B0F18E191572E33A6112206E49D
SHA1:	872C8ADD0FB0B043C9349A179786BD85A6311F01
SHA-256:	DCBD8C0E4067D0186E12435A009F7CD00EEF6168871BCD26CB8ED317DEC384ED
SHA-512:	A02AA8F7C33AD9611D6BAB4455D80BB862718267FAEFED8764FA47E1EF1B4360B7FDC506C87C7BD1FCD3EEF2BD17476582EFF45C19F79D0330F29365EF471FD
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...\... ..(..#...E.. ..R!..LA@.h...(@..3.B....?.&.J...a?.k.gHS.....)..P41.4fy.v...Kr..*&....uS..O.E.&O..A.t..{Qr.$.3.....*...88.5\.'..E..A,1@."...`.....?.....wa ....Z.J.Z.&h....K.>....Q.P{.1..{T.MJtt.....9.i...gG..'.>.d..R.Z.,..(...Bb....L.....pO.....z8_..:E...(....."...{E.<.O.y..QD.....<H.)o....9....:.tF....p..,.c.+.&o...m..,z.J....sm...q....-Q..J.E.....(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAud6Gv[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):	356
Entropy (8bit):	7.101459310090333
Encrypted:	false
SSDEEP:	6:6v/lhPahmpAKG4NDBbCySVUc3/qF9Hio9hbifyZQw+bS2LblMid1Rc9ruhiFp:6v/73bCLVYHio9h8kQw+7BMW1W9rAir
MD5:	A94D5FFB98CBCA323E6AEA6A826B9ACF
SHA1:	D4F20C419292258A27A06511955A02400C767723
SHA-256:	7527C0E97B871894A7AC475D714D51E82F51BB965848DCD03657B12D5808BCAB
SHA-512:	D2B0D68C085457161F612B50508548D9FD6F7F48DE74AEC8009C65375A0CF0D58469BC8B93AC2705B4AB4A0F0D3FE07E8207500AD896FFC676D7D50649643A7D
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...j.A.....A..y..X....$.E.'.b.:.h!.bc%...:.FlD..L.@:...F...o...u..+.>nvf..v..n.;08..<.,C....-|A.x.D1.Mx....B.R>.....3..d@....%....v.Z...5.C....3@.a.[..iku.....%.(....p.h..m.](..s>F.&...q.^..dH.....0<a1...4. .z.Q.@<W...,...4..?M.b.....@{X..L..x...|:.B..B..K...j..k6/..LE@....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1ftEY0[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.316910976448212
Encrypted:	false
SSDEEP:	12:6v/7YEtTvpTjO7q/cW7Xt3T4kL+JxK0ew3Jw61:rEtTRTj/XtjNSJMkJw61
MD5:	7FBE5C45678D25895F86E36149E83534
SHA1:	173D85747B8724B1C78ABB8223542C2D741F77A9
SHA-256:	9E32BF7E8805F283D02E5976C2894072AC37687E3C7090552529C9F8EF4DB7C6
SHA-512:	E9DE94C6F18C3E013AB0FF1D3FF318F4111BAF2F4B6645F1E90E5433689B9AE522AE3A899975EAA0AECA14A7D042F6DF1A265BA8BC4B7F73847B585E3C12C26 2
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\4PB7FJMT\BBMW3y8[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):	407
Entropy (8bit):	7.260473594371947
Encrypted:	false
SSDEEP:	6:6v/lhPahmIkCDxHtNgQw6jve9sKu7oaHrKUXNbjjYXJlq2iyoyXnZV1tGB18aMeX:6v/72kOHYQNW9sKuLdNDwbtoyFtgKq7
MD5:	08BE52491E3B8D2BA30C5110FC4B3FF3
SHA1:	E311FB3A1E1EAFDBD0F967F1AEAA0D2A1CE302C8
SHA-256:	C67293877308BB292365B4CD71577F670519822E98ADE59E21C44AEE14729468
SHA-512:	16A2802F1A280A9281188BD036FB53120146C2B9330C651ED65F7BE531A9D111AA8727C4F6971B4CD5FBE60C05F4874E81C1C881F03512E3C087710F96217816
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IIDATx...O+Da..'f....g.O..(...(R..)%..."[..Bd....a...2.l...9...:..y.y...s.{..?....k....p.;...p...')....;..8..J$.....E/..P...aA.o...>c.i.a...o0e.. Zb.3.<...._.~..~.,@.'..L.....i..[...AC..C.(.-i>E..P..v...u5..E...,...r..f.-...|X..~4x}<.M....S.../....U.B(.....D.>....t.6.X.F]...'._.gq.W.R_..{..x..M.)27...RT...@.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBUZVvV[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):	415
Entropy (8bit):	7.093730449593416
Encrypted:	false
SSDEEP:	12:6v/7C7Stjm5n9HPBQrd/9a5cFWziVYbALUO1:BAm59irna55uYMb1
MD5:	16B34C1836A5FC244145527EC79361D4
SHA1:	18CB908457B380545D89D8A4D3F91CDABF3ADC78
SHA-256:	DB797DF4F1E320C21BD6019E89E6CCC5569C5CED57E1D3BDD736F3B4A9371BC0
SHA-512:	3FFFFB5F6876B8C246F2728A3AEA8EDF2997032F8CD9CE375497D8063939F810BB819E4CDC56B1ECA5E8A70B27E7355C2A9B7F23BDF8919307F01536008D4D7
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....QIDATx.cy.(.....B.^.V.....6..OD9... .b..1.o.c.y....v.+..sK..>N.....W.... .....aL....Z..<I.`..ek.~.<.W.....`..O..~C. .....%. .3.. 1..~....h(...[...}...u.J.....&=..?.....aa.....r...;..4q..3....[.....q...];.^^se`...K..6..UK...X..)..k;...X.U..2....0.....f.t.....p.....[]..n;H...P ..va....'..N.....!.....).&O...Fqo.%.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBVuddh[2].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:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C1 3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBVuddh[2].png	
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\4PB7FJMT\BBY7ARN[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):	779
Entropy (8bit):	7.670456272038463
Encrypted:	false
SSDEEP:	24:dYsfeTaIfpVFdpxXMyN2fFIKdko2boYfm:Jf5ILpCyN29lC5boD
MD5:	30801A14BDC1842F543DA129067EA9D8
SHA1:	1900A9E6E1FA79FE3DF5EC8B77A6A24BD9F5FD7F
SHA-256:	70BB586490198437FFE06C1F44700A2171290B4D2F2F5B6F3E5037EAEBC968A4
SHA-512:	8B146404DE0C8E08796C4A6C46DF8315F7335BC896AF11EE30ABFB080E564ED354D0B70AEDE7AF793A2684A319197A472F05A44E2B5C892F117B40F3AF938617
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.eSMHTQ...7.o.8#3.0....M.BPJDi..*.E..h.A...6..0.Z$..i.A...B....H0*.rl..F.y:?...9O..^.....=.J..h..M]f>.I...d...V.D..@....T..5`. .....@..PK.t6....#,.....o&.U*.lJ @...4S.J$..&.....%v.B.w.Fc....'B...7...B..0..#z..J..>r.F.Ch..(.U&.\..O.s+-.,]Z..w..s.>.I_.....U$D..CP.<....].\w..4..~...Q...._...h...L.....X.{i... {.. &.w.:.....$.W.....W...''..S.pu..').=2.C#X..D.....}.$..H.F}.f...8...s..:.....2..S.LL..'&.g.....j.#....oH..EhG'...`.p..Ei...D...T.fP.m3.CwD).q.....x....?..+..2....wPyW...j.....$..1.....!W*u *e"..Q.N#.q..kg...%`w.-.o..z..CO.k.....&..g..@{..k.J._...)X..4)x...ra.#....i._1...f..j...2..&.J.^. .@$.`0N.t.....D.....iL...d/.|Or.L._...;a..Y.]i.._J....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28
Category:	dropped
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A57 40EF7
Malicious:	false
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e. ....Q... ..-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,.A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.t]S.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.I:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....\|~\|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otSDKStub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19145
Entropy (8bit):	5.333194115540307
Encrypted:	false
SSDEEP:	384:7RoViYMusfTaiBMFHRy0I2VMwG4JRuIKBf:7aViMsffBMnktf
MD5:	0D2A3807FB77D862C97924D018C7B04C
SHA1:	9D17F3621001D08F7B98395AC571FC5F6CDA7FEF
SHA-256:	75DE71E7FEAC92082AF2F49B7079C0B587B16A5E2BB4DABDA7E7EB66327402FB
SHA-512:	409ABCD5E970CAFF9F489D3E7F3D9464B2C5189118D2D046CA99E42CEC630C2C65B30397B8A87C3860E3426CF9F7E0A5F86511539CA9D9AEDA26C74CA90559
Malicious:	false
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,A,b,y,v,C,I,w,S,L,T,R,B,D,P,_,E,G,U,O,k,F,V,N,x,j,H,M,K,z,q,W,J,Y,Q,X,Z,$,ee=new function(){ this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTru stIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation", this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]=''Unknown",o[o.BannerCloseButton=1]="BannerCloseButton",o[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\tag[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\tag[1].js	
Size (bytes):	10157
Entropy (8bit):	5.433955043303664
Encrypted:	false
SSDEEP:	192:4EamzdxOBoOBpxYzKhp5foeeXwhJTvlXQuzSqH3wgiKGWdrBpOIztlomlRokr:4EamR7OrxYSLQdiMoH3wgxGWdrz4+
MD5:	DDFF3756F9EFD3A46CF3325875D813A1
SHA1:	05D238659959B28B786CCE43E9E55A728E69428E
SHA-256:	E80C669818773959643790269ED9448F71BD45D27D61FAFD73BC44C0F40BAACD
SHA-512:	7E6D325A705718D0B4060BB4A2FACC538B3812B5767CBEF9F15F787C20EFB492F9E72F8F4B215A3C4D4F684236F49D80C37597E2C13F9B482C3CB441B6CA574
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\B87Z87FM\AAKp8YX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.3622228747283405
Encrypted:	false
SSDEEP:	12:6v/7YBQ24PosfCOy6itR+xmWHsdAmbDw/9uTomxQK:rBQ24LqOyJtR+xTHs+jUx9
MD5:	CD651A0EDF20BE87F85DB1216A6D96E5
SHA1:	A8C281820E066796DA45E78CE43C5DD17802869C
SHA-256:	F1C5921D7FF944FB34B4864249A32142F97C29F181E068A919C4D67D89B90475
SHA-512:	9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929E D
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..S=K.A.}{...3E..X.....`..S.A.k.l.....X..g.FTD,....&D...3.....^..of.....B....d....,.....P...#.P.....Y.~...8:..k..`.(.!1?.....]*.E. '.$.A&A.F..._~.l....L<7A{G.....W.(.Eei..1rq....K....c.@.d..zG..|.?.B.)....`.T+.4...X..P...V .^....1..../.6.z.L.`...d.|t...;.pm..X...P]..4...{..Y.3.no(....<..\l...7T.....U..G..,a..N..b.t ..vwH#..qZ.f5;.K.C.f^L..Z..e`...lxW.....f...?..qZ....F.....>.t....e[.L...o..3.qX.....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAPwesU[1].png	
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.e.{L.q..?.s.]uq.H..)QV.J.....56.f.I..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\B87Z87FM\AAQXYTC[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):	15021
Entropy (8bit):	7.958178636194347
Encrypted:	false
SSDEEP:	384:0nPwNOhvtkC6iiObfavSGWYW2TE7LQ4ufG/:0Pouv5J1XYWn7Lnufo
MD5:	B46948E466B8C06EB01FE100980D95A8
SHA1:	CDDAF977E936D0C8674C23ACC65FEACF95BB48FC
SHA-256:	2CB891436C9947EE9587F462262C11DB39F52EF2F163B4709ABCA2DE14CA00DF
SHA-512:	3340EBA697438C0DCD993E53F58AFAAA3DAF5340EC98814FA27695EB2B4611A50B5E1F56426E1FF2D7217FDC0FE160389B14BFE9504CC2319C0C3AF270519C3
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...E..qqex.e.J.....^.....v..5r..;*.D..03....H.[}7L.n~.i...\..fO'.....-...../b...i...Gs8H....H.9..'..Kcec....'.su.F....N..|.Q./+Cr.,dB.C.....%g .;....0.I.`.....El..4..97...?..sR.....0.(.....h.U...;....*J,'.:R(.....s....T..\..1.....3...s.S.-.=)...U?..q.Gj.[.a{y..7.>g#...J...9;#..@-#..p.n.v6A.....EG.]...[.....@.2..%Q*.....,f5.B~da...4 X.e\xz...F...&...?...c..WZ{#..r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQY08U[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):	17094
Entropy (8bit):	7.9461517554041174
Encrypted:	false
SSDEEP:	384:NftBCoV+WftvCbYDQUCy23Q810x0f8EBfR/zRjq3kXg:NfzCoYWf9LDXL2n1WpExVoUXg
MD5:	075E7FB657B601F6173D6FD71F4FFECD
SHA1:	0BB816D1DA102C0981591098B48197BEFF78E330
SHA-256:	CF753FED6493B9709DB05FD542FABF1178821008436BA98D0B60CD31B71944C4
SHA-512:	668E726711E304D53641AF4BEC10439CB8B5AFCFEFA5299B0A23D5D0D56C3A759ECCE22B1EC92E1B4AEF8CF6E107C0A6703A2A1C5C5C6D21EAD3C8B2A630D 00C
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..bF.....7..p.....\,4.W..{v#...u.r...bf./J..*....B.tV..4....=..\@.Y3.].HY'....U..SQ...y5.:z...%....9\....^.....[.L.....'..1u...\|.....J..Z.[...k.A#.Tl.K.A.F*$\..>...Z...0.N]{.M=.*I...h-Qd...3u.n.....>..nn....i.HSW(...S...E.fiy$.I.i$^X.P.)...8..dF.....(..LA...ks.v...q.....r)E....e...}'./p.(.'Q.:alu.{.K.#>J..*.I&h.....\i..G.+x TR9.Qq..7^..f#....$N..T.i7..iN..l.7..l

