ID: 526201
Sample Name:
619b721d39f71.dll
Cookbook: default.jbs
Time: 11:36:24
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

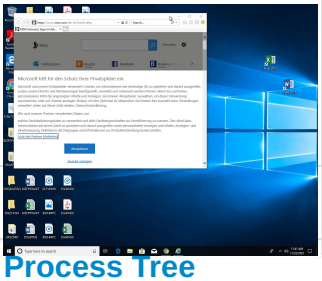
Windows Analysis Report 619b721d39f71.dll

Overview

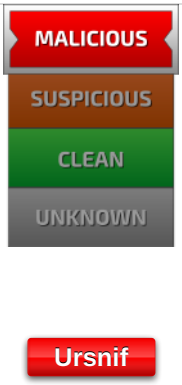
General Information

Sample Name:	619b721d39f71.dll
Analysis ID:	526201
MD5:	5adbb59a4def2a9.
SHA1:	5a64fc794c133a5..
SHA256:	e5ddae0f09c15a7.
Tags:	dll enel enelenergia gozi isfb ITA ursnfi
Infos:	

Most interesting Screenshot:



Detection

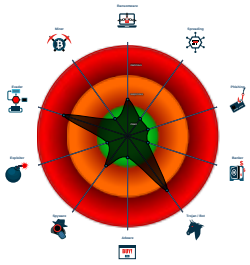


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Tries to detect virtualization through…
- Potentially malicious time measurem…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- 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 …

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 576 cmdline: loaddll32.exe "C:\Users\user\Desktop\619b721d39f71.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 5708 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\619b721d39f71.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 984 cmdline: rundll32.exe "C:\Users\user\Desktop\619b721d39f71.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 5308 cmdline: regsvr32.exe /s C:\Users\user\Desktop\619b721d39f71.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 4404 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 6204 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:4404 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 5180 cmdline: rundll32.exe C:\Users\user\Desktop\619b721d39f71.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6268 cmdline: rundll32.exe C:\Users\user\Desktop\619b721d39f71.dll,ajdpigjhocqby MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6368 cmdline: rundll32.exe C:\Users\user\Desktop\619b721d39f71.dll,arjmszzymit 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
00000002.00000002.839159615.00000000031D0000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000000.00000002.838163135.0000000001100000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000002.839120739.00000000031C0000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000005.00000002.838215057.0000000000CE0000.00000004.00000010.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000002.839122166.0000000004CB0000.00000004.00000010.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.31d0000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.cf0000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.4cc0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.cf0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.regsvr32.exe.31d0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 7 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

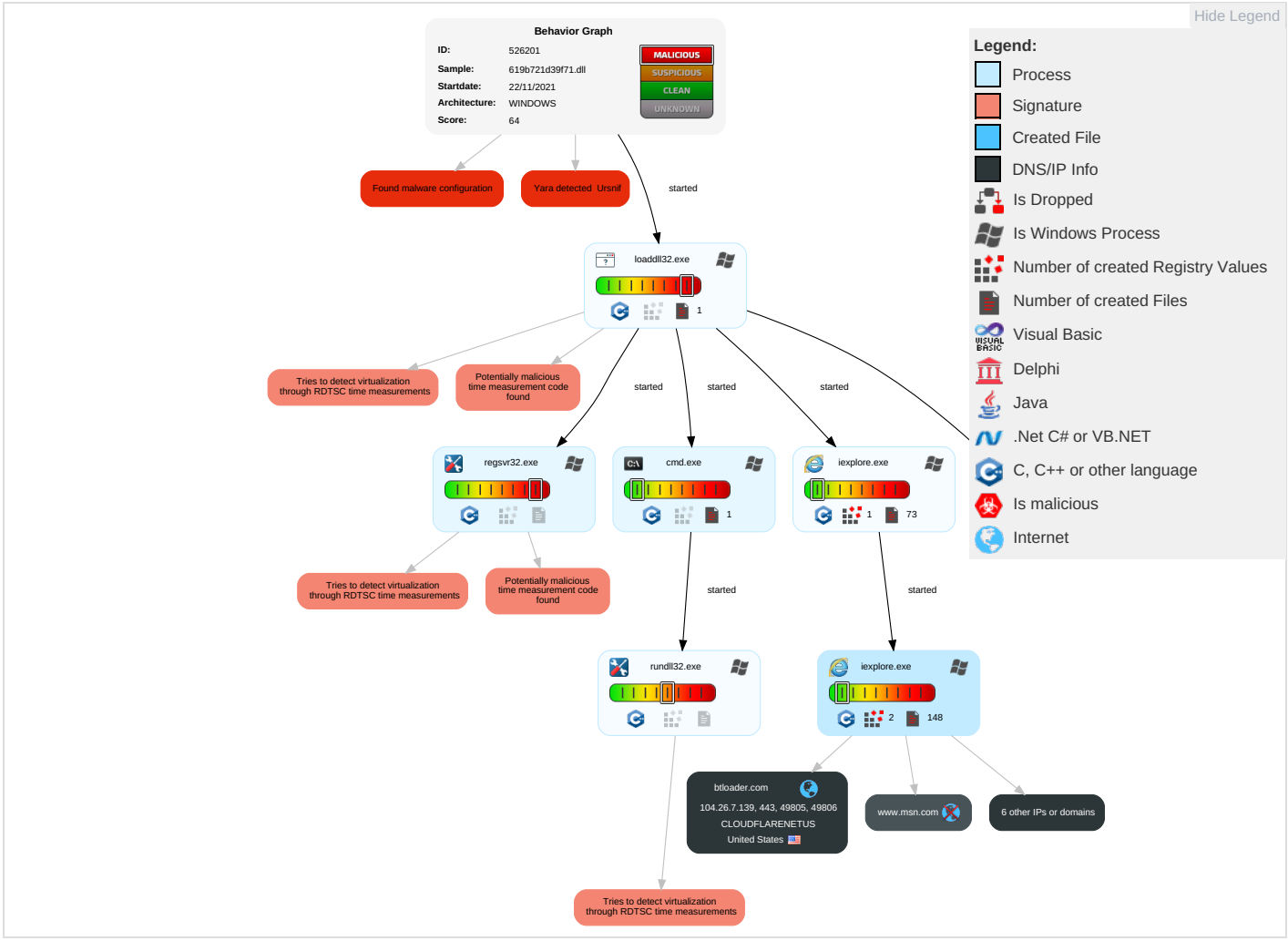
Remote Access Functionality:

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	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 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	Data from Removable Media	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 Bacl
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	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