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQYPIL[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):	30202
Entropy (8bit):	7.9697259072009565
Encrypted:	false
SSDEEP:	384:NrAlHZj6NO4ZVIm4jqRsXXefTPYZagdwN9SwLyq75baiozlHFT5xM4uYG7UHVyKU:NrQ5gVhpma3BjSwWqVai0Tc4ZG+8KU
MD5:	660992F97B2E1B2C2CC645FD9976E2E9
SHA1:	BDAB06368143FD3C6CD15CCB37D6F9FE08BEA10A
SHA-256:	1168F6445B43B458C9AC9AC37EFC8CC8CA1FAF3921AC325D59A109990602411E
SHA-512:	6679437963115840D91F8C9B8C820CC7C3A3E2F0C8014951C56A137EEB971CE4ED229FBDFBA1CD8E99F01D121D0A541C62EBECEAEFAAEA23F567A2F85EA02A 70
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....,.....z.Xn5.k.|.b.....h.C...vQ+pq..)]1.60.(..fI...r1..).....O.P.do{.....k....V..d.4r.qe.....3hE.dbc.$.....',...8q..O.T..r...0. .T..$>d/...o....z~.Aq..h;.}~_../e ...7u..S.4:R.....W..e%E.....4...4.v./J=.....\|{\z.M.w.7..@.B...`..Dc....{.wA."...%.}...Vb....3...T..r.....s i.R.8...4..C#...g.....7...G+.!c$...o|. HD.Y..>={P!Lj:...LDeS<...*,=C.#.X...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQYSOX[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):	4803
Entropy (8bit):	7.556207184129386
Encrypted:	false
SSDEEP:	96:QfPEQqAq7qRbq3PKvBeo2s1vWjk/e1O3AJks243A6mJiGanlXqzC5SyMOtus:QnlqAqaq/KvBeoujrO3ATtA6mxMNMOtT
MD5:	3DF85C786B813129767F7FF5ADF90AA4
SHA1:	013AB07FAF3987577A1460A8A1828CF664A96EBE
SHA-256:	0AE595E15AF96C595342EBCCE0852AF325CDDE20498902577CEC009EB055CC08
SHA-512:	DF46FB9345ACF98956D0453FAB3C7D0BC73C9C54B412CCCCDFF1CCC9A72AE048473CAF70398CDA8287FFB2FAE7A2C85C14ADE79D35FBF68997E6A3AA752B02A
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....(...@....P.P.@.@.....P.@.....P.@.../.Q=....dj.h.....Bh.....@..A@.....S..4\.....jd..S.....(.(.....(.(.....#..'.Q=...3J..J.Ec}MM0.q..3*Hq3....oR..f...!.....P.q@...LP.b.....P.M.%.4..M.lV.!L....(.....(.....(.(.(.....".'..Ob..^...V.....t}+S...."O.f.4[....L.....M.%.!....i4.m..h.f.1..(.....(.(.....(.....P.@.@.@.@.L~x...TOb..^..=...v....6S..V.%W..]'.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQYULr[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):	15081
Entropy (8bit):	7.927000529392556
Encrypted:	false
SSDEEP:	192:Q2YieBOy7JVvGCT+6qjts0SvtL9pduhgn6DW2pzJBLR3puz1tm+R2DYETmJ2BkTc:N14vlVvGQqjiPtLnVn6DbQzJRpctkzPU
MD5:	985B1868C277EB8E85D1F7B4091E5208
SHA1:	A5DAFF826FBA9DA1E82449FBA9525E8FED1403D4
SHA-256:	B226C1C7D78988AD3704A3D33C7B925E4B4E6484FC047ED7B1CB41E0D92164F0
SHA-512:	E690DEDD645409BC1B7C3E7EAF2B7BBE91DF1ABDA500EFA94F4600323BE8AEE9018149E90D4FF006F686A5851600CA41CC340E707B9C4C32ABE349E20219BBCE
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....@.4.....*;.}...5.6bZ30`.$.=..I.....S]Ks}.b.v...t....dr..'M....C"..qes .SF@..JS%..q...k.I`.....F.!..s....`...t...lk.b.....=dV.I.N.sY.f.ldx.m.B1..*.nMg..xt`8...M=....P..&[.....BM.F...v...0.A...D.FM.....kH..R]I.P....^.q.`..3U.....:Q'f...mV...E)4.h...Xi.*..C1(.(...@.@..3)...0..&..R.JR..r...\\1B.=k...2.....>d.Fj...U.$Tu-$(E._.Xx$....d..?..d1..m4.%.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQYrvs[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):	57864
Entropy (8bit):	7.965834432074916
Encrypted:	false
SSDEEP:	1536:I7jBu/EAaNVi2vSfyhS3DKLgEOZdaEowJaIQyU:J/EA8bvBhcejiawJE
MD5:	95E5BA42BB2806777D34F8088E3503E1
SHA1:	F3629E9573E275BD189EBBD8265AD8764BF5EA5A
SHA-256:	0E0D14C14F1FEAD0881F0F8C8A5290EBE106BD5DF2489FE3BE830AB60BAAFFB7
SHA-512:	C7C36196A0C8669E257C65520A3962BD8CD024DF4C93E0481D99996F754303D712AE8F524A2DC6C8DB7D0CAA223836FADC33DEDEA6421CE81DD495CBBC989A
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....(.l.\W..c6'1...>..!.....ESb..H.$.~..!...[.m.....J.H....=+*r..Cf....f.:..;.a5b`..Fkd.n!4..g....3.=h.3@.h..h..<..f..v....'.Lw....]l....f...Yp..2T.H.v@..ar&.....%!..`>`.....#.....+X..C..$....M+.E..dPA.2...%...T6..4\l..<.M.RpH.!....0.![....\..#>h.R.a.....'q...R..-F!....[...Q..Y.6$A..+...3j.).fr.2..'';..$..k...SL%...cE...#cx.T.}.....3..'>...b.$k.Tt.zU..+....8&..:E.7t.p.....4|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQYvQT[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):	35815

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQYvQT[1].jpg	
Entropy (8bit):	7.953257870398609
Encrypted:	false
SSDEEP:	768:luAsX3YrnxKgwLWrruWvpSlHTO7X/ic8jNl6IXd2n5c7cLultlkILil/CW:I/eljxBruWvslzxceNlQaBUkILTCW
MD5:	946D24C5A984175C65F10663AF925A36
SHA1:	6731589DB3B2F2B71D7A550881A032601D48F80F
SHA-256:	062D6AD349BF4475B181B91AB1C5FB4904B6509C33F841EC93DC6669778EDBE7
SHA-512:	1A3D43D7803F594A46B048B5A829E265822AF44E60C0467CECFDB4086CCF149254BDF2A42A5BCD4BC644277362F6584E537CFE0470A34FE76DF5FEFAF1071B1
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..W4.j.....:s.....-.B9..i..5..r....C@.GU[.7.ps...32..+..A..U_.Ou4...(D.L2c'..b9.x..C&..^..F..i...k.Y-.3`0.L...m.&D#fz.@....]..%s.G j..q....W.i....G...C54.=..<...4..s.L.|Ro...W.....h._!...}s+.X...7.9..}...mi.K..4.gh.h..p.P.&....%D...~Q.@..@..FM.Uw.....7.....l.....+.....rs....zT.....@.b....p.....@....h.3q.?xP.}. ~...CU.%.a..2l&.....C.u7P.!.8.....j..$.D..Pi4.8mA.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB10MkbM[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):	936
Entropy (8bit):	7.711185429072882
Encrypted:	false
SSDEEP:	24:IJJuYNKuGlZLocJZlxAgAbiuoSrZzi1g3+:IJn94F/lxAZiuoSNYgO
MD5:	19B9391F3CA20AA5671834C668105A22
SHA1:	81C2522FC7C808683191D2469426DFC06100F574
SHA-256:	3557A603145306F90828FF3EA70902A1822E8B117F4BDF39933A2A413A79399F
SHA-512:	0E4BA430498B10CE0622FF745A4AE352FDA75E44C50C7D5EBBC270E68D56D8750CE89435AE3819ACA7C2DD709264E71CE7415B7EBAB24704B83380A5B99C66 C
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....ZIDATx.m._hSW....?....E...U.Z.M..a.1.}P..6+.....l.....LDA.....u.a.U..P..&k..Iz...&....R_.q.=p8....~.'...5..}....._.I$FS.\.c][4#... .....+...U@fZz.Y.....|.7....r.x..S.?.ws....B9.P.-Yt*..N.}.'V.....G...5....uc....XV.=.{..ai.pw.v)...(.9.z\|.3:Q..,qr.es...ZTp..Mt.iB.2.{w.C*WB..F...b../.H..\..*.).0l.R.....c.....@S5.? 3...q..:..8.?....p.=6`..T...5.nn.....]..b.j.,..pf.....8...".M..?.@K...L.='.1.O.2Kb.p..(..\.D.....n..._.....0.....w^bR....v\..)..l..f..l..M.m.6t.7....U.Y3?.h=..!.<.._.....pL..V"[..... {[P....e07...Wc....IH.T@...*..A@.....;....>Gt&...}...o...KP...7W1.sm~...&.....00.....>/....I.#.t.....2.....L_Owu.*.A)...-.w.*.1/+.)....XR.A#;..X...p..3!...H.....f.ok;..\|x..1.R.\W.H\...<.. <&.M!mk:\|....%.<..,.%.g..g..G@z^Q..I...T.D^..G.&v6$.J.2J....~..Y\kX.j.....c.&.>.3.....ek..+..~B.\.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB6Ma4a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	368
Entropy (8bit):	6.811857078347448
Encrypted:	false
SSDEEP:	6:6v/lhPahm7HmoUvP34NS7QRdujbt1S+bQkW1oFjTZLKrdmhtIargWoaf90736wDm:6v/7xkHA2QRdsbt1pBcrshtvgWoaO7qZ
MD5:	C144BE9E6D1FA9A7DB6BD090D23F3453
SHA1:	203335FA5AD5E9D98771E6EA448E02EE5C0D91F3
SHA-256:	FAC240D4CA688818C08A72C363168DC9B73CFED7B8858172F7AD994450A8D459
SHA-512:	67B572743A917A651BD05D2C9DCEC20712FD9E802EC6C1A3D8E61385EB2FEBB1F19248F16E906AF0B62111B16C0EA05769AEA1C44D81A02427C1150CB035EA7 8
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\B87Z87FM\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB7hg4[1].png	
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\B87Z87FM\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\B87Z87FM\checksync[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):	21717
Entropy (8bit):	5.305602492520896
Encrypted:	false
SSDEEP:	384:fuAGcVXlblcqnzleZSweg2f5ng+7naMnpuZOrQWwY4RXrqt:A86qhbS2RJpusrQWwY4RXrqt
MD5:	677C48207F5A13E6D6DADF30D2D6C52B
SHA1:	10BCE9871F228CA247E92B0A6366D5FE2A4426C8
SHA-256:	16872C9C9305146F1665B47C30EAF0AF695450B80E6B659781C71E3B45526027
SHA-512:	7C35E7BE4917DEF18676DCD367EA060F9073A093D9B66D6104784845E8B3AA3C14846F617661384E9A4F07E9FE149156A0C54DBF1030CBB4ED972CAF5F115CF
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime" :"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":"data- bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cook ie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx" ,"csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm"," som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21717
Entropy (8bit):	5.305602492520896
Encrypted:	false
SSDEEP:	384:fuAGcVXlblcqnzleZSweg2f5ng+7naMnpuZOrQWwY4RXrqt:A86qhbS2RJpusrQWwY4RXrqt
MD5:	677C48207F5A13E6D6DADF30D2D6C52B
SHA1:	10BCE9871F228CA247E92B0A6366D5FE2A4426C8
SHA-256:	16872C9C9305146F1665B47C30EAF0AF695450B80E6B659781C71E3B45526027
SHA-512:	7C35E7BE4917DEF18676DCD367EA060F9073A093D9B66D6104784845E8B3AA3C14846F617661384E9A4F07E9FE149156A0C54DBF1030CBB4ED972CAF5F115CF
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime" :"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":"data- bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cook ie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx" ,"csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm"," som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[4].htm	
Size (bytes):	21717
Entropy (8bit):	5.305602492520896
Encrypted:	false
SSDEEP:	384:fuAGcVXlblcqnzleZSweg2f5ng+7naMnpuZOrQWwY4RXrqt:A86qhbS2RJpusrQWwY4RXrqt
MD5:	677C48207F5A13E6D6DADF30D2D6C52B
SHA1:	10BCE9871F228CA247E92B0A6366D5FE2A4426C8
SHA-256:	16872C9C9305146F1665B47C30EAF0AF695450B80E6B659781C71E3B45526027
SHA-512:	7C35E7BE4917DEF18676DCD367EA060F9073A093D9B66D6104784845E8B3AA3C14846F617661384E9A4F07E9FE149156A0C54DBF1030CBB4ED972CAF5F115CF
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":"data-bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[5].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21717
Entropy (8bit):	5.305602492520896
Encrypted:	false
SSDEEP:	384:fuAGcVXlblcqnzleZSweg2f5ng+7naMnpuZOrQWwY4RXrqt:A86qhbS2RJpusrQWwY4RXrqt
MD5:	677C48207F5A13E6D6DADF30D2D6C52B
SHA1:	10BCE9871F228CA247E92B0A6366D5FE2A4426C8
SHA-256:	16872C9C9305146F1665B47C30EAF0AF695450B80E6B659781C71E3B45526027
SHA-512:	7C35E7BE4917DEF18676DCD367EA060F9073A093D9B66D6104784845E8B3AA3C14846F617661384E9A4F07E9FE149156A0C54DBF1030CBB4ED972CAF5F115CF
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":"data-bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\de-ch[2].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	79097
Entropy (8bit):	5.337866393801766
Encrypted:	false
SSDEEP:	768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B
MD5:	408DDD452219F77E388108945DE7D0FE
SHA1:	C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7
SHA-256:	197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385
SHA-512:	17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB1B
Malicious:	false
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\iab2Data[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	271194
Entropy (8bit):	5.144309124586737
Encrypted:	false
SSDEEP:	1536:l3JqIHQCSq23YILFMPpWje+KULpfqjI9zT:hqCSVyIeiijq
MD5:	69E873EC1DB1AA38922F46E435785B61

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\iab2Data[1].json	
SHA1:	0E17DD5D16C19D40847AEEEC9AF898BB7F228801
SHA-256:	D90C45999873C12E05B6A850C7C5473E1CB3DA9BD087DB5F038F56ABD65F108C
SHA-512:	27F403FDC906C317F4023735B29ABB090867CAA41103CE2FD19E487323EBEE15884DF10A353741C218BB83C748464BE3D75459F5D086FDE983DB85FC86ADA4D
Malicious:	false
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with your online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\nrrV52461[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	91348
Entropy (8bit):	5.423638505240867
Encrypted:	false
SSDEEP:	1536:uEuukXGs7ui3gn7qeOdillEx5Q3YzuCp9oZuvby3TdXPH6viqQDnjs2i:aKiw0di378uQMfHgjV
MD5:	9C4A60B2332E94D3BFF324BD8DF61A31
SHA1:	6245D60C273E175D3EC798CE8ABB65AD75F24E09
SHA-256:	8C38115211EB4E291CE6F38629C8AEE0F882EBED06B66F3DB3D6587C1EBDF52F
SHA-512:	31830D8DE79206C5C5B178DBC798D3A2AF597BA14D9075EE25CC82B096083B180B0B41CB5DC24640AC2A8329575102A3D724DA1F4307DDFB57DBC5C64A8738
Malicious:	false
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\B87Z87FM\nrrV52461[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	91348
Entropy (8bit):	5.423638505240867
Encrypted:	false
SSDEEP:	1536:uEuukXGs7ui3gn7qeOdillEx5Q3YzuCp9oZuvby3TdXPH6viqQDnjs2i:aKiw0di378uQMfHgjV
MD5:	9C4A60B2332E94D3BFF324BD8DF61A31
SHA1:	6245D60C273E175D3EC798CE8ABB65AD75F24E09
SHA-256:	8C38115211EB4E291CE6F38629C8AEE0F882EBED06B66F3DB3D6587C1EBDF52F
SHA-512:	31830D8DE79206C5C5B178DBC798D3A2AF597BA14D9075EE25CC82B096083B180B0B41CB5DC24640AC2A8329575102A3D724DA1F4307DDFB57DBC5C64A8738
Malicious:	false
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\B87Z87FM\otBannerSdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	325178
Entropy (8bit):	5.3450457320873355
Encrypted:	false
SSDEEP:	6144:7Kk89fToixHtGt3mBC4VcW3fUAbJ7Kz0yzGO:acixHMPzfJ
MD5:	56B5E93BFB078B9EEF2BA41DB521EA9B
SHA1:	A61A4949BCBCA6B8148CC6821D7CF88FBD90062F
SHA-256:	B8603101616C7960752244D2EC66D2A845BBE0094B83E7CC2877880A3A93402D
SHA-512:	C10E26F5C9B66E1FA82926AD43C7C70EDF00D3BEBE376DA674B325FB34EDB47EDF490BF84457BBC085BBFA1AF37D92F20067AA46B1334D623D2AE80B66810C02
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otBannerSdk[1].js	
Preview:	/** .. * onetrust-banner-sdk.. * v6.25.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){"use strict";var o=function(e,t){return(o=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(e,t){e.__proto__=t}||function(e,t){for(var o in t)t.hasOwnProperty(o)&&(e[o]=t[o])})(e,t)};var v,e,r=function(){return(r=Object.assign||function(e){for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,l,a){return new(l=l||Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l(function(e){e(t.value)}).then(o,n)}r((a=a.apply(s,i||[])).next())})}function p(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otTCF-ie[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	103536
Entropy (8bit):	5.315961772640951
Encrypted:	false
SSDEEP:	768:nq79kuJrnt6JjU7cVbkhS/G+FBlTjmSmjCRp0QRaPXJHJVhXKNTUCL29kJlXYoXY:49jht4bbkAOCRpl6TVgTUCLBX10UU/px
MD5:	6E60674C04FFF923CE6E30A0CD4B1A04
SHA1:	D77ED2B9FA6DD82C7A5F740777CC38858D9CBDDD
SHA-256:	48221F1DE0F509D6C365D9F4BA1D7DB8619E01C6BC4AC8462536836E582CDC66
SHA-512:	62F5068BDEDBA361DAD0B50B66F617A2A964B9D3DB748BF9DE29C4F6307B1891AF9A4D384F3CEB25C77B62D245F338D967084301391A41BAB9772E2632B36B9
Malicious:	false
Preview:	var otTCF=function(e){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function t(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function n(e,t){return e(t={exports:{}},t.exports),t.exports}function r(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return I.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return L(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\17-361657-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F
Malicious:	false
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.localStorage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c.data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("office")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-dependent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\55a804ab-e5c6-4b97-9319-86263d365d28[2].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3278
Entropy (8bit):	4.87966793369991
Encrypted:	false
SSDEEP:	96:Oy9Dwb40zrvdip5GKZa6AyYs9vjxWCKTS2jQt4ZaX:zqlipc6vxLCSCbZaX
MD5:	073E1A67C16B7E2B0F240F20BAC53174
SHA1:	778663FBA0201814BE193EB38E4F9D8875F322ED
SHA-256:	886E0D5D43DFB17D92EB8C5C80AB0671ED9DE247EC4AD9D71B358F32F7613287
SHA-512:	97FA869A8BE850E759BDB5AAA0E850B787358CC4EED55796F6B51D1AFD5B6B25CF7A6FAC5FCD67AA9588876F208D40449ED94886046177B6FEAA083743B0169 6
Malicious:	false
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":true,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","gb","ws","gd","ge","gg"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO 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\NUEPGTR9\AAQBdIv[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):	22371
Entropy (8bit):	7.7949964619592285
Encrypted:	false
SSDEEP:	384:IY3asYjHnqTeXCnV+vWN8ZiadjNBzJNCGNFq/NFfqoY7mZdd+f0naWx:IdHnmeyI+yi6NB25/NFfbFJnP
MD5:	F4B452436A19591E7C0ED1A7916B9259
SHA1:	5BA326F2E57A89A106689E4EC00B23D30AAA9DBE
SHA-256:	B13869EEC4400F3BDE2DE2F864E786ACC568D413FDA7FC619FC4AF87E6328B5D
SHA-512:	313B26FD6A8C652B5AA50EA698B070D324C7A0B8A202BEF0A1A87EB3ECB633BD0DD9CBD574598F107A4374FCA6FA2ADAB1DC028EC5446EBDD402B044D325F 90C
Malicious:	false
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..:.(......(......(......(......(......(......(......(......(..........b..P...1@.(.(......(......(......(......(......(......(......(......(......(......(......(......(......(......(......(.h......(.(........(............(.....P.P...(.(......(......(......(......(......(......(......(......(......(......(......(......Z.(.......b...J.(.h.....P...P.....A@....h..#."....1@...(........(......(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQCmUS[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):	31947
Entropy (8bit):	7.892422553435186