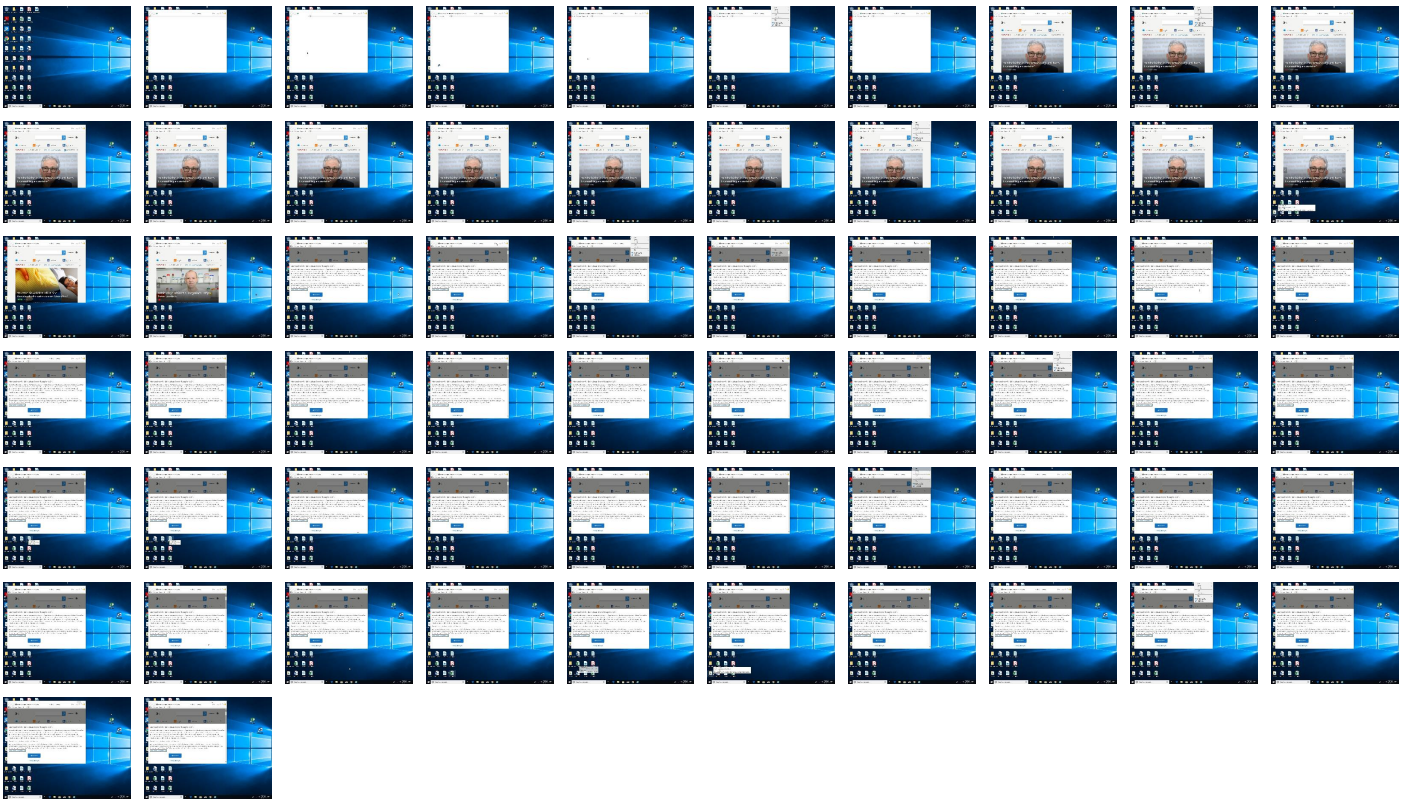
Behavior Graph

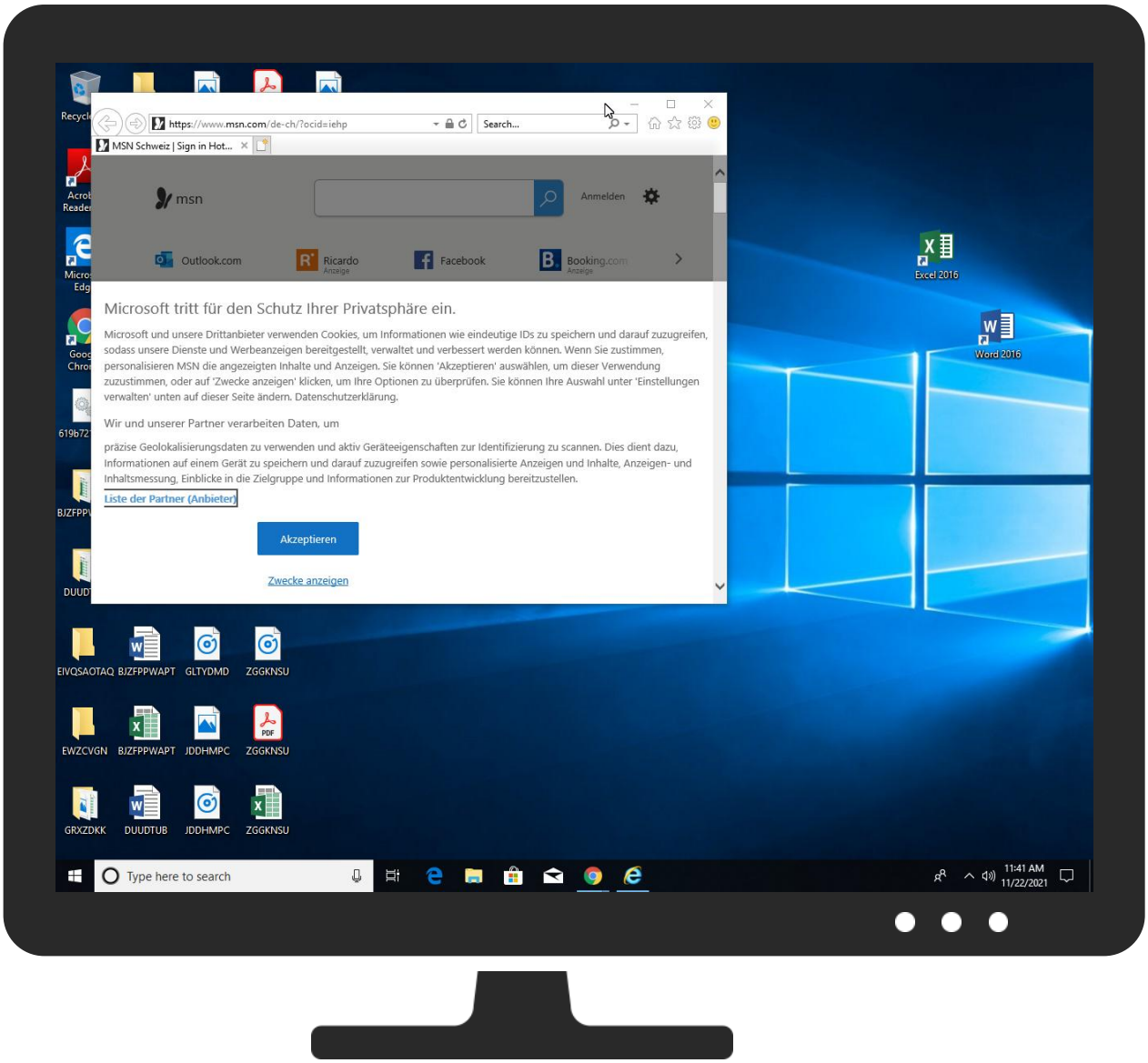


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
619b721d39f71.dll	3%	Virustotal		Browse
619b721d39f71.dll	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.rundll32.exe.cf0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.2.loaddll32.exe.1100000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
btloader.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://https://www.botman.ninja/privacy-policy	0%	Avira URL Cloud	safe	
http://https://www.queryclick.com/privacy-policy	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	
http://https://www.stroeer.de/werben-mit-stroeer/onlinewerbung/programmatic-data/sdi-datenschutz-b2c	0%	Avira URL Cloud	safe	
http://https://silvermob.com/privacy	0%	Avira URL Cloud	safe	
http://https://tools.applemediaservices.com/api/badges/download-on-the-app-store/black/de-de?"	0%	URL Reputation	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	0%	URL Reputation	safe	
http://https://doceree.com/.well-known/deviceStorage.json	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	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	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	2.18.160.23	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	104.26.7.139	true	false	• 1%, Virustotal, Browse	unknown
assets.msn.com	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
www.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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.7.139	btloader.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526201
Start date:	22.11.2021
Start time:	11:36:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	619b721d39f71.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:	19
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@17/118@8/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 92.1%) • Quality average: 80.2% • Quality standard deviation: 30.6%
HCA Information:	• Successful, ratio: 72% • 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
104.26.7.139	0MGLPJiSa5.dll	Get hash	malicious	Browse	
	malware.dll	Get hash	malicious	Browse	
	wMidyLtyIL.dll	Get hash	malicious	Browse	
	Fuutbqvhmc.dll	Get hash	malicious	Browse	
	data.dll	Get hash	malicious	Browse	
	5555555.dll	Get hash	malicious	Browse	
	EYWCET97LV2U.dll	Get hash	malicious	Browse	
	EYWCET97LV2U.dll	Get hash	malicious	Browse	
	GLpkbbRAp2.dll	Get hash	malicious	Browse	
	44508.5578762732.dat.dll	Get hash	malicious	Browse	
	bebys12.dll	Get hash	malicious	Browse	
	Payment 2280_2.dll	Get hash	malicious	Browse	
	Order_21182_2.dll	Get hash	malicious	Browse	
	Bill.10099_2.dll	Get hash	malicious	Browse	
	0QVwqx6bPL.dll	Get hash	malicious	Browse	
	zuroq8.dll	Get hash	malicious	Browse	
	zuroq1.dll	Get hash	malicious	Browse	
	nextNextLike.dll	Get hash	malicious	Browse	
	tbConn.dll	Get hash	malicious	Browse	
	w6fIE0MCvl.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
contextual.media.net	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
	wsEUOSJMF6.dll	Get hash	malicious	Browse	• 2.18.160.23
	wsEUOSJMF6.dll	Get hash	malicious	Browse	• 2.18.160.23
	X4V4jFmFhO.dll	Get hash	malicious	Browse	• 23.211.6.95
hblg.media.net	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
	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
	wsEUOSJMF6.dll	Get hash	malicious	Browse	• 2.18.160.23
	wsEUOSJMF6.dll	Get hash	malicious	Browse	• 2.18.160.23
	X4V4jFmFhO.dll	Get hash	malicious	Browse	• 23.211.6.95
	EYWCET97LV2U.dll	Get hash	malicious	Browse	• 23.211.6.95

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	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
	New Offer.exe	Get hash	malicious	Browse	• 172.67.182.50
	items.doc	Get hash	malicious	Browse	• 104.21.79.142
	VN-98766.exe	Get hash	malicious	Browse	• 104.21.19.200
	new order.exe	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO 842321.exe	Get hash	malicious	Browse	• 172.67.188.154
	UVtbsFD7YT.exe	Get hash	malicious	Browse	• 172.67.188.154
	gj6m12wLo1.exe	Get hash	malicious	Browse	• 162.159.130.233
	hrQxkblsgx.exe	Get hash	malicious	Browse	• 162.159.134.233
	5Kt0MqaTKc.exe	Get hash	malicious	Browse	• 104.18.114.97
	IRQ2107799.ppam	Get hash	malicious	Browse	• 104.16.202.237
	Halkbank_Ekstre_20211101_073653_270424.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Y5EGM7BygT.exe	Get hash	malicious	Browse	• 162.159.130.233
	(SA213-317L)_INHA_20211122.exe	Get hash	malicious	Browse	• 172.67.173.148
	wxnDURlkJ3.exe	Get hash	malicious	Browse	• 172.67.160.125
	(SA213-317L)_INHA_20211122.exe	Get hash	malicious	Browse	• 104.21.89.55
	NGjsDJbDUp.exe	Get hash	malicious	Browse	• 104.21.79.142