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQCmUS[1].jpg	
Encrypted:	false
SSDEEP:	768:IaBjbh6TFQqvZ54il2R40NXypZfdvRB+6KCOfH:IaBXOQqX4igl4zZRB+ffH
MD5:	62A8482CFB648DD0D95E83D2B22FAE7A
SHA1:	D6F0CD6A1834A60F4C5994067CED244E2E921FA8
SHA-256:	8361D066356EB990AF5B6D5E6A77225982A6B40D3BCA809274FD3FB40F6FD92D
SHA-512:	A6834B4CA196B46432AA31C5A5F0EC16E41852C2A2D7D09C3374CC942795DC4A0A958C7DC72DA6FFFB6A437462AF67C75FC01FFABFC9565A7EACB0C9F9DE2B3
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...]....4K.T.bcpM.....*S.&.j.P....(..h.v...P....c..;.P!....!v...P!Yp(Bd{y. .@.m10.@.m.&.....p.0...\P0....CB.(....C..c.Hc....@.(.).Hc....I...H..)..).x...).....I..R.@...@...\P.....@...p.Lx...b.(@8S....@..-.(.A@.....Z.(.....@..F.5H.4.E11.(..h.Qi.1.i.pJ.v...h.6.1B..pC@..s@...0%T.....S.....LM..LP ...(.@...@.P1v.).....P.....HhxZ.....).....$..C.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQT0oN[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):	49430
Entropy (8bit):	7.968250182302868
Encrypted:	false
SSDEEP:	768:ISMx6UYVvLG0DAyhz+1V+dqheEiic7giJRS8p3BDvaUj5OeGWFxl4e2fxgspTlQ/:ISMsUYVHbmEdqheH/gRkvaUNhGeke+zS
MD5:	778D5F7FF643535754426B22D1655699
SHA1:	033850198C0E81418CCF29ADAEA98D8814AA5F96
SHA-256:	79E97D0F92A1E054FE44AAD7CDBF21C2D918DF000B9C0DB374DC3B186AA212C1
SHA-512:	B5C228EC6033866669A7D3B36FA29BE171B48745F0FDF857E330B0EE31AF36BAEACDE2CBA7DB62C8DBA84E9736EDA62DC6811A27C1B0F793F6D915032F570B38
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....$b.0c....'...Vb..^.H.a!y>....9.Ri.]%.F.q..\.Z.....[N.H.2.....[...#a....f..z..}ji4..m.....Cf...*...?.U....;....Z.....H...@..rv.....N.o..1..0..0pzR...Nv,.s.ED.{".=..k...s..o...|..P._C.*.mH.._....v...Jn..rI.....N.B.....P.Td.*9.8.0h.q`.$0..Fw).}G.@..M...6.U..#.0.T".J7g.P.<.;..t...:fb...R.(.B..I.47.Ei%'....v..0+.c.R..3....{.q3.Ad[.WN.F.n...1Z.'cGI.&....y[.p6..8...L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQVtAu[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):	19353
Entropy (8bit):	7.759923173787334
Encrypted:	false
SSDEEP:	384:IWHFoJoL9JdqB+osyLtr3JN5rSwxi55JPZZQDm0tHelvTCn:IWHFsyTdltpTdhivJBZH0t+FS
MD5:	E816AA08895A8364BBBFE53AD815ED4E
SHA1:	17B84C624BA2CDBD33D301A55A91582BDB7AF63D
SHA-256:	F800A4F3965D72E5926E78D37DD60DA9C5B5CC6C4C03C615DE4D6E20C56D1036
SHA-512:	7BCCBE050D366D53B5F6D79F085E666799170B0CA4B143F2125A2563D4A81C6392CB2494DAF1CB416FAB0950FF59879A8FF49996E6F0486FA38BB2F4EC703B05
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.....?..JE...8.@-....(.h..@..a@...1@.(..... ....).....Ub..h...%.j..L..`<.....@...1@...1@....(..P.....gjw.g.~3.CcH./.....=.IE].&..h.....Q@.....S+@...9..@..N).z..M $.v..,G.1.....1JC.Q.=.1..e.B.....P....b....LP.b..P...P1..4.!.P1.....B(.....!...P.q@.(...,(.s@..(...C.(..P1..R.(.....Z.Z.(.ph.B...P..P...abk|.P..6.V....b.....b....p..b....b.....@.....=(..@.wJ..C|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQY5wp[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):	19782
Entropy (8bit):	7.879863395208828
Encrypted:	false
SSDEEP:	384:N7rdVbDzyJWYwwbZ4bGDV6cfWzPPhXsZUr4beTLUhguzB1kmN1GRHGC:NfdVbfyJhb6bGDQc0P5XCUrkek7zBt7Y
MD5:	CEC9F2AADCCEBE3F3C6392A872F1CC39
SHA1:	3484B4FB224D139DA9CA812A69CEAD559BEE8C38
SHA-256:	10F23EEE479EF2361B9765AB284445FB74044C1797A8BC80883FD2E051605BF5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQY5wp[1].jpg	
SHA-512:	E9B251DD02FA469605E57E6A227A2A671E68E282438EC914F6168803EDABF0F61E45799D452903F66BA55039653CD64250486A4F3CDA3946283418607A700193
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..Y..h?.X...W...)l\A....8R1@....<.....3d.%.Jd..r8.....$.....-...6?3Q=..6y.(kn..@..~*.e..'.f...j.f.j...y.KB'.-P^.....B...]..q.J..6.h.s.....:H..&.=..*&Tl.Y.&r2}(.K..,.....V.....P.>..oz....M..'V....=.....N.q....&>~.H{..M :{a."....?..*#.r;.e.q..S.6b....ld..Pw..4..P..@.^"@t.._.Mn.....Z.F?..&i....8.%.....?..jD..>.FC..aL.y|t.h.Q}.V?0..#.gw.....JF.....4Kb.=.GN*...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQYUU3[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):	11434
Entropy (8bit):	7.8398861809660385
Encrypted:	false
SSDEEP:	192:Q2C959aS/xQOMOYHA3lwCtxRK1lwSXN1dUZfjcY6ptgTO9k8/WnYOAbnJL7XJnSG:NC79aSyOU0MXiw4LdUdYzQTO9k8/yYNf
MD5:	59B445EB127DDE6D408FD02EBF608492
SHA1:	4011C264FF8FC0731A7B3F349C5948A04D85F735
SHA-256:	CDFC1F3923CD42DE86B02D2AACE9D219BC85FACAB04A6F675CBE5B244B2577DD
SHA-512:	B4B85890B7E60327ADBFF48C9759102A66A0895EAD5E8A37EE04115B6237C85ED2B5D811906F1BEF097AE9226D84E9DF5F97BC9ADE4625FB4DB6B0E195A67A14
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...9...WbnR.Ku..S...As.....S....`}.....HL..MP.....D..m#.<r`...q...g.@v....p*9..i.x...'..?O...A...x.K...P}....\..q5K..[....K../.....}.,1..b:....}.,..Y.[....E.S..:L$.p.....r..8..7..4.B.). ...,...G(\~".....(\...v..y./.....+...2.p....X..Q.....].J..56.=.-...P.@....P.@....P.@....P.@...ld..@..g..;...!...".-X\..\...!.....[.V!...9IV..E1.=.[.U~7...&.{.?.(.\....B..4.G

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQYYTT[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):	6853
Entropy (8bit):	7.324104220761635
Encrypted:	false
SSDEEP:	192:Q2JLXqUuxqgXquaXUbz3AG2K4gjLAP5XVEtgIsRQr:NJrJux3X2XsDAG2KjsPLvRQr
MD5:	86F73DEE74D629016FD1DC02F856FC0D
SHA1:	D4E062C0C6D563D6B46C200A50A7689E48CA84FB
SHA-256:	CE01C2B9BDB161FB546265C45F3BEDC1286D562D1BD564DC8EDDE7C96E1CB051
SHA-512:	63C6C56106BEC6B9AB9F9D90B7165A49AF64A074E5EB1EFA4298ABC2C02916C0D108961B747F9202D1B5502199C96C85B30B61671C9BACB2B43070ADD26E1D77
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..k..)...P.@..-...P.@....P.@....(...Jc...@%...(...@....(...R..... ....(.(.R.....@.@......P.@..-...P.@....).).P ..H...`..P.@.....P.H...@. ..(.(.(...P...@..-.....P.@.....P .....).(...LA@....@.@.@....P.@. .`%...(.....a@.@..-.....P.@..-...P.@.....L...L....(...P.@....P.@.....P.@....J`..(.(.P...@..-...P...@..-...P.L...0..(.....(.P.@.....P...P.@.....P.@..%.%!.@..-.....P.@.@....P.@.@.0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQYqMl[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):	12085
Entropy (8bit):	7.868445665118221
Encrypted:	false
SSDEEP:	192:Q29PYGiyDX2g6kKZUB3wvR0/pjAyWugqQW4S+v8xq+cIJEfsT8zhS3:NeG5x6ZUBwmwExQIpT8zhS3
MD5:	BE7D49E27B34AC5B0E8A91C4A769B854
SHA1:	26FC2880083BF13416735A890FA4399DF870820F
SHA-256:	77F20DB93B5A56C97BCC0C07A35DC592DCBE3072B69DF9807176234E7AC5FE0B
SHA-512:	5A16D09F0CF6158214BCDA5AA34E7F32ED900DEC4DD8B284D06C6661A63A60540AB98E79C0B363E3149C0D1CB69B721EDA763103A3670FBCCFF7EB5951278CC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQYqMl[1].jpg	
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..+....(..411..1.UA...F*YC."...4....i....x.....rZ.@.....i...JB..(..,hZC.....qsN..E..f....)Xw..,.....2.3.....Rli.....K*...AJ.(..o.0r..k[+w...c.1.w8.R...2..6....~xgm..Q.....b.|L@..... .....'.O.$...|.\..t.{C.UE...W...+~...i...kGQ.....i.....XN(..BP...3L.....@.:P..1).P.L.%....).).(.i.R.....L.;....(..5-..<1..w...m..z8U.<.z..H.R.....D.>TA.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAzb5EX[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):	322
Entropy (8bit):	6.966129933463651
Encrypted:	false
SSDEEP:	6:6v/lhPahmKxf8jCAw4DGQJe1kvnxIekdOgcKOtQExGTFDDv4bp:6v/7IxkjyzQEyaI1QmGTlW
MD5:	89E1141C659F2127DD80809F71326697
SHA1:	3262110C91000071FDBB0D33893EC1EC8026ADEC
SHA-256:	98763AAD3E2B7507E7729711ACD2DACCBD56164FE6DDB10410047B212275C279
SHA-512:	1D32DF0DB191F0A3FA152BC47F5F463234224F215A283A26E4EBAF95095A0977ABF5B9D9804FA4DDB276CA8DAE2865789802BB8A18B02B232A9DBB22D5F19E49
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..=..@..C.....K..`-(.`...vb.....vV...`g.!D....!....7..../Qg.Z...Y.....c....t.....c..).....)@.:.....8..t1{P_\.1..3Ao.....A].....5G_.....\5..x5R....'...VS.....\.`...~.....+....H^..1E^...0.,')....qJ8!..D.!O}.i1..E(....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1fdtSt[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):	438
Entropy (8bit):	7.245257101036661
Encrypted:	false
SSDEEP:	12:6v/7DHVT2T6ESAN2ISAy22UaU8Pa7+/LB:4Tq0AN2IjyPaqV
MD5:	3F46112E8E54A82D0D7F8883CF12A86F
SHA1:	AA1A3340F167A655D0A0A087D0F6CBF98026296C
SHA-256:	E447211712478A81E419A9794678B6377AE3ACA057DEA78FC9EF6A971E652CFB
SHA-512:	EBBF357EF6B388E4BD1B261D51DE923D15DBF3AC4740874BEBDEF336BB8133C3B63AEA9D8D95D2D1A044F6E43B7DD654586661462C9239E4FFA6B8328E6B49A6
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....hIDATx...O+DQ../]....f..(.,.-.!.L..X..ee.,.. .I.D..h..P,&.|.c.L.i.E.{.k..~.}.}.....t...W...*.5.2..0)X0I.c.wbU.....N..,....-F...J#lSq.;....a...*.....D .w.g..N.....F)l.....`_..s..A;?.4..+..ob.....Qh.H.:A.....(....;.z./..?.:...t.[.e..b.....{..t.A....M..0.>8&_"... Ev.Z`.."...=/..F.}X....#|.Ny. Z.....W...{HX;..F..w..M:...?W.<4B..!.I.....I.o...s....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\auction[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	11694

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\auction[2].htm	
Entropy (8bit):	5.849575695824997
Encrypted:	false
SSDEEP:	192:q4ppAn30M0ead2z1rvdpoJCU2oxy/V/VB8grc7WgUGG/Bjy72YdiW:q4ppAn1MYdvdaJCqK/D8grcyt/By7xEW
MD5:	8B74CFF70D3D87E3F0C24D6AFA518DA9
SHA1:	085C71527B0B4B010B691CE341BA0976CD3B5F85
SHA-256:	39A15FA1B6D9F0403C49C3458EF5A8E70AA21FAED0CEAF4DB1C1ED89AA2885E0
SHA-512:	155203A1E24AEBE18CA42FA9D4AE0EEA3070B3D0C4318B1EFD37940E7A937D6D3D02461676F67ABA53FD692B405DD3F703E4877015228609ADD15691794A746
Malicious:	false
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_194ce0325cd3d55ee1127b6acbbe4fd8_c0ae076f-8a07-433d-86ff-fe385f4d90f2-tuct89520bb_1637587771_1637587771_CIi3jgYQr4c_GJ2N2vDC46vl7gEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaKKcqr2pwqnJjgFwAA"},"tbsessionid":"v2_194ce0325cd3d55ee1127b6acbbe4fd8_c0ae076f-8a07-433d-86ff-fe385f4d90f2-tuct89520bb_1637587771_1637587771_CIi3jgYQr4c_GJ2N2vDC46vl7gEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaKKcqr2pwqnJjgFwAA","pageViewId":"89e9c689e4e442bc8decc0870f35ae96","RequestLevelBeaconUrls":[]}">..</script>....<li class="single serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"gemini","e":true}" data-provider="gemini" data-ad-region="infopane" data-ad-index="2" data-viewabil

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 16 colors, 32x32, 16 colors
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	1.240940859118772
Encrypted:	false
SSDEEP:	3:etFEh9HYflvlNl/AXll1pe/WNN0000000000000000000000000000000000001:QNtY6+lKY6
MD5:	4123CE1E1732F202F60292941FF1487D
SHA1:	9F12B11BDE582DAE37CE8C160537D919C561C464
SHA-256:	D961B08E4321250926DE6F79087594975FE20AD1518DE8F91EB711AF5D1A6EF8
SHA-512:	11B24C2E622C408E4774FAE120B719A21A0B2ACFA53230126C35AD6CA57D33D4DE79CBE11D296CFBDE9613CAA03D66B721BD20CF4EE030CF75F5A1FD8A286A9
Malicious:	false
Preview:	.....(...&... .....N...(..... .....(... ...@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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):	411778
Entropy (8bit):	5.487186890057773
Encrypted:	false
SSDEEP:	6144:z7JkYqP1vG2jnmuynGJ8nKM03VCuPb8XEcJuzYmD:A1vFjKnGJ8KMGxT9YmD
MD5:	BA03B59C779E95D1FA242A8157A4D408
SHA1:	6956C2A67A8DEA1173F4B0D03C60DB97DC8A09D5
SHA-256:	5EBFD5850A8855C84F005BD0FE676AC505BB3E78A9F83DA7BEC3B0EF2F35B6C2
SHA-512:	5EF1C108E309499A3CC65B0324C308DF41096F508CCA1C475D3E41758DC70159C37EBEDB2CBDEE7CFC6AAA06B6F4A02301B35A400B98718C5D5BB1727B8DAB0
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\NUEPGTR9\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):	411779
Entropy (8bit):	5.487195093908782
Encrypted:	false
SSDEEP:	6144:z7JkYqP1vG2jnmuynGJ8nKM03VCuPbmXEcJuzYmD:A1vFjKnGJ8KMGxTPYmD
MD5:	8E2D27B007FB92770E40D1DF43C37346
SHA1:	1011A522C912819C5F24613B77FC165699B7D640

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\medianet[2].htm	
SHA-256:	EA85133CE5090B0F0D13EDE0FF11985636FBBFF7D07BFF269640EFFF4E944CB9
SHA-512:	63D308DB6D4464F087E8C7947ABDF04118CD267FEE6FF6F331D938AFB15822C8B5FD5ACABF564707CD6D408D266EAA7620FDF12E6BA9DC4C082B5ADA04B80 2F
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]:{lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otCommonStyles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20953
Entropy (8bit):	5.003252373878778
Encrypted:	false
SSDEEP:	192:LIsia0zYw49vRn4l7cWQjRkmSxoU/4OIZZTg8l9Qonnq3WwHpUkG4HfeXiPcB2jk:HRc7fQxNGoFBlCHcXaivSYBQY2YpuML
MD5:	E4F88E3AF211BD9EA203D23CB0B261D5
SHA1:	6067E95844B3E11A275ADD0B41D7AD3F00A426FD
SHA-256:	E58322F14AC511762E2C74932104D7205440281520CF98E66F15B40AA8E60D05
SHA-512:	B2C8870B61E9132DC7D7167F50F7C85BFE67EAC6DA711BDF0B9C85EB026249A95E8D67FFB0699934EAA304F971E44F0180E8578AFD8353943154FCE689690B76
Malicious:	false
Preview:	#onetrust-banner-sdk{-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}#onetrust-banner-sdk .onetrust-vendors-list-handler{cursor:pointer;color:#1f96db;font-size:in herit;font-weight:bold;text-decoration:none;margin-left:5px}#onetrust-banner-sdk .onetrust-vendors-list-handler:hover{color:#1f96db}#onetrust-banner-sdk:focus{outline:2px solid #000;outline-offset:-2px}#onetrust-banner-sdk a:focus{outline:2px solid #000}#onetrust-banner-sdk #onetrust-accept-btn-handler,#onetrust-banner-sdk #onetrust-rejec t-all-handler,#onetrust-banner-sdk #onetrust-pc-btn-handler{outline-offset:1px}#onetrust-banner-sdk .ot-close-icon,#onetrust-pc-sdk .ot-close-icon,#ot-sync-ntfy .ot-close-icon{background-image:url(" s9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkveGxpbmsiIHg9IjBweCIgeT0iMHB4IiB3aWR0aD0iMzQ4LjMzM3B4IiBoZWlnaHQ9IjM0OC4zMzNweCIgdmlld0JveD0iMCAw IDM0OC4zMzMgMzQ4LjMzNCIgc3R5bGU9ImVuYWJsZS1iYWNrZ3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otFlat[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12859
Entropy (8bit):	5.237784426016011
Encrypted:	false
SSDEEP:	384:Mjuyejbn42OdP85csXfn/BoH6iAHyPtJJAk:M6ye1/m
MD5:	0097436CBD4943F832AB9C81968CB6A0
SHA1:	4734EF2D8D859E6BFF2E4F3F7696BA979135062C
SHA-256:	F330D3AE039F615FF31563E4174AAE9CEAD8E99E00297146143335F65199A7A9
SHA-512:	3CC406AE3430001B8F305FA5C3964F992BA64CE652CCABD69924FE35E69675524E77A9E288DDE9BCF697B9C1C080871076C84399CDFAD491794B8F2642008BE
Malicious:	false
Preview:	.. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCI+PGRpdiByb2xlPSJhbGVydGR pYWxvZyIgYXJpYS1kZXNjcmliZWRieT0ib25ldHJ1c3QtcG9saWN5LXRleHQiPjxkaXYgY2xhc3M9Im90LXNkay1jb250YWluZXIiPjxkaXYgY2xhc3M9Im90LXNkay1yb 3ciPjxkaXYgaWQ9Im9uZXRydXN0LWdyb3VwLWNvbnRhaW5lciIgY2xhc3M9Im90LXNkay1laWdodCBvdC1zZGstY29sdW1ucyI+PGRpdiBjbGFzcz0iYmFubmVyX2xvZ28 iPjwvZGl2PjxkaXYgaWQ9Im9uZXRydXN0LXBvbGljeSI+PGgzIGlkPSJvbmV0cnVzdC1wb2xpY3ktdGl0bGUiPlRpdGxlPC9oMz48cCBpZD0ib25ldHJ1c3QtcG9saWN5L XRleHQiPnRpdGxlPGEgaHJlZj0iIyI+cG9saWN5PC9hPjwvcD48L2diIGNsYXNzPSJvdC1kaGQtY29udGFpbmVyIj48aDMgY2xhc3M9Im90LWRwZC10aXRsZSI+V2UgY29 sbGVjdCBkYXRhIGluIG9yZGVyIHRvIHByb3ZpZGU6PC9oMz48ZGl2IGNsYXNzPSJvdC1kcGQtY29udGVudCI+PHAgY2xhc3M9Im90LWRwZC1kZXNjIj5kZXNjcmlwdGlvb jwvcD48L2Rpdj48L2Rpdj48L2Rpdj48L2Rpdj48ZGl2IGlkPSJvbmV0cnVzdC1idXR0b24tZ3JvdXAtcGFyZW50IiBjbGFzcz0ib3Qtc2RrLXRocmVlIG90LXNkay1jb2x 1bW5zIj48ZGl2IGlkPSJvbmV0cnVzdC1idXR0b24tZ3JvdXAiPjxidXR0b24