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	AP_Remittance_SWT130003815_0.html	Get hash	malicious	Browse	• 104.26.7.139
	Order Enquiry_CRM07540001965-pdf(109KB).exe	Get hash	malicious	Browse	• 104.26.7.139
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 104.26.7.139
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 104.26.7.139
	malware.dll	Get hash	malicious	Browse	• 104.26.7.139
	kZ45hWt9ul.dll	Get hash	malicious	Browse	• 104.26.7.139
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 104.26.7.139
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 104.26.7.139
	loveTubeLike.dll	Get hash	malicious	Browse	• 104.26.7.139
	ATT00330.HTM	Get hash	malicious	Browse	• 104.26.7.139
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 104.26.7.139
	data.dll	Get hash	malicious	Browse	• 104.26.7.139
	TELEFAX_Davidson-techOLX831OLX23AY2AY.HTM	Get hash	malicious	Browse	• 104.26.7.139
	Receipt_INV_460Kbps fdp.htm	Get hash	malicious	Browse	• 104.26.7.139
	MrBfVHgunq.exe	Get hash	malicious	Browse	• 104.26.7.139
	Kathleen.xz.0.dll	Get hash	malicious	Browse	• 104.26.7.139
	TELEFAX_SaccountyZNT142ZNT08YN8YN.HTM	Get hash	malicious	Browse	• 104.26.7.139
	Remittance-11162021.html	Get hash	malicious	Browse	• 104.26.7.139
	delta.dll	Get hash	malicious	Browse	• 104.26.7.139
	2021-11-15-DLL-returned-from-softwareupdatechecking.at.dll	Get hash	malicious	Browse	• 104.26.7.139

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):	5.198173440983228
Encrypted:	false
SSDEEP:	3:D9yRtFwsx6wmxvFuqLHIfiAANEJGX7T4mEYldVzBM9qSmSFAFKb:JUFkduqsiAANEIXH4mE8dR6ljukb
MD5:	5BE8E142DE15891774A5ED02F0AC2DAC
SHA1:	DA08647DC46CE1F19885DB3C1D15BDE32F34A9EC
SHA-256:	183AADDA54F07088AA89C640AA45819DB1633A89333AF7555E1370A7FAFFE492
SHA-512:	21E3548155BC80408A42298B2E8731E0F91320E7BEF6BF8E64C2EE33DF8A2D4DB46DED0F4B86621D5DCCA4CE583D802681CE5431105B1F78C7DE240973893E9
Malicious:	false
Reputation:	low
Preview:	<root><item name="BT_AA_DETECTION" value="{"ab":true,"acceptable":false}" ltime="2172231040" htime="30924760" /></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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\contextual.media[1].xml	
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9B18B08C-4BCB-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):	5632
Entropy (8bit):	2.0520323506393527
Encrypted:	false
SSDEEP:	24:rwvOGo/QMyhGW/Qy3Jy8AJy69lWmc9lW8:rIOGo4MeGWogV0omR
MD5:	1EC97528AF9F8138724DBAF800FC832C
SHA1:	8256354E515AE8EEA216A2F3A47343F06281EDDD
SHA-256:	83417D63E45AD7847C4BE37CA190AECBA39B2F8CFEDDA1305E1791EEF1BE091D
SHA-512:	0EA78542B866EBC3B7E942E5371A48237A627AEF4D4CDF68B8B0E8205F5CB4B0F93916EF2EBB4DE2BB314B98795712AA1575FFE0D9CCAB7351FDA6161D8B3E 70
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....o^.....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.j.b.A.Y.m.8.t.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\{9B18B08E-4BCB-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	332288
Entropy (8bit):	3.5959689270887703
Encrypted:	false
SSDEEP:	3072:6Z/2Bfcdmu5kgTzGt6Z/2Bfc+mu5kgTzGthZ/2Bfcdmu5kgTzGt6Z/2Bfc+mu5kn:ztvt
MD5:	7179AF671CBEB609E5DC3D81AF362FBA
SHA1:	D8BF8769893E51156A847262D3B553C1AECB7717
SHA-256:	4538559499BF1FA91B9C870A9819DCEBDA2394E87C77C75FEB77E12D580FF731
SHA-512:	FA74CB7EAF3DD5A721820A28FCD77BB861DD2965E3EAAE3281DFCC27A280DF94B6749549DFE065C6BC6744F468589B46E86882391CB71205195EA1F302E1DAE B
Malicious:	false
Preview:	.....>.....F...G...H...I..... .....R.o.o.t. . E.n.t.r.y.....I.....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):	5.134746109708556
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc41E01usRpATD90/QL3WIZK0QhPPFVDHkEtMjwu:TMHdNMNxOE01usRpAnWiml00ONVbkEty
MD5:	6CDD598642AF0B2B58A4F97ECBA532B2
SHA1:	864D8C6C5BCA339FB27EE9D4B26E1765C75B29E1
SHA-256:	D122C021FC16C2978F0E3DF7EFDAE945244D5E0DB2EF872EA6F9C734A9C7ADD3
SHA-512:	DDAE3716AC97F9B2FC30A90D6D336F22627D66C6F9C45D74C8B5C690A1BACE7430C3735EBA47F2E3D22B85AEEA5E320533C1FDCEED6026E8D69166820E4257 D3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x944461bb,0x01d7dfd8</date> accdate>0x95f64eb3,0x01d7dfd8</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\T witter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.1418483901658485
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4fLGTkkdLU6uNBwATD90/QL3WIZK0QhPPFkI5kU5EtMjwu:TMHdNMNxe2kkhU6uNBwAnWimI00ONkan
MD5:	8438DD5297BC629286F3668EB943747C
SHA1:	78B53193C1456BB7B6524EB825C725ABCDB0F839
SHA-256:	D53EAA127A84E15192FE9C10C222C8C7725FB37E819D8607EF1480A02E1CCDCD
SHA-512:	FC212A073E7527AD90CD5532EF23E3B320FDDACE1CC4B14CA15478000A989CFE1C9F837BBF5CAEE3A6C6EE79554E49FFB9F3C655F4D4152F3456078D2D84808
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x92a0c458,0x01d7dfd8</date><accdate>0x92bfc2ff,0x01d7dfd8</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):	5.1502735484885145
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4GLlauNTATD90/QL3WIZK0QhPPFyhBcEEtMjwu:TMHdNMNxvLlauBAnWimI00ONmZEtMb
MD5:	AAC60241DF5F75442879A00B44DEDE49
SHA1:	C71A31C454AD6781E3350AFCD01B053CB3B599FC
SHA-256:	5E0FA25E53B392F1467902C998A16760B39AFAA6ED17F085137A235543A73722
SHA-512:	4E9B85C3D7AB2AE296CA5066AD91AA4C158115A0CF4A8CBED688DC1B0DD37C0CB8A0FC927B8CE56A61FC232F29A322A070497443ED78777AF971AEC64D0813B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x988752b3,0x01d7dfd8</date><accdate>0x99271160,0x01d7dfd8</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):	5.111143752545607
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4JIowud5V/ATD90/QL3WIZK0QhPPFgE5EtMjwu:TMHdNMNxi3wuh/AnWimI00ONd5EtMb
MD5:	1B90A220B0FF546582AA1ED000BB25ED
SHA1:	C92811902B66F268C10F9516B77E02B65DB9EF17
SHA-256:	32DDBD499F51B9B9D2701ECE7300150503BF3774B6F418A9D633B6AC89361FDF
SHA-512:	0609BBE311AE95F8071C1E10FDEA5BA2397E1609EADA0AEC4EECD10CEA4992E6E68985DFDC34B1C2CC210A466C2B097AB0AC7FACCA9037AFFAE565431ADAC227
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x934081ef,0x01d7dfd8</date><accdate>0x935f805a,0x01d7dfd8</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):	5.134308679479284
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4UxGwAF/u0OBwATD90/QL3WIZK0QhPPF8K0QU5EtMjwu:TMHdNMNxhGwAF/u9BwAnWimI00ON8K0z
MD5:	2B1CC4B410D502FC1E66CFEC211F9B10
SHA1:	F76BC32819432DEB5C267D06941F61AD9243E923
SHA-256:	315CD73CF4B849082E86FB36EE524ACD80B654FEE8009B04D7F058EE3E0D9F89
SHA-512:	11B1B65C0528632536AF3245D96CFA228DEC25396925346B7762BFDE20A1789FC7FAF7AC39D701876E0E4ECE206B1A4502CBBBBBC5247850D42B336DBB28416