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otPcCenter[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	48633
Entropy (8bit):	5.555948771441324
Encrypted:	false
SSDEEP:	768:VwcBWh5ZSMYib6pWXlzZz6c18tiHoQqhI:VwqZYdZz6c18tySI
MD5:	928BD4F058C3CE1FD20BE50FE74F1CD8
SHA1:	5CBF71DB356E50C3FFCB58E309439ED7EB1B892E
SHA-256:	6048F2D571D6AE8F49E078A449EB84113D399DD5EA69FB5AC9C69241CD7BA945
SHA-512:	1E165855CEF80DDFBE2129FA49A0053055561ADEFF7756DE5EA22338D0770925313CCB0993AD032B95ACE336594A5F38E9EE0F0B58ADFE1552FE9251993391C1
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otPcCenter[1].json	
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImFsZXJ0ZGlhbG9nIj48IS0tIENsb3NlIEJ1dHRvbiAtLT48ZGl2IGNsYXNzPSJvdC1wYy1oZWFkZXIiPjwhLS0gTG9nbyB UYWcgLS0+PGRpdiBjbGFzcz0ib3QtcGMtbG9nbyIgcm9sZT0iaW1nIiBhcmlhLWxhYmVsPSJDb21wYW55IExvZ28iPjwvZGl2PjwhLS0gQnV0dG9uPjxkaXYgaWQ9Im9 0LXBjLWNvbnRlbnQiIGNsYXNzPSJvdC1wYy1zY3JvbGxiYXIiPjxoMiBpZD0ib3QtcGMtdGl0bGUiPllvdXIgUHJpdmFjeTwvaDI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyBvdC1 jYXQtZ3JwIj48aDMgaWQ9Im90LWNhdGVnb3J5LXRpdGxlIj5NYW5hZ2UgQ29va2llIFByZWZlcmVuY2VzPC9oMz48ZGl2IGNsYXNzPSJvdC1wbGktaGRyIj48c3BhbiBjb GFzcz0ib3QtbGktdGl0bGUiPkNvbnNlbnQ8L3NwYW4+IDxzcGFuIGNsYXNzPSJvdC1saS1
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\px[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJ9pse:Gl3QEsJLse
MD5:	AD4B0F606E0F8465BC4C4C170B37E1A3
SHA1:	50B30FD5F87C85FE5CBA2635CB83316CA71250D7
SHA-256:	CF4724B2F736ED1A0AE6BC28F1EAD963D9CD2C1FD87B6EF32E7799FC1C5C8BDA
SHA-512:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A 910
Malicious:	false
Preview:	GIF89a.....!.....,.....L..;
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\2d-0e97d4-185735b[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	251398
Entropy (8bit):	5.2940351809352855
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvJZkrqq7pjD4tQH:Fa0ULTAHLOUdvwZkrqq7pjD4tQH
MD5:	24D71CC2CC17F9E0F7167D724347DBA4
SHA1:	4188B4EE11CFDC8EA05E7DA7F475F6A464951E27
SHA-256:	4EF29E187222C5E2960E1E265C87AA7DA7268408C3383CC3274D97127F389B22
SHA-512:	43CF44624EF76F5B83DE10A2FB1C27608A290BC21BF023A1BFDB77B2EBB4964805C8683F82815045668A3ECCF2F16A4D7948C1C5AC526AC71760F50C82AADE2 B
Malicious:	false
Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expe cted semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weigh t:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.todaymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem ;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption, .todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.todaymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead {bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.title):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .captio
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\52-478955-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	397554
Entropy (8bit):	5.324293513672579
Encrypted:	false
SSDEEP:	6144:YXP9M/wSg/Ms1JuKb4K7hmnidfWPqIjHSjaTCr1BgxO0DkV4FcjtIuNK:CW/ycnidfWPqIjHdO16tbcjut
MD5:	E0EE2633FE41EB7DDC1CAE8022DFB4D2
SHA1:	943A97B03F6B3BE7053CB2EDE05E1E19839B3790
SHA-256:	9B752E3E13C79007FC41FE147485990CED773DDEEE63D7409CC5DEB45062393F
SHA-512:	22994B9288054B22B49A9D439F5DF7A4DBA4507DCA56F20BF222113AA60544E374DEF9FCBCB214DF0684DA68A3550898CCB5B47EAA57C20FCC52BDC735653E 4
Malicious:	false
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMa rker("TimeToJsBundleExecutionStart");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 nu ll";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=="function"&&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,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAOr6Ee[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):	23952
Entropy (8bit):	7.717838617904555
Encrypted:	false
SSDEEP:	384:IIHDAA2l+lx2hLMicOb0WIO//nMUIvENuMAKr/EUs1W+W30npOGYjElTu0Ja1:IIHt2l2hQicb4HM5vEJQj1WvknpOMlPI
MD5:	5321079247607C448C15CF6446E1F155
SHA1:	7DA88FE223914B121776A5301C7C88F248EBA31E
SHA-256:	BBB6AE5F20EA7EF347B15431CF24AFFE30FCB51218C1779FEB5B387F24877F94
SHA-512:	42CD55111E8E384D83BF222B0D38472A2DA8AF626DF616D4E5B665A4C0C6251625E3337B3951DC3244B3EF7942AC1251548B78A4BED982F5C8C70967B4DE4B3
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...@..P.@..-...P.@.....zP..GPG.P.P.@....P.@.@..-...P.@....P.@.h.....J.(.....4...P...P.@..-...P.@.h.....J.(.h.(.h.....(.....].....P....J.(.h....h.(.(.h.(.....(.(.h.....(.....Q#.w.8..x.N:T..L..y.kH.....%.m.....e..q.@.. ..(.....(.....(.....J.Z.(.(....9o....9$.Ah.K:...Q.t.h..O.x.TR.1M.=m...0.."....nD~.6...(...m..>.u..^.*..d.z.j....P.@....P.@.@.....P

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQTQg3[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):	16552
Entropy (8bit):	7.962704167525703
Encrypted:	false
SSDEEP:	384:bwUOEG07947y6MuqZ3a0hLx8cWlHLSLJI1sz5G1i3KmthC:bwex47nMuCVH/WlaJfMi3KmthC
MD5:	30C5DFAB992D12D27C5FF58B3CD3B81D
SHA1:	F19657FA21E005441FAEAE1D107C8D2203593C5D
SHA-256:	EB2BBF30F0A20C1D2F1B5C96A9D7DF32115F7ABD4E68374DF2A0B996ABB0C23E
SHA-512:	EC89E47D9C49DB7B5E8E5388A29C5F1C5424C0293DC972D9878A332C58A0174F083BACAC07574A761844E5CD6A2E33BF4648B92DB7494129DDA4CC11FEBDAAC8
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...M*.(.!..V`.>o..;.[a.B.....F...$.....Us.ME..J.lV.h.,.....(.n....cz."..A(...yu.....c.FJu.U.....Q.....d....ws...8....&s..Oj.?~...m,R..l/.2.(..c...]8....ubIu44.@F.y..'..\....#;6>...S:.....c..J._eY'.M)F.\.... bc..~.=....].2w...1l.....y..l3*...X^.?.lR.+_.3,.Zm..q.Cg-.v..i'..o.R... ...J.S&...`.ul...5....B..].....qT.l....*K..x....L....n.N.e^.Ya.~".G.#..u8.}+HJ...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQXTtj[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):	14320
Entropy (8bit):	7.89477873630106
Encrypted:	false
SSDEEP:	192:Q28fp8fRQ0nTuzxPf+upDBHKj583EG9QN93SNxSPKmJSksiwFWOfdJ7HgIYyv0mi:N8RmnMuwBHKjyQN9iNxAD0FWOrfYyMT
MD5:	A0ADD5BB3AB71485AB8C23FD851EF4C7
SHA1:	2E1B680CDC5CD69BABBF450CEAF287301D6CC221
SHA-256:	6159DB7282EA3312B03E7BF5966C59D3768FB0E0AEE0731398AE8E3B51637E28
SHA-512:	801C24DCDEC2FDE0400D7DE5F2A18331085A45F4104334153C3DC2560320927DF0D9A5A8B5F41CBE442D74B5EC2CB71C3F4B83B5F8E97E15DCA3E485CE500E5
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..Hd...lZD.....=...HY.....9....P.5.$..1..8.f..D@.a....?..mZ.G....3..Q.#<S.g..b...1L.....B..S.....BP...J.J.(."..h....h....h....i...!..3...3J.=.(.>mn.8.<..`~...R...g."_S..i\v)Hf.....?.j.|v.....Y...V.=.P..a.|.8..h.'....i.D..T..b..^.=..8D.$..c]...c.....ci...i<.ub2z....._%\.....m1XKp..T..S.M...`.....1@.0.P.@.....J`%.....@.4..(....4.k..,@...2..6..r.8.I.1...W...H%.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQY2dE[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):	18396
Entropy (8bit):	7.950793431842648

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQY2dE[1].jpg	
Encrypted:	false
SSDEEP:	384:NgUXDiFM/kDFQCEIswPbfDjexQR1LZQfQaYtjyN/e/hsdzW7b:NgQsD+CR9PL3z1LWETyMf
MD5:	A6024E416A00FDB451476565B5AA9D3E
SHA1:	C222C3CD25172BD71157EAF8A9FCBDC1B4057316
SHA-256:	639943B0A2BB70755A9FC7335E008D4BA1443D58711E4DEBE002CB4A4B0D56DF
SHA-512:	B9056E80A79A051FDBC961B554660BA0EEB329A9864B4332FAF48DF9EC2454FB7C243D9E7D3AB2EC06C11F758CA59A12F76796F9050A047B05CB8B8F5616C27
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..LQ...2..."0..8....tP1...c...E. X..i..|...D .....N.&..e.....T..C..`...EZ...g...h.|.q.....S...2-.....G.jEym...- 2..h..:q.)7..k5.<...8X. ..P.Z...k.xr...raoI"....A.....A,...;...QwZ.j....(..J..v. .....a..hi.....p8...M\\.....i.....J.d./....NYbV....9.s..x.A.3....>r....!R?..>.H9..G.....48XW.....<....6E_*?.....y...(..DQ..4...E.@.(. .)?.I.a.G.yi..|.....X.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQY4m2[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):	9546
Entropy (8bit):	7.940815331104628
Encrypted:	false
SSDEEP:	192:QohDT8RJu7ZVwpn0GY3D4aDgLepmmqzHujlOAYW0H7YN/FXxCnXq:bhDT8S4plY3DDismmhlOxWjpQnXq
MD5:	BD27BDE77157ACB67E62FBB86B5C844A
SHA1:	4FEBC5D1AE2DE3B04D419235F4F8F9D977EF95D0
SHA-256:	C5931E19328CC56BE1AADF9D04A2FBCC73ACC0AF1A1A5E5AD0AAFDAF49872C36
SHA-512:	D606CA204396AB8726ED7B620CBBAA0A63F22A97F90E8E230AD838CE00EC1083C2A94516521513F6AD73E9338C357CDF48DA24A7884ACEEF0368491D3B7893A
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....P.....~a....<.....5'....8..TS..`).F.]...~...q....Y.0... .....4.....(..p3..cI.&.....~.-...N.7i.k.nz....#..{.UOa.s&..m.h....=..s.}.hX... ....c.K...q%..J.$H9.1..G.....Ly.O.C.".....'l"~g.Q{....Q.=..y*xU.....m...Ww..3..=H.....F.K0r..c..E.ui".N..I.....I.8.....8.c..?+.....K.D...(.S@-0.....+.A..s..G`{..[....._../..Q..3.....S...n vH}s..j..zH.....C...A...n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQY5UV[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):	7009
Entropy (8bit):	7.836882517627216
Encrypted:	false
SSDEEP:	192:QoLulElU7JZihMNcIKN6rJvHT4jB8dRoNrV:bLjlyJZihMCIKKF0jBAoNx
MD5:	562188910D5608DBA1D9AF237FCB54A8
SHA1:	9D7B7DDE24A2FC0EC9178FCF7BF3DAF1AB689F26
SHA-256:	17A93A8E9DAAB42C9CBF5A723610AD7AFDD1260D023D6A673E863E50F6C970A7
SHA-512:	071327A5A15469F1E35F69095488E1A0A08AC2FFD66BF26F32F1846A9E21415161BB14340A8AB0DAC65F934A5D0604B31D1321A11A69BB701C57C508145C50C3
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...P...G+....*.M.K?.O.~\z..H.....v.T.[R...&m*].|.f...i.q(...6..%...[...5.*.r\sI..2.....XO}.9.d .....!.}.=8.>G.i}.W...b[+.J]a.(.....4 .R..m.a....+KP{.....h..Y=...4.V.y.....B..Bj.....J....f$Qv5..EF1..?.^M+..Y....B|...?.K.a.....(.P.R.(.....).z....@-.!..MK.{m.S..{.k..N.*d...+...zv.l.PkW.a..!W|.....UqWdI.h...h.W....f... ....P..J.$..'.2..{X...e...Y.....j)...r..8.m.a.F8/..EO2.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQY8ZI[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):	8659
Entropy (8bit):	7.9285351845729215
Encrypted:	false
SSDEEP:	192:QovTZyaXO6NI/sPbtBwweO+dd/20/1FkoyhyDc00Oe7iG4:brwsIkPbsOId/f/DihyDc0Ne774
MD5:	69F548B1C470B471FF70AAC87E0CA8D7
SHA1:	43D8565909357FABDFA1A38A02741A05146DFD39
SHA-256:	1F9581691FE4A28BC0DE30718DCE3CD1F581D398790F9F4D7C21A48E8D620E82
SHA-512:	2B1E777C45A821EFDF0A794867C597DD04CF42056839C0F1EEA5AF42066556200B32F1A821AA0B3B2121AA316990E447634CA770F61605B5E921C4AA8944ECB5

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQY8ZI[1].jpg</th></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?...7...*..7...,..j9..OnG.w...-.E..m......(.Jb%h..(.];Ok....sI..7F.....|.. ..-.{..GA......I$q..6.q..d@...j.THn.8..F...bK..}4L@.'|.{..T.
!m...M.:.r.......w...A.q..e4...M........0 $.2Tt>.gO....\...-.j....G......*/[.....WUI+..r...X@..F8......t..E...2)S..(...Z.M.m.qJ\......9.....$.....Mw..<.y&..3..;.....R..X..3....b..)..}.y_2.(...B..Z.&....
(.-..m.8.s....r9.......ma.K#..p=</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQYCwH[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>18774</td></tr>
<tr><td>Entropy (8bit):</td><td>7.653540204478841</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:IobkyZV5phSu5ZfUQ1dLehs/yqFO85YBCLv/KZ+zX7tSwXCE:IoYyTfVfB1dShs7x5faZ6SwSE</td></tr>
<tr><td>MD5:</td><td>01499D3DDDE3D289D9E293CE10D4F565</td></tr>
<tr><td>SHA1:</td><td>352EB15BE34328E449A92136BF2AE67DD1FD5A5A</td></tr>
<tr><td>SHA-256:</td><td>5A79C1936C68184A1952E7384BCBB0A6ABAA88E905DB02D90BD3A7E47981653B</td></tr>
<tr><td>SHA-512:</td><td>57C7BC03557C8610600119B8994F7F81477C0F55A2BD81C10ED26527D2E1B6F25AC10E42CA26C5F8DA55DC94D6620309912A5C1800E2442C549C5F87EB538D4F</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......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.........
....?....(......(......(......(......(......(......(......(......(......(......(......(..........(......(......(......(......(......(......(......(......(......(......(......
(......(......(......(......(......(..........(......(......(......(......(......(......(......(......(......(......(......(......(......(......(......(......(......(......(......h.(......(......(......(.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQYSTg[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>22085</td></tr>
<tr><td>Entropy (8bit):</td><td>7.835373264723497</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:IFQLkIwIuFmHbM6rIonocDXB/KLgaXBxQq3IVjQipYbqrO/+rQK/sixBS6IigPm/:I6kvFSXIolDXByUqYVkipYurXQK/txsW</td></tr>
<tr><td>MD5:</td><td>06E10697284E39A85FD5A8E598C44641</td></tr>
<tr><td>SHA1:</td><td>D38F23FDF74D510178C875D8BCF7105383BC2575</td></tr>
<tr><td>SHA-256:</td><td>878BD9D235D9E85EC0E1A57ABDEB938495FBDF8D8FA534A0E6C1835D78BC713F</td></tr>
<tr><td>SHA-512:</td><td>554703B928AA1A7A9B307D4D1C982241DB4B6B0E2F408E56D36921A21581D416D93090951DEA9745CC163388B24570C741126A401CFED8E76BBA80FFC34FD855</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..7b.......!.....P.34.(.B..N.a..\d...c5m...h...NG.@...P...J.:S...LW...qR.n.......x..4.P...@...^.........h.o..h.....9@>..b..<G..w...K.@
v..p.U..S.!..<@....~".!k;f..>.@@.dg.[.@..O.C...q@.C..vG.,.z7"....W.1q.?....*..|Un./..w.ir..Km{L.;|.R{?..ar.Ky.....@.B..R..0......#@..G......,...?........c.....P...?:.p.z.h...o.a..,
@mc.a/...lR.....:H?..?...$.G.-.?......<.......z,..K!^UI=OJ@=$f.hd</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQYWm8[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, 206x250, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>13217</td></tr>
<tr><td>Entropy (8bit):</td><td>7.95801980085305</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:QoQulhJzy/nBnhg+WPACfLC2MqMRVg2wI5j3FrStIeP4P06ImiE48y+IIo31PN3G:bjkk+Wo8mrq6gNI3xg4PDNiJAY1l3Dub</td></tr>
<tr><td>MD5:</td><td>18BAB962F492552B63A7A3840027DF1F</td></tr>
<tr><td>SHA1:</td><td>F7922984A15284BED0F76CAD29C0E12B531CEF01</td></tr>
<tr><td>SHA-256:</td><td>7B55394387A29FDB898A36B89C61B17FC1DA7E9763920ED9A746A49F9156EC9D</td></tr>
<tr><td>SHA-512:</td><td>0C1E51FB106363BCD49BB2ACDACF48D8EC03677F4DED48740DBA4C05A8D8A98E75B99B49B7A5DED23BD1D2C70CE8A5DC6FE09C41B627DE4006BAF43B3DCI
3A9D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......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.........
....?..u..@n!l).........D.N0kS.B...*...{5,.:.Q..3...~...L.F.....w.i....P...Q..[..|.H...5.......%...!...GJ..u..K.K...(.....'..9.x4......a.,......;.5B%
g+.....%w.*d..T.........z.mG.][@.G.....f...j...'.>_ANI Wf\.7-..9!A....N..\.1.........3P....".-..\sR.{.Vg;[.J.\J..W...%....M~e.X..5....s...h..VAf.X..i9a...F..lAq.....E..e;..f..........Kqn.G.=
Eh`\........l...;g....J.."....!.X</td></tr>
</table>

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.736841739951072
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.40% • Clipper DOS Executable (2020/12) 0.20% • 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:	2zTgaLRFkL.dll
File size:	136192
MD5:	096d27e730a16660704e6713fdc89173
SHA1:	880a73f218d5b4ba3f734c14ed3b84ef036aa85a
SHA256:	5bbba6d13c8222ef2cc5c4aecf14043f1e74d164ab2a1b3e4b68ee6cb086900c
SHA512:	295a9eff04f9a69286dda01364dd32c76585eaf18e09e2a7a57481f9f3bbb1a428b9dadc4a5c5034c60a2b18ac90d036cd7bfc31ec64965cc0cbc5c00d382b66
SSDEEP:	3072:wonUFuZWnUWaCezzbqMlJuIqf59+fbbAxSdk6Atue:woU/U3zXdx+eaL7t/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10002b61
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619A4C0F [Sun Nov 21 13:39:27 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:	4c89e39b5ebc619c69b957c6b4f65780

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb748	0xb800	False	0.604853091033	data	6.60960432653	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0xd000	0x13d02	0x13e00	False	0.679318985849	Applesoft BASIC program data, first line number 2	6.22213777784	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x21000	0x13a8	0xa00	False	0.137109375	data	1.83938352827	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x23000	0xf8	0x200	False	0.3359375	data	2.52105374013	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x24000	0xdb0	0xe00	False	0.775948660714	data	6.46060411689	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 14:28:49.704560995 CET	192.168.2.5	8.8.8.8	0xecb9	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Nov 22, 2021 14:28:54.533123016 CET	192.168.2.5	8.8.8.8	0x644a	Standard query (0)	web.vortex.data.msn.com	A (IP address)	IN (0x0001)
Nov 22, 2021 14:28:55.437889099 CET	192.168.2.5	8.8.8.8	0x3acf	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Nov 22, 2021 14:28:57.111588001 CET	192.168.2.5	8.8.8.8	0x41e1	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:00.386215925 CET	192.168.2.5	8.8.8.8	0xcbd4	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:01.498487949 CET	192.168.2.5	8.8.8.8	0x61c8	Standard query (0)	assets.msn.com	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:17.838159084 CET	192.168.2.5	8.8.8.8	0x82d2	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:18.691239119 CET	192.168.2.5	8.8.8.8	0x61b8	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:28.688193083 CET	192.168.2.5	8.8.8.8	0xf7a5	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:28.894833088 CET	192.168.2.5	8.8.8.8	0x9d25	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:30.198256969 CET	192.168.2.5	8.8.8.8	0xcdbd	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 14:28:49.723954916 CET	8.8.8.8	192.168.2.5	0xecb9	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2021 14:28:54.553054094 CET	8.8.8.8	192.168.2.5	0x644a	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2021 14:28:55.458055019 CET	8.8.8.8	192.168.2.5	0x3acf	No error (0)	contextual.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Nov 22, 2021 14:28:57.134823084 CET	8.8.8.8	192.168.2.5	0x41e1	No error (0)	lg3.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:00.405869007 CET	8.8.8.8	192.168.2.5	0xcbd4	No error (0)	hblg.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:01.518820047 CET	8.8.8.8	192.168.2.5	0x61c8	No error (0)	assets.msn.com	assets.msn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2021 14:29:17.859129906 CET	8.8.8.8	192.168.2.5	0x82d2	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2021 14:29:18.712405920 CET	8.8.8.8	192.168.2.5	0x61b8	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:18.712405920 CET	8.8.8.8	192.168.2.5	0x61b8	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:18.712405920 CET	8.8.8.8	192.168.2.5	0x61b8	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:28.717139959 CET	8.8.8.8	192.168.2.5	0xf7a5	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2021 14:29:28.717139959 CET	8.8.8.8	192.168.2.5	0xf7a5	No error (0)	dart.l.doubleclick.net		142.250.203.102	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:28.916603088 CET	8.8.8.8	192.168.2.5	0x9d25	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:28.916603088 CET	8.8.8.8	192.168.2.5	0x9d25	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:28.916603088 CET	8.8.8.8	192.168.2.5	0x9d25	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Nov 22, 2021 14:29:30.217794895 CET	8.8.8.8	192.168.2.5	0xcdbd	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2021 14:29:30.217794895 CET	8.8.8.8	192.168.2.5	0xcdbd	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - btloader.com
  - ad.doubleclick.net
  - ad-delivery.net