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x999a977c,0x01d7dfd8</date><accdate>0x9b8a8086,0x01d7dfd8</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):	5.11228855708839
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4QuniX/uQ7ATD90/QL3WIZK0QhPPFAkEtMjwu:TMHdNMNx0nivu+AnWimI00ONxEtMb
MD5:	FFBFFA81F0811E122CB18F611020B348
SHA1:	482CB98847D561764146F8AE207D8ACFFE45A028
SHA-256:	7AC852E397AB49B1693E91358BEE90FDF535FA6E13BBF29E6D6FF2FD2D4FE6CC
SHA-512:	A6EDFB479DF680A82F16C4FB2992BF18414A5C4726B6839A033D19DA095042E6C4D623C33B6D24F7100A4587D4BBD6E1671A5463B131813F3755D3D1CFEDA33
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x940d8c55,0x01d7dfd8</date><accdate>0x942c8a83,0x01d7dfd8</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.166648237603958
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4oTPEwusd/ATD90/QL3WIZK0QhPPF6Kq5EtMjwu:TMHdNMNxxPEwukAnWimI00ON6Kq5EtMb
MD5:	AC83939AB503561FD99EF4D6A9745663
SHA1:	0F961893F7A616624EA75DAFD25959EB2B75943E
SHA-256:	E5F020E3ECAC0D3E1420E9AA0960142E46AD94E7BAAB67310F3F6F599F2F2779
SHA-512:	DB29698262270B5F1746ECCC399DC0F2F916EF937E5439104AB2C55B251664C7909C620AEE6063CFDCE0BC6F779DB4A12AF58632F74E15E14F1AAE26A9A494A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x937e7e76,0x01d7dfd8</date><accdate>0x93f81645,0x01d7dfd8</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.151840309655415
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4YX2n4AwuQLYwATD90/QL3WIZK0QhPPF02CqEtMjwu:TMHdNMNxc4AwuM/AnWimI00ONVEtMb
MD5:	7579A7700C64AA765D805128910B0DF8
SHA1:	DC2964E6D0439A4F4443DC85B26B7C6B9A6B6186
SHA-256:	D6B795766CE894DD5EB675C40A517E62F9E0B16425B653C605714DB9839C5B7C
SHA-512:	347329937295EEDDFDCD46FBC87FC2BB41FBFCD875FFBFE3BDB6BCB0401324D93BF3F480B66F4C0353667C3E1092E4C5A5B2642A61E14989D03F5BA8B749D5E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x92dc6006,0x01d7dfd8</date><accdate>0x92f43659,0x01d7dfd8</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):	5.098487494950754
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4Insw1un4ATD90/QL3WIZK0QhPPFiwE5EtMjwu:TMHdNMNxfn51u4AnWimI00ONe5EtMb
MD5:	DBF0A83FF9DFF5B7697FEB68BA26F1D5
SHA1:	0C37D0F50376F15A3B961CAB528CE67FA12E8A42
SHA-256:	04515914ABD103BFF059648F95EF936F7B80C1E90BD26210428E9C3B1A22BBB5
SHA-512:	AF288B2FAEF98018B698DC3EAC9845D94957B0D7C2AA46307716D42791211F8E4D26391EBCA6361F825D6EBBB510DA6BD884BE8E04740DF1A50677C348335C7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x931334f8,0x01d7dfd8</date><accdate>0x9328aaaa,0x01d7dfd8</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	22330
Entropy (8bit):	4.293009581776701
Encrypted:	false
SSDEEP:	96:eQQQQQ1n9KlyzS29dcBUXqupkE1OwDzXIzS29dcBUXqQ:3n4QzSAcBQpkEgcz4zSAcBq
MD5:	2E568573A391D6D98B5328BD1DFF1F34
SHA1:	3135BE1D6125B069DF0B772F67165C815DBCD22E
SHA-256:	921AE65C7C2E4B4D2EF8553C9FB9791C4FFAD7C488C19C23FF28358CDD442867
SHA-512:	9078CDDE45BFB60E985E0038FF058F4B5CB669067B9E3D9562224E64EA56E4AD304967265C88592D9EF870DB13078D217FDF651ADC2EDD6A089D5A8A8F8C2A5
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\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+nSECIr1X/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............($LKloca...`...f...f....maxp...P... ... .name... ....IU..post....... ... .*...........I.A_.<........... ....d.*.......................^...q.d.Z...3.......3.....f..............................HL .@...U...f...................... ....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.d.b.d.b.d.,.d.,.d.b.d.b.d...d...d...d.7.d.b.d.1. d.b.d.b.d...d...d...d...d...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...d.r.d.I.d._.d.b.d.b.d.b.d.V.d.Z.d.b.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AA6wTdK[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	550
Entropy (8bit):	7.444195674983303
Encrypted:	false
SSDEEP:	12:6v/7jGhB1J/EfQCF2bAVNvYxZxdgQ+JIy9XD5hb6Fg9a6:ZJOf0APgfG+o1oFgc6
MD5:	6468CE276C808DA186AEF8AA10AB8DCC
SHA1:	F11A97DE272DAE4A61EC9990DEA171EFCF39B742
SHA-256:	CF782CC89F554E9ACF21D36909F6AC19DDE218BF0250179B48CDAB67728912B8
SHA-512:	6439670A62A38D289374812D5DACCE219D01E19F5CC4CEC4105F72BA703BF70078FC92DFD2A2C43669AA78EE8D03121E234E53DD3C73DF6CFB984049CE3637(
Malicious:	false
Preview:	.PNG........IHDR................a....pHYs..........+......IDATx..R.O.Q.=...Z.mq0-0`M....t...0qqjM.... .tq.&R..p...$......0P.R'.M.A.#......=H.(1......s..}.oGOC.:.M.&..S>...W.....t...^..}..... .b.F6.R..,.PN...n...@_[...4.+.]..-4K...54........w.....r{..3...9W.~.>;.G@.F...Q.Bx..AW....J.g|.B.q../..._M...T.4.....j.G......}B7..`..B1.!...w3.hW.....+...p...D......&,#.h...D........T.....V ...H..`...,,..........Qb.h..g.a~<.............K.p,...|......@S.l5.?.r).&....<{ad3.P.,M...H..W........SI%.WX.q>..8.....Z.V.n.U.......\..... ..7....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....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...I.\'.....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\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
Encrypted:	false
SSDEEP:	768:IaBjbh6TFQqvZ54il2R40NXypZfdvRB+6KCOfH:IaBXOQqX4igl4zZRB+ffH
MD5:	62A8482CFB648DD0D95E83D2B22FAE7A
SHA1:	D6F0CD6A1834A60F4C5994067CED244E2E921FA8
SHA-256:	8361D066356EB990AF5B6D5E6A77225982A6B40D3BCA809274FD3FB40F6FD92D
SHA-512:	A6834B4CA196B46432AA31C5A5F0EC16E41852C2A2D7D09C3374CC942795DC4A0A958C7DC72DA6FFFB6A437462AF67C75FC01FFABFC9565A7EACB0C9F9DE2 B3
Malicious:	false
Preview:	.....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....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\4PB7FJMT\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:IWHFsyTdItpTdhivJBZH0t+FS

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQVtAu[1].jpg	
MD5:	E816AA08895A8364BBBFE53AD815ED4E
SHA1:	17B84C624BA2CDBD33D301A55A91582BDB7AF63D
SHA-256:	F800A4F3965D72E5926E78D37DD60DA9C5B5CC6C4C03C615DE4D6E20C56D1036
SHA-512:	7BCCBE050D366D53B5F6D79F085E666799170B0CA4B143F2125A2563D4A81C6392CB2494DAF1CB416FAB0950FF59879A8FF49996E6F0486FA38BB2F4EC703B05
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.....?..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\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
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..d`....2..F..i..M....H.Fr..,&.nL.\{.L.P..$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\AAQW6nE[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):	20589
Entropy (8bit):	7.955212462976607
Encrypted:	false
SSDEEP:	384:NRgkdcnUYvqnF91wCJHVk+5eCrdJpU3udJPVZjEwyC829ltwzgm:NKkGnUYSn/1wO1kCe6JpvbPIUbm
MD5:	DD653B09C0287070A7DA33AD5DA01123
SHA1:	5D1DBF57B3C62FD93D545278B67B2C06E36EAB06
SHA-256:	9213CCF328811FFB440C06D202A1CC1A3C9438139C3CA1DBF58506079014F706
SHA-512:	5DA584F8EFDBEB940A4B4A17AF631BC456262D2851F1B9EE0041DABAC5C928B19BEE6578F2AF5731E0A7E50F9E0159F9E5428D39FACA4B0B5188EA713BB55D42
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..9l....9].Z..gI[.(.....4_...ED.C:*..y.G&....v9....k./..np}.V..s4=.....$.:..Q.=.t..X.u.i,..?.~.....OI.K.c..Z')".`pA."'..OTI.l...y4.....1..i.fi.J.....R.F..&....4....0.8.p.W...|.3E.1.J.r.@L....d..#p.|0.i....H...m.$c.>....N.r...c5R..w.Sr.X."x+..]...R..\.i.\..#q..C../[..:x3.$...~.)=..S.#n..zE.MiL.n`V...J..=...^.....+4...6../.n.....s..=...Y...6O.*y.....z..#W..,..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQWMEO[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):	17419
Entropy (8bit):	7.521403114504258
Encrypted:	false
SSDEEP:	384:IFjNEFe0TZUIybheFYNNUvS8uB4sB3MMKflJOWPUlG0nRdY:IFaFxqPbE2HSgB4sB3MjIsU+
MD5:	A177E358F1D71BEC14F0E20C6807E0CD
SHA1:	680C8E5BB94A25799D9AAC3665B4344DE914F25B
SHA-256:	A9A942B2563A787837D53238BC097B0F97B25D201F3EBAE919859C3834ED8E82
SHA-512:	FF6AED14F3FFA9C2A1600B04DCFF520BD4682757DEE7CD16B4BEB1C51DBC700B858B169568C143DD973B66DC9E69D81581B39E90B117DEAA9230689C01912CC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQWMEO[1].jpg	
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..Q.....C..&(..P.@..<P...(.....P...(...4.P.@....t..P...a..L...3H.4.3@.@....@...(.....Z...(.....R...P....(.....M.%.8P....h..&...N..P.N....h.....(.....4.P.....P..@...e0..QH...C@.....P..(.(.h.....P.....J.(....@!..P.(.h.h.....Z.P(.h...6.....M.)..s.`.h.3@.h.z..h.....@.Z..R`.....:..h.....`4....\P.P.@..%.%.(.@.....P.P...L.....h....4..@....@.....J.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQWN27[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):	20084
Entropy (8bit):	7.952135561729653
Encrypted:	false
SSDEEP:	384:NkutMulvimxLMdBGbDRbtuDg2Kqz99Jo62163cXjdyPjjydXA+LYOj9brbd+jyXw:NkutMy6mxLeUNtuMABf/CgczGfyxA+LW
MD5:	0F85A59AFD921E06E739234EBBFCFF7F
SHA1:	0A081F5CDA7224A219E97E6668FE5C079F473F3D
SHA-256:	86F91238B0C5BA5D297E3C58835DA37D58A00FA218D75FC1FB9B482CD75A2CE8
SHA-512:	E8E1C93F9114DFF133A8CCA08D8FA10870E7550193377C4A069EBF625B4803FBA6121563B5470FDA5498BF3E96ECD52C02354D2B1002CD0F3D115261EA1ABF7
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..W...V...~.y.Wh..B*..#l.&N.z..G9..Km.m(.....K..f..@j..2.&.b..4...h.0h...././jk....v..G...7.....e.kBO.3.S....d|..R1.q@.4..@..3`.89...[...a.k".M.,j.M.H...\.W)Dd..9S.hLM.....)...%fF.#4.....'h.....L.14.....H...q..q.Y..&...Z..^G..9<S...+.._7#...NBE5..H\`.T.B..XP...{.\j..".....B(.....[.t...].e..R1J.@.....@.@?z.Z...d '.B(9.@....`.....6MWAu)H..vg5.d0&.0p...V$.H.p.....d.a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQWQUY[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):	2014
Entropy (8bit):	7.761983314281628
Encrypted:	false
SSDEEP:	24:QI/OtlM0XxDuLHeOWXG427DAJuLHenX3nny6fPrXACW8pZ/DWbakmIoEO9TQ+xlv:QfAuETAZlL1WS/DWb/FHQdFeGsy4NQ
MD5:	29607252C5FCF2A96368732F1A8900E8
SHA1:	F423E8FBC783CD29F69E1596005F1410FCCB9769
SHA-256:	23B66500B6A0FCBC3931FCB7A4DB1AF67872176B0CB0555AD63CAE1C23697D68
SHA-512:	C2B4EA8E1821EE5318E9DE38ED3142364EE759BC2B4C9B7EF0C72AC344C90BFFDC47F76E5B13532BB79D3B4A060CF8C0389FE2CF40BEB987459973C398FEFF E4
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..Uk...*..2.h.d..Y6$.@#[C..4..Q._S.../.ZI.8.....e...{Tev.y..y...Q\.75.v.2.r|...I...p.oFy..j..t3.}...J...B.Oc...Z...`&(..D....*.-....J .h...)..vmm.%Y.B.^k.....s....q.I.us$P..6....y.....s...3.....p.p.tS..j%f...a]....._....-..t.....J...GC&Z.K&A[D...Q.....r..f...6....r.:..[.XZ.....K...#....Fq.O...F...[..#}4...]...7L..4..C(e9..]... ..*/...q=..t...P.R..Z..$.V.e...g"e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQWRAi[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):	17965
Entropy (8bit):	7.9402624985944374
Encrypted:	false
SSDEEP:	384:NPtDaOvnt5+0KR2ajeLaXpVG6+PE/AD8N3nC7xVgqg27nycCyHgfAF0z:N9WX7MJsYD8N3C1QSyclHEN
MD5:	62DC31D42C2073E578061D8AA5AF9880
SHA1:	6151EE880C1CC8A7B45CE2C45A8C148F1820F495
SHA-256:	32D920A227FB52AA1A5503287ACF9A37F8108E806E43B2F6BAF0165CB12B20F2
SHA-512:	42C0009CC3295F4B9CF46C3D0D2ECFF55DF3B3F701B270AD77BB96DDD39B13C9129994AD4F6C4AE41741B4BBC9BDFBE0BE73047CF0ABFD1DB7D11258F020F 5C
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.bi.G2.r.k>t+.W....r..+.V.8.z.Rj....-.*.$?M..$a#eMf.H..)&.(.Vq.=...._}EtD.....-..4Q.....D..y..._.....u.a...Z.....=.4....vY...C.=.M 0Q..@.(.....5.BI*.>f.zf.v)+...`...|..fr.....!.r.C..d..#.66.<f.2\K(...3'.ATH..0Fh.RK.[.H...X..{w...c.@.....$K.P%...L...8.d..@.@...Z.5...(.....}Jwb.!..Y..=....P.)..r=(@...U./J.v...3....'. *:V...[.C4.cm....&Z*...*..0.ZB.+I.Lw..)p...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQWeGa[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):	12503
Entropy (8bit):	7.861125255017763
Encrypted:	false
SSDEEP:	384:NOxz4RTFHGSd1PGyjC1qJvd/ernz9Bc+ACiUhb:NIz6TFmEGyEqvozJz
MD5:	593272E4883F05B819B99C6A4E27E320
SHA1:	7C0EAA8D680B0BD013F4215A9AED0BBBAB732ED7
SHA-256:	EEF26258D6D8B72752EC7D53B19DB2078F133898614EFFD4496620582E5A507D
SHA-512:	37AAEA107ABDEF120CD2C6230B7EA207A3FD7EC109006EDC8ACA0B5580E062E67DA22EC8B5F413F319B743BF1A967AA66FD5A76E3D9E077CE407B052D5D8EE7C
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....R1. #..0..I..R.....LA@.m....'e.zPH..?.....c..4...#&.g.i..a.(.E.|.....@.)..Z.<{...h...X..J,.I....`.....=(...1.@.....u."....s.0$NV....&4#...P.8...3T@)..,A.)..gz.S@....=.6.j.,...#4.F.....(....(.-!...2i..`....S..@7..S.>....Z.....2..b.....#...4.@.$9.....(.....#4.U...M..9.L.y4.4...c..i.%.9..7?.....\s.. .....Z....D.cOZ.(.4.P.....K'.....29H..c..N...@.....0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQWoU7[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):	39072
Entropy (8bit):	7.937923999480942
Encrypted:	false
SSDEEP:	768:Iz33XkqI9lFgFawfMJROOE34pQhywL9oXUw2Ms5GQKCe05qKt:Iz3kJTFt/JRQtMaAU35e09t
MD5:	1EB143491D51EA684068584FB1D4EE0E
SHA1:	470E5E50E9487BA51353EA058460EEA098177058
SHA-256:	64441934637FB136FC9808C663C4380A43D8AEC4091BE648B4590E0F92BB0E5A
SHA-512:	EB068A6750CC6226967D0FBC8FBEAB189814A6E6D6AD8CF464887FC18F1EF1AE0CE394F81433F039245DF7A41362A4565A7261557A0D425EF54C4481B3ADA6E
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..om......_.Di.-.z~.LN.H...MP...J.kh..U.3d<BE.....?..XC7.+..s!...a...&].....7ZL...g5|....qx.>..'..9..j.r....{8.)T..J....Z.^.....f.#I.h.Q[.....u.;\.....P{}H..Mf.F[..D.....V3.BF....kv....yu....h.Wr..:Tg.h..}KJ[.q.{...l.LRM..@^.5#.q&.D@~.;...h.....m...h....&kYiQ.....b..V..M.H.... .A@.G.n.P./.C...E4.6..N..F.d....c.K(..)..-.uh...*.'.>..sh.!..4.....2.5 >.j...H.'.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQWsEr[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):	11880
Entropy (8bit):	7.731668592970506
Encrypted:	false
SSDEEP:	192:Q2908xINsE6DwPwOEEImdVbXKFFQswXNJCQEJirT0CjojrFvrAOogerQlfVj:N90AGsEkw4ObIyVbiEWJqTbjotvsOo8z
MD5:	CB5AA468DD63AE9D0B9F4C92870667DF
SHA1:	31EA2E9891AE477FC4D4CB829F44C5C1E3C7C664
SHA-256:	600E98F85715E3E3492E129EE55EC5AF7BBEA2E5C3EE5851785C1FD233605BFC
SHA-512:	A43E7CD39F2F6C993BBB26FA51AFC4D942DBDECC7B6587B4939B77ED952313569C642FE5863C34B44DEA99DF0B27260BA1B88B4E4BD615C6AA4EBF35A036E58B
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.....?....B...(.....0..Z@..(.....(.....@%...(.....(.....(.h...P0.@i...P..F..S..A@....(.....@..(.....3H.4.f...).P.@. .....L....%....h.....@.0..(....P.@.....P.@....J.(.....0. .....3L.4.f..@%0..Z.(.(.....L.....P.@.0..u ..3@.....J.Z.....P.P...@.@.@.@.BP.@.....(.....4...(.P .....(.i.f..h.s@.h.....Z.J.....%...P.@....P0.BP1i...(.P.@...(..A@....P.@..b.@..P...@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQX6iK[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):	7225
Entropy (8bit):	7.891107837881851

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQX6iK[1].jpg	
Encrypted:	false
SSDEEP:	192:QonVl2kIEvdQMHrLc40qcdloN+Mo14iPByRh86LpQT:bVl2laSMoqT4/BAh51QT
MD5:	7E1470608BEF10E4310324A4DB948F46
SHA1:	46179F4A40147CD02EA27E457E44388A16DB7ECA
SHA-256:	0BA6B7782DE6823CEF7D8607CC69D421EDC7D2D3188D73E4EB132142F1E8EDF6
SHA-512:	AA6DCC43E01ECEA4D1B59E087164A2D4AC75AF856A5AD595286F5989B81262AE56654C7489094BEAB0D3B5669F5B3B598EA249E6FD3BA56319FF46165EF9C85 4
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..>.7.s..''..M.@r .d......Oz..7....*..?....QE.Ty1...$..Z6.....w..M..#B..P..5-...qM-.$.....\.V.Zfkn...r...mL..1.H.{"...%l\..>*nn.h.k...S Z.+".'f@...H....jnl.c.25.....g.t.1R"....)+..$.[S8..KS.D!.J....kM.SZ..B.#P....@....P....3N'=Vm.jb.Z.r&.s..=H.....R+XE..E%.u...Y.9..Z...._QE.x.$]'..o..l.Gm.:+....i.q.n.%)..fQn.3.E... .....J....*..hT....'3...Z....h.2....0..Q.m<k...T.!E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQX9PM[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):	13851
Entropy (8bit):	7.95415540606334
Encrypted:	false
SSDEEP:	384:bu9YHVX4da6dEVva43+ppjh4WwaVT27jyUc:bLHZ4o8k+R4WwaVq7jyB
MD5:	E2C9D4F07D49AB62D2D8D02410A365CE
SHA1:	0046356F6FF5284C878A11B899D26DBCC8FDEAF8
SHA-256:	798FC89242999671AC2AB6D0508F3A9010977939E05D91458E7305E8380F3754
SHA-512:	737562969550262F4E4DFAB02E215D1CBE0E30607E2D0454E904C74A9550061611287E7A94BB473F8A9B5A3F7D536458176207264E5A8F6CAC2EF726CFA1DC87
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?...@.XC(.r.m....#..BE...8.H.w."f. ......3.....O=H4Z.W.<..,...;P.*"..L.=Tw5...5.I.FG.......EZ.<..O.......`.c...?%@;FH.R....(..~b?..r.. ..;...=.i.AH.3..h.c.....}...)l2..g.EM.;.Y.d.fQnO.Eva..).2.h..<.I.y..2..8..3..K.W4J..M..H....!7..g.....@.39l.*....'.Z8S.V.t..K.n..V,fI...aN..L[...T.....T.(A...7....}...2.{..........G.K..> ........Ar.. .0G`3.@c....Mt..."......s..[........}.+....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAQXnHc[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):	7586
Entropy (8bit):	7.875929294733613
Encrypted:	false
SSDEEP:	192:Qovzkv7KVSxBgeAhTsWWYmLh1WJfwZiirx46OO:bvzsBgeAhD6LcfqiirGRO
MD5:	C337B0228F6F257A9C3016B47D02EC99
SHA1:	68BA1826BA5DB767E5561BF9E5889B7822672474
SHA-256:	D1F03ACA9C0474505E543903DA2405F200CC62E31A2B60A050D2EBA91E393715
SHA-512:	A47BC7FBCA60D26883879FEE0C26026B3C29B7ED348A5BC2469CD6B4E1DB3EB3B0DA3F0B2656F1B8F43D008BD82C0869B6493ED11657215344290E836B1AD1I F
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....A..!...*...Hec"7G...25.....\l......k...;....zb!_.)1...Dx....d.z...km....,.K..E.F...S.."k[.....S.....Q.$\b...h.sE.p.4X.d^kVz\...`7....4.6~".. B.....9.....k:..!....T.K....2(..9.L.m...G.1.@b..VW.L..w..~..v.S.[eXb......)..f\.=.....I......W......^R.W.......q.S.\...G!.4r.0...v...R.-....X>...6.~....W..w. #.i4Zg..>.[.....J.:`./...[X.....w*F..9.d.. ....Q..4.7P0..@..`(j..

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAzb5EX[1].png	
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\4PB7FJMT\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:	0E4BA430498B10CE0622FF745A4AE352FDA75E44C50C7D5EBBC270E68D56D8750CE89435AE3819ACA7C2DD709264E71CE7415B7EBAB24704B83380A5B99C66C
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..lz...&....R_.q.=p8....~.'...5..}.....,_.I$FS.\.c][4#.....+...U@fZz.Y.....|.7....r.x..S.?.ws....B9.P.-Yt*..N.}.'V.....G...5....uc....XV.=.{..ai.pw.v)...(.9.z\|.3:Q..,qr.es...ZTp..Mt.iB.2.{w.C*WB..F...b../.H..\..*.).0l.R.....c.....@S5.?3...q..:...8.?....p.=6`..T...5.nn.....].b.j.,..pf.....8...".M..?.@K...L.='.1.O.2Kb.p..(..\.D.....n..._.....0.....w^bR....v\..)..l..f..l..M.m.6t.7....U.Y3?.h=..!.<.._.....pL..V"[.....{[P....e07...Wc....IH.T@...*..A@.....;....>Gt&...}...o...KP...7W1.sm~...&.....00.....>/....l.#.t.....2.....L_Owu.*.A)...-.w.*.1/+.)....XR.A#;..X...p..3!...H.....f.ok;..\|x..1.R.\W.H\...<..<&.M!mk:\|....%.<..,.%.g..g..G@z^Q..I...T.D^..G.&v6$.J.2J....~..Y\kX.j.....c.&.>.3.....ek..+..~B.\.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\checksync[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):	21717
Entropy (8bit):	5.305602492520896
Encrypted:	false
SSDEEP:	384:fuAGcVXlblcqnzleZSweg2f5ng+7naMnpuZOrQWwY4RXrqt:A86qhbS2RJpusrQWwY4RXrqt
MD5:	677C48207F5A13E6D6DADF30D2D6C52B
SHA1:	10BCE9871F228CA247E92B0A6366D5FE2A4426C8
SHA-256:	16872C9C9305146F1665B47C30EAF0AF695450B80E6B659781C71E3B45526027
SHA-512:	7C35E7BE4917DEF18676DCD367EA060F9073A093D9B66D6104784845E8B3AA3C14846F617661384E9A4F07E9FE149156A0C54DBF1030CBB4ED972CAF5F115CF8
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\4PB7FJMT\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:	7C35E7BE4917DEF18676DCD367EA060F9073A093D9B66D6104784845E8B3AA3C14846F617661384E9A4F07E9FE149156A0C54DBF1030CBB4ED972CAF5F115CF8
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\4PB7FJMT\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","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\4PB7FJMT\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\4PB7FJMT\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
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\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\17-361657-68ddb2ab[1].js	
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.local Storage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find ("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c. data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("of fice")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-de pendent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\33b341a7-11bf-42ad-8d2d-b90ecd999fda[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):	77818
Entropy (8bit):	7.977041177841507
Encrypted:	false
SSDEEP:	1536:nnrO1vecaL66jy4QbssGEmw/mHXgf3Keq25ipoRCvAahHpI:gvecaL66QbsbEmBXKq2DMoahJI
MD5:	916397CB7EAB6FF49EFB327E8C423179
SHA1:	F136937445C3906914510D03CBCA6D469AA5C0A7
SHA-256:	C4DBCA3DC233B7BB4FEA711127920E7925031FADC52DC9162659DE69B7B2CA6A
SHA-512:	09A038EC20D272EDA434E77CF2B2A047D8AE4F573E92055D898335B8DDF452B32E82292BBF65DDFC672A21D818B7DDD57A89590B6D6D789531C4B330D1E9AA6
Malicious:	false
Preview:	......JFIF.....C.....C.....!...1."AQ. 2aq..#.$B...R.3....%Cbr..&4T.....D.....!1...A"Qa..q...#2....$B..3...Rb%...&Cr.....?.l|.iL...K....PO4,...F.*.v#..o..<.|.uF.K.O..a.I.'.%....o %.7.+A.pA....gB.B..=.....M.....5Ty9]*[/V@+H..(...&.....jX..f%...g'M.T*.....{6..]..=.E....jXr...O2)...P.w..a.....(..#0..0.%.j$.&PBJ....n,..=T.$.x}.7.....dt.J...B.M.5..`.3 .FK.~.6.+...9%$..P..l6.....Z....q4../..VGa.)I!..3..f.....<8]W.-.?G-j.....(N?...Gb....Z..Y.....(.r....i..CSX.u."..:.S"..g...>.M.?....U.....+Gy...7.\|$.:.@...A....&.R[v.....).<.!R#..,.%.! 6Fe:.P.&5..Q..:l.....R\.....y(Xi..A!`.N. ..!.<.c..k.....),N.`...eSnJ.w;...+.^k5&c1...w..;7.(...!IN.....y...o.v.....r.7.N,.v...[..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\3800c42a-77f1-4646-be94-2e7946c601e6[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):	79525
Entropy (8bit):	7.975780946113385
Encrypted:	false
SSDEEP:	1536:Fo03ECsPqXRuPIzOV0XHK/uVcKU1nV/kopHfLRAJuNzGgMX:q03ECsU7zzmurIh5zRAJuNzGgMX
MD5:	594A7FAF22FCB17927646DEF8D6260C9
SHA1:	CE047252BFDBED79130A5CABCDC8256E09A5BC7E
SHA-256:	A404724B5409AB4DB8A331B1B39E843BF73FFFD04043DB6D854C1E3DA2393E82
SHA-512:	5755B5D6437157EB7ABBDA9B1E64B9BE902D8F41953E676F14B7441CF5F0F3A0966E47F690B1C6A30A1BD5BF7AD44F08B2AFA58DCDB2FE2EBAF0A50A858724D6
Malicious:	false
Preview:	......JFIF.....C.....C.....H.....!...1.."A #Qa.2q..$3B....%R...&C...4bcr.FST.....@.....!...1A.Q.."a.2q..B.#.....3Rb...r.$Sc...CT.....?...a.....i...2J<j#....XA*..#Q...w&.j.....j.&C.yk. ..=B.0n.....l..+...WE..`2.0.a-...)Ze.L..Y,..yc.Z...G=.B#Q....TDG..f..S.....vq.9.B#..\tE...Gl.9..F....w.v_.t~..z=q...+%F...R....l.....-2".....{,r.....cF.....T..;....F../.....V..Ze..y..e`i..VCd... .dV6...!)..2...4.c..).+.q.z["..].U.{...^.#WtF.~....^..h..?...t.h5.....p.D`..Xn.e.)..Eq.d.Z.{j...5.1%ERE&;> ...d..+.Q...w...ee\.>.Xt.....hj..9^79..b0G.$vz.....b...9.u...l.K<t....f.=...ro..]. .y.....B53Y.S.t.,IU..]f.h.....)...E.4c^ek..U...]..*/.m."m....6O....f..W..U...!.UM.....#{..Q.U.M....9.k.U.EV.7...EM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3278
Entropy (8bit):	4.87966793369991
Encrypted:	false
SSDEEP:	96:Oy9Dwb40zrvdip5GKZa6AyYs9vjxWCKTS2jQt4ZaX:zqlipc6vxLCSCbZaX
MD5:	073E1A67C16B7E2B0F240F20BAC53174
SHA1:	778663FBA0201814BE193EB38E4F9D8875F322ED
SHA-256:	886E0D5D43DFB17D92EB8C5C80AB0671ED9DE247EC4AD9D71B358F32F7613287
SHA-512:	97FA869A8BE850E759BDB5AAA0E850B787358CC4EED55796F6B51D1AFD5B6B25CF7A6FAC5FCD67AA9588876F208D40449ED94886046177B6FEAA083743B01696

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Malicious:	false
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":true,"ScriptType":"LOCAL","Version":"6.4.0","Optan onDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca 92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs" ,"bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg" ,"sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um" ,"us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","gb","ws","gd","ge","gg"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	677CDE3738656508AEDBE2DA698B21B5AA15EBA8EDECE60192A5B61004E6CB6A1F718A02066AFF367021C31B9B13D2DDD703976E8F26C22272AE8AADBECC5 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\B87Z87FM\AAHxkqw[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):	780
Entropy (8bit):	7.63276321014427
Encrypted:	false
SSDEEP:	12:6v/7vOWYWeiBpmTUOEd01LuUviHQKP1tha71TDeII+HKV9WGGd4BzLNjFQFP68:IPec4UOEkIQK5CTiGSXGP68
MD5:	9EC146F1EC3EEF5735E36A1BE63B9C67
SHA1:	411DA70ACA1DB1A0D3F8B5F1ED616BD30C7AF310
SHA-256:	63C7EAE620F3D8F17ED979A7A09CCBFFB1577FCE29772CC3C8FEB1B6C2751856
SHA-512:	1F684E83509B4D92A9651ED1DDB35F09B206EE3824546BADD3CB2FD565155D752439A47E39E23F95C4051247F5DA37E8329769C3750A93D1D99CD47D7A5A17E
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.%S=kTA.=..6&f7.M0b...v.....$..j.../...VP.H.E,R. J..?!.hc..IV.Z.Y7.....f.~.{....H..`.$X..m.M.h<.....0).....\.2....,.Ld. .14&.ebZ. ....._.....+y...n..$....`.....c@O..|b.....r..... m.....o.q}...}...?,.M.Go.....0J.*..E....j#}....'..d.....y....Ex.....NV"+G.cs....;...+.V..."....w...W...@..$..rl_..V..m...I"...] [3^..C.'..<...,...C.yH9*...~<..V..U4%A.d...%._,p'a....E.....,"...Z..\...Z.vu.{.7 .r"...).z._....IT...B..b..".T.....~m r>.%I...lXdSg.D.O.C...z..!..G$.P...4.e9}...U..c:a(M.).{...B...$..mA.+= ...XA...<.p...6.F.b...d.?ESL(...J...z..G.R.....z.I.t:.....+TF.>T..)..D5"y....H....r)\...7.....xafF3$.....(.T.....&a1%.....:..B*.H..A.G.H....v.....8.L._}.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO......p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..pn..+1..(...P1.L..s.4..1@.8^2h....2)J...P"0..@.c..g<.!<..)..BW.J.."Xm4..0.....4$..z.C+mL.....*..6.?. <.....4. .Hb(.&8....=..1..* ....A4..(.2.....HT...5.p.....{.E.4.p.....L.....{P....+HBc4..8.3l...y.S`d....7.k.U....B.....^(..h...H.m;..c...@..1@...B.@.Bc....p....4.}(..H..:S@.#..4...!...P!)..T.i..M..M...h..a..1.c..n(.....H ...<?..1.....!...S.`8.1.J.1..0..h.H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\B87Z87FM\AAPFmi4[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	846
Entropy (8bit):	7.686542726414513
Encrypted:	false
SSDEEP:	12:6v/7cM4j39Et8keaWbqx5608BcA5Anj/HwvwFxobkq4vIkOR3+XOq9zo7pZEz:1MAES35OxE0CAHDFxrEkU0tzo7p2z
MD5:	6F93C3616FBC7B9E97E87E718DF27B14
SHA1:	33F4B22E6C3DC6E9A2BDE8BECC3FC20D2F90A1B3
SHA-256:	DFCE8AE7B7C17FE90C55D7EE093936137DD0528FC4CC5BACDB5ED071FD2E312E
SHA-512:	99599A61F4D2FE8F28F32DDD62239E6FF86A68249A59D5B56AFF1F5D76B41FA841C20890C6BD943078CFBFC807CEDB1711499657866B7C259CC20C55D675D73
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...]LSg....=-x....!.....'.H.).$c].xc.7F.,r.eK.x...hf.[.D..}...%.nj..D...H.....@[(.~p.....n..=..o.....G.....V..n>J..p.`,....g1m..ZjK@.VHV..Bst.B.1..z5$M.q..q..0.u*g.5l.P. K..Cq.|....k....]l..p..0..[1.4n.....z..it..H.0.O...B...,!..[.....`.k..d..'..~...7S.X(....&...,.&R..UU...L6s._8....D.=.. 2.7w...9....!....J...<.q....}r...|.#...GB.....u....u.....b9*l.....%lb.....LGQ..G."a....[..B...sYdM.!.A...7vv.J$x..U.H(9..d.....U\8....N...9....N..U\=9....2SmG.....s,&.b.3.....7....,..[.....Eb$.=w...x8M:..*z....b.2..8f#.-".....~-."......E.S.Q.....[(.D.....zB...z.^.H_.]U.9h.....N^..4f0M.....%.An.xin....4.....7..^[...w'./.....:.2nw....L...J.....N5W..5.q.....}..wT.....,.R.N;4W:x..e.U...j. ...)/.dj#.d._.je.x...@."_.@z.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAPwrS4[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	573
Entropy (8bit):	7.438664837450848
Encrypted:	false
SSDEEP:	12:6v/7NzFouDfSmgPEBv2aglxp1ATFlmASPBk3YRRiRHTu9L2p3A5k/1:mpouDft7v9IGpg5k3YRRCxAc
MD5:	BD4DAB976E44AB21C770DE6EBC9F620C
SHA1:	61D80892172A51C39CB605065CD7971D093EFF16
SHA-256:	9EB1FDAB9D3AFBEC190C1BDD7172F14B427BDD0222230302C7C7B7068CF3B39E
SHA-512:	3D24557B9626115E897C191200AEF0F7044FADC33CFC35B30A291A2BA5BF547A33B087E8C14E1BA947B14E48D2D0E3593BF38995140AE2E978845A850A2E9B1B
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...KkSQ...$..l....R.-VJ..Vp.DG...:.s'.....p.D..EPD..VZ...Zl|..M.p.{R..Y69....k..oT-e..aQ..qj...z.j..H"..$..L.O.6..._....&.N.....e.....Z..@.....D...?....D.....@.$lo..+...U.....t...N....;.h6...9!.....J....._.eF.;....1P..]X...K0<.%..7..3...Cp.Oe.....H...k.l.A&..(...&.B@.[`e.]9..ba.....0T.?'..Y....V...@....JG:...rAk..n'".Qp_}.j..hV[WD...?...../kA..I.{....G.....%.....B.....y....O..j~...E.6wH{.T.AC.y.l. ..'.7...i.....D.....'....!p..b...U.?{.....i.c.....&.)....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQUJZl[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):	12798
Entropy (8bit):	7.863453403898195
Encrypted:	false
SSDEEP:	384:NmYG3DiSJUux7ezQMVsIcvA+MEhPSZbHubXDW:NqziSJUqez24NubXq
MD5:	7B1A37F58AF2B4A58EEC1C4B7304442A
SHA1:	C7C30EC849C57FA1304C100B3803112932E38D8F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQUJZI[1].jpg	
SHA-256:	897ED691CE4E116FB441ABD48B7FDF7B8C66583F83BDEA67EB22DE87A05F0DAC
SHA-512:	D3ABA4BBA3D59AE1751A353FD6E63076B2869B59331FDF759BF02C039CE53F056C8128FF2A95E21739DB13CE3A8FC805A97D44520086BFAA9D9EB51FEFC5360 1
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&...&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..2i..4.P..q..b.>..noZ.7.....h.....|.....x...I..@..I..@...?.....S.T..:_.P.y.....p.O.P...?.@..'...|.?.@..'..(.O.P...?.@.%...I!.h.x. Y..j@X6.....@..._... ..g.J.v".U2..... ...LC|...y.z....z....@..'..cP...@..b..@..-.-...P.....-..@.....(.(.....Z.(.h.....-.B.....XT..xH.9<..sE...kMJd&;..{..?Z...y..&E....\..*.....Y..F..a.)6..'V. ...n.c.u..*.&...j.&h.....4..@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQVTID[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):	11634
Entropy (8bit):	7.950478399271463
Encrypted:	false
SSDEEP:	192:QnXAknmy3tImAVaB4KGSiFtapviNhXgb63atNrT14vc7PX2XpnSkUMJjcmX+:0XAknB3tIDk4/7fNhXgbUatNrT1tott+
MD5:	4168D8846819EE038AF7AC491FDB0EF5
SHA1:	2933B9B253C14D9D515D4E7065BCE93243B819FD
SHA-256:	85721294758FCF121AF77C628960BD6379D9F6D9A69B888CA5EEBE12790173CA
SHA-512:	2F85B52188672BB53F92C7B80A8F2E3B2B31D0E6F99A3CB4D5D2C89A5F414CCC697DD6709689E619126902E6D0F7CB7866C8A2B3E6EECA8D3319F438DBBF852 3
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&...&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(...:.. ...e....[.GbD?/.jFt..l..=.....H.$(.....(....1.]..".....\.4...~./.....%.kck.G:...#..T7....$(.....(.....\.....E:.u.U...(.6..Z..n.K....]..\P.9< .....J..y.5v...2...>....*.Q..-LiM...d.f..{.....KX..[.$n... b..<.....,.....CE..n..E.. .S..i.....w.....P...1.P.c]F!@..y.e.....Z.{.....jJ:?.77.....Y!@....P.@.....5?....3...D_..?..XKr...?. 1U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQWZxV[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):	9332
Entropy (8bit):	7.932579128607671
Encrypted:	false
SSDEEP:	192:QoSUS/VsG2/4T+Gw5jNczWdgNMvaMrs83NlX0dXPj/lqRQmbHOBKewFh+Hw:b/SsGEp5j4m+MvNadXPj4QQOBVwWHw
MD5:	60CB00F7EF35C1AEADD22818888645F1
SHA1:	13A904F4B0D5BED20AE499F4345569D47846A0F1
SHA-256:	21BEE73BFD6B2AED248A55D7F02416C7CD2DDDBDCDBE6C9C3CA0C70C71C5617F
SHA-512:	D0A76E45A0AE63CD2DDBF1D2CCD43EDF696EB4D2D86EF852715F0200BCDA15DAC294C575F7179F2E0F39BC98368BF59871865CA6F8BC92528AB530A119579E 3
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&...&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..zV P....|..M.....J.....RO.+`B4jG".DA._..OJ]G..\g..S.....v.LP..q.....+.:....l.JCZ.....+....LA@....P.zP.1..`.$.i.;....r...N..F\.. h.K..t.....V+]...o.V\...K$3."9...d.l2...2.~i..bC.....u.x.....[.q.I...#F..9..{...Cu.....4s._.....O.....*Dz.}.[..#8.4.o...)u.B.....J.Y?..."....FDv.....r..E<m.....h.-}.c.".H!.Yf1.pGRG .\mX.LA@....P.@.mkig.O$y..<T.r.x.N..g..v.2.....k

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQX4Y6[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):	23074
Entropy (8bit):	7.837346451149232
Encrypted:	false
SSDEEP:	384:IEHjid4U8ygMNrpD6L2aLK9ywUplskdIQxFa/tAldbFY0deVtKnSOebrSVjE+grk:IPRgMs0kwUZI1qRd1SOaSVjerQ3
MD5:	7865427A0294FE0705C2FA28AB1558DF
SHA1:	B9C9D90FB04A2D80000F3BC5904B2458E7D24E68
SHA-256:	85876BEF86E6E188383B5ECE1E5EF35313AC6CECA2FB05EEF77EBD5426A24065
SHA-512:	64FDB4A85A199FE1F2278AA09FB26B524D1B44F8D9D9849D9D1572AD716445EE5BDF41F43AE89580B2C440C60F05D6836B6BD10822E54480B2659ADFFAC0FEF A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQX4Y6[1].jpg	
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..:....i.....{...:|.....4r.:..z.....f...I._..?.A{AF.....?.@.....vT...i..8.ij.....8.m....._....3...9Ps...0..H.p....)....I.I.3..UX.b...h..s.U.0.m..62.s....k.?:z.3...t...Z...d...dY.9..XWe....cQ.^.0...j.qi....!.}D!..X..*C.#..'...>.....^.Ii...VR.....I....L../c..Y.,o1..O.@=.N..f....._.....G$C.}.&b...${..].....=(.^}.?.\.n.?J9P....?....M....QT....u.@.7h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQXfYg[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):	11342
Entropy (8bit):	7.947897306615944
Encrypted:	false
SSDEEP:	192:Qo52krOOO0Nhg2+Sxc8St1KfbfmCqosWjhwAb1HpdEiLfmR1PjL7OZQrpRkcd2Vw:b52kq4USxc8St1KfbqWjhwAb3aiL+fjP
MD5:	9BF20F4698EE1CEBCFD7356D5A855FE3
SHA1:	DE5F6CBA1DF6DED80862378E28DEABC14169ED71
SHA-256:	25E964A3DE3B20F4BADC0E0987EB6311508270BB66A33AF9CBD6397B4146D23D
SHA-512:	E0CF4117DCB1AC66791CB4858833FF3FC156DC4BF4F19ACF1DFDB08A89D5AB87BBC9DAF4E4B8F563CCEF41F9056DA4BD355A0875AB49BCDFB020599D3EC4A0E
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....TM..h.....@.....i3..Mj.|.Rf.$..I.>qY.....K..Z.S&)..H.>H...tAh7a.]..8..tz>...T*$....3X...u....Ecw`..gR..3.i..qJ...NR6...1.:.z....N..0@.u#!.EB...O.r:..E.K7..9.PH.z...h.[.\F.!GL..c...W8..,..}.....Q.R..M.v)L3...t.<..#...I.H..Z....-sdF.~X..V..K"m%..h.'.9..eGk.?..Q+..mk..:..qh.E...Q....d.EI.....(G)..9ToA.Hl..'S..@V...H....H%...j.U....*9u..U...]f.#....S(.....}....s.q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQXiHB[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):	17033
Entropy (8bit):	7.94429179620019
Encrypted:	false
SSDEEP:	384:NVO6pyWhfl83GcC7xW+xUKp8NL0y5pFBNJ+DD4CM:NRImaEWcp8NL0y5pFnJIDVM
MD5:	C406E5C8E50D4B7C607A703682F00AEF
SHA1:	79A5E6100B83552679B756D9CC9F30DEFA436D65
SHA-256:	750DC3D45C232DD8E1127B7860F0E38E6C9A6BD3888F05615C18215179E8609C
SHA-512:	0AF8BE812D1A05915C06EE377AD3CEB7C612A699238A3FDB07326FBDDD6E3539E8AC8FA643485383644FB67D1F284B0F52E81DCE75591D14CC5EFE950B798B32
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.....?...&....~Z.@.....Z...@.b..(.sO. PR7`I....J..ZL..&. #..D.....v..Q%0.A.....fe.u.FE.|.`e..`B:..F.!.~..Q...Z.c4.V+.....p;.....:;...3@..W!3.&4.K....[.S_.....ov.W)7!{.4.Er...zv..27.;..|....t....&b.2.@9. $..vh.wP....6t.....F..(....'SH.N.M..%.N.f.%Y0h.O2.....g.....pz..M.z`d.L..P.V].....".h(....MU:....6....+..Y.Y54.8ni.,g.../.@.a\[.I95H..I.z.. ...A.+.&..h...J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQXkUK[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):	8696
Entropy (8bit):	7.913734514082386
Encrypted:	false
SSDEEP:	192:QoifkOmGLnwIJu2Tjve86rNpvz9JpPscwfCSE/0L:bikfGLnwInTjz6hpvz9Jpbsg/0L
MD5:	B046E0D27EB64211DE94642363502123
SHA1:	B9FB4A5A5E05468E65E30F9455C26AB5B793BF73
SHA-256:	1BEAE0DD824FED1E301393FFF3B54E5F0DDCF2DEB80A816E3D8E876DC0501D11
SHA-512:	E3B0FF068E7C903C4D06FDDE07288F4121ACF1A24E59067AB65FCB1C94DF66FE6E5246BDB3098E4EA80B380CFB5ABF38AA6AAF6A0175C94FC3421CA30E4CBBD8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQXkUK[1].jpg	
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..|.+.N].S..p...$.r9'...GSU.+...7....B.....5l\...L..G-.4+.i....a...>..=x.....1.4.*\l.....#.I.W..4.%...&A...'.=.p..NC/.fnP....*.S..&.E.!,.. .Q...a0`....._..H..{...k..l.....\..&.a(>c...k`Hu.P3....q...N.f..Et..i~.....o...z".I...cJ...65..H...UQ.n+J7..L{k.D..S.Ri.f...B../.`7.:P.0M.sM\C._.*