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49757	172.67.70.134	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-22 13:29:18 UTC	0	OUT	GET /tag?o=6208086025961472&upapi=true HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: btloader.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-11-22 13:29:18 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 13:29:18 GMT Content-Type: application/javascript Content-Length: 10157 Connection: close Cache-Control: public, max-age=1800, must-revalidate Etag: "643eb1aad6ba3932ca744b96ffc00048" Vary: Origin Via: 1.1 google CF-Cache-Status: HIT Age: 2610 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=c%2F3wFlbJEoPhaGnxVMHSn1QGiQjUEXM1sHDQZf48JEA6uerDzXMti9ubLCVkAmqaFO4Keo9XAtz%2Fv5wBuUOrZlecZSH%2FRZ0FJBPVC378dzzmtpD6pgRYyG9E%2FQMg8A%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b228184fa5768fe-FRA
2021-11-22 13:29:18 UTC	1	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 6c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 7b 74 28 65 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 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
2021-11-22 13:29:18 UTC	1	IN	Data Raw: 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 74 3b Data Ascii: nction(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;
2021-11-22 13:29:18 UTC	2	IN	Data Raw: 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 69 66 Data Ascii: nt).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){if
2021-11-22 13:29:18 UTC	4	IN	Data Raw: 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 65 62 Data Ascii: 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,web
2021-11-22 13:29:18 UTC	5	IN	Data Raw: 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 7d 76 Data Ascii: in: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})}v
2021-11-22 13:29:18 UTC	7	IN	Data Raw: 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 3b 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 69 6e 74 72 6e 6c 3d 7b 74 72 61 63 65 49 44 3a 77 2e 74 72 61 63 65 49 44 7d 3b 74 72 79 7b 21 66 75 6e 63 74 69 6f 6e 28 29 7b 72 28 74 68 69 73 2c 76 6f 69 64 20 30 2c 76 6f 69 64 20 30 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 2c 6e 2c 6f 3b 72 65 74 75 72 6e 20 69 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 73 77 69 74 63 68 28 Data Ascii: }var a=document.createEvent("CustomEvent");a.initCustomEvent(t,n.bubbles,n.cancelable,n.detail),window.dispatchEvent(a)}f={},window.__bt_intrnl={traceID:w.traceID};try{!function(){r(this,void 0,void 0,function(){var t,n,o;return i(this,function(e){switch(

Timestamp	kBytes transferred	Direction	Data
2021-11-22 13:29:18 UTC	8	IN	Data Raw: 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 22 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 4d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 29 2c 70 2e 77 65 62 73 69 74 65 49 44 26 26 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 26 26 28 21 28 6e 3d 2f 28 61 6e 64 72 6f 69 64 7c 62 62 5c 64 2b 7c 6d 65 65 67 6f 29 2e 2b 6d 6f 62 69 6c 65 7c 61 76 61 6e 74 67 6f 7c 62 61 64 61 5c 2f 7c 62 6c 61 63 6b 62 65 72 72 79 7c 62 6c 61 7a 65 72 7c 63 6f 6d 70 61 6c 7c 65 6c 61 69 6e 65 7c 66 65 6e 6e 65 63 7c 68 69 70 74 6f 70 7c 69 65 6d 6f 62 69 6c 65 7c 69 70 28 68 6f 6e 65 7c 6f 64 29 7c 69 72 69 73 7c 6b 69 6e 64 6c 65 Data Ascii: bileContentEnabled="true"==localStorage.getItem("forceMobileContent")||p.mobileContentEnabled),p.websiteID&&p.contentEnabled&&(!(n=/(android|bb\d+|meego).+mobile|avantgo|bada\/|blackberry|blazer|compal|elaine|fennec|hiptop|iemobile|ip(hone|od)|iris|kindle
2021-11-22 13:29:18 UTC	9	IN	Data Raw: 20 7c 6f 7c 76 29 7c 7a 7a 29 7c 6d 74 28 35 30 7c 70 31 7c 76 20 29 7c 6d 77 62 70 7c 6d 79 77 61 7c 6e 31 30 5b 30 2d 32 5d 7c 6e 32 30 5b 32 2d 33 5d 7c 6e 33 30 28 30 7c 32 29 7c 6e 35 30 28 30 7c 32 7c 35 29 7c 6e 37 28 30 28 30 7c 31 29 7c 31 30 29 7c 6e 65 28 28 63 7c 6d 29 5c 2d 7c 6f 6e 7c 74 66 7c 77 66 7c 77 67 7c 77 74 29 7c 6e 6f 6b 28 36 7c 69 29 7c 6e 7a 70 68 7c 6f 32 69 6d 7c 6f 70 28 74 69 7c 77 76 29 7c 6f 72 61 6e 7c 6f 77 67 31 7c 70 38 30 30 7c 70 61 6e 28 61 7c 64 7c 74 29 7c 70 64 78 67 7c 70 67 28 31 33 7c 5c 2d 28 5b 31 2d 38 5d 7c 63 29 29 7c 70 68 69 6c 7c 70 69 72 65 7c 70 6c 28 61 79 7c 75 63 29 7c 70 6e 5c 2d 32 7c 70 6f 28 63 6b 7c 72 74 7c 73 65 29 7c 70 72 6f 78 7c 70 73 69 6f 7c 70 74 5c 2d 67 7c 71 61 5c 2d 61 7c 71 63 Data Ascii: |o|v)|zz)|mt(50|p1|v)|mwbp|mywa|n10[0-2]|n20[2-3]|n30(0|2)|n50(0|2|5)|n7(0(0|1)|10)|ne((c|m)\-|on|tf|wf|wg|wt)|nok(6|i)|nzph|o2im|op(ti|wv)|oran|owg1|p800|pan(a|d|t)|pdxg|pg(13|\-([1-8]|c))|phil|pire|pl(ay|uc)|pn\-2|po(ck|rt|se)|prox|psio|pt\-g|qa\-a|qc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49760	142.250.203.102	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-22 13:29:28 UTC	11	OUT	GET /favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ad.doubleclick.net Connection: Keep-Alive
2021-11-22 13:29:29 UTC	11	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Vary: Accept-Encoding Content-Type: image/x-icon Access-Control-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="ads-doubleclick-media" Report-To: {"group":"ads-doubleclick-media","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/ads-doubleclick-media"}]} Content-Length: 1078 Date: Mon, 22 Nov 2021 13:16:17 GMT Expires: Tue, 23 Nov 2021 13:16:17 GMT Last-Modified: Tue, 08 May 2012 13:08:06 GMT X-Content-Type-Options: nosniff Server: sffe X-XSS-Protection: 0 Age: 792 Cache-Control: public, max-age=86400 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-11-22 13:29:29 UTC	12	IN	Data Raw: 00 00 01 00 02 00 10 10 10 00 00 00 00 00 28 01 00 00 26 00 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 4e 01 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 Data Ascii: (& N(
2021-11-22 13:29:29 UTC	12	IN	Data Raw: 11 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49761	104.26.3.70	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-11-22 13:29:29 UTC	13	OUT	GET /px.gif?ch=1&e=0.4482105559414631 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ad-delivery.net Connection: Keep-Alive
2021-11-22 13:29:29 UTC	13	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 13:29:29 GMT Content-Type: image/gif Content-Length: 43 Connection: close X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HlCnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34sctt0vecv7iFCJZExLBCcbRvF7nEjw Expires: Mon, 22 Nov 2021 12:53:48 GMT Last-Modified: Wed, 05 May 2021 19:25:32 GMT ETag: "ad4b0f606e0f8465bc4c4c170b37e1a3" x-goog-generation: 1620242732037093 x-goog-metageneration: 5 x-goog-stored-content-encoding: identity x-goog-stored-content-length: 43 x-goog-hash: crc32c=cpEfJQ== x-goog-hash: md5=rUsPYG4PhGW8TEwXCzfhow== x-goog-storage-class: MULTI_REGIONAL Access-Control-Allow-Origin: * Access-Control-Expose-Headers: *, Content-Length, Date, Server, Transfer-Encoding, X-GUploader-UploadID, X-Google-Trace Age: 3285 Cache-Control: public, max-age=86400 CF-Cache-Status: HIT Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=lruqchTT%2BBTz%2Fj9VAaTqlnGgyzWdQOqLpICht5738DIpEUGYfjer1A3IhyGk8osDGsaVOdeAk9xXoFSH3BcuimtT1oD%2B1P%2Bxm7fvPRpw7o6XCBQ1YE2y6oofIN3J6aBJOw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b2281c6cd8d4e80-FRA
2021-11-22 13:29:29 UTC	14	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 00 ff ff ff 21 f9 04 01 00 Data Ascii: GIF89a!
2021-11-22 13:29:29 UTC	14	IN	Data Raw: 00 01 00 2c 00 00 00 00 01 00 01 00 00 02 02 4c 01 00 3b Data Ascii: ,L;

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5092 Parent PID: 6020

General

Start time:	14:28:43
Start date:	22/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true

Commandline:	loaddll32.exe "C:\Users\user\Desktop\2zTgaLRFkL.dll"
Imagebase:	0xdd0000
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: 2244 Parent PID: 5092

General

Start time:	14:28:43
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\2zTgaLRFkL.dll",#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 2076 Parent PID: 5092

General

Start time:	14:28:44
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\2zTgaLRFkL.dll
Imagebase:	0xa60000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.911757798.0000000004620000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.911635582.0000000004600000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4888 Parent PID: 2244

General

Start time:	14:28:44
Start date:	22/11/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\2zTgaLRFkL.dll",#1
Imagebase:	0xa00000
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: 764 Parent PID: 5092

General

Start time:	14:28:44
Start date:	22/11/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff7949f0000
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: 5132 Parent PID: 5092

General

Start time:	14:28:45
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2zTgaLRFkL.dll,DllRegisterServer
Imagebase:	0xa00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.911557435.0000000002ED0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.911406171.0000000002EB0000.00000004.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: iexplore.exe PID: 5164 Parent PID: 764

General

Start time:	14:28:46
Start date:	22/11/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:764 CREDAT:17410 /prefetch:2
Imagebase:	0x2a0000
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: 4380 Parent PID: 5092

General

Start time:	14:28:50
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2zTgaLRFkL.dll,abetfoehywujav
Imagebase:	0xa00000
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: 6004 Parent PID: 5092

General

Start time:	14:28:54
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2zTgaLRFkL.dll,abjqkqaxstop
Imagebase:	0xa00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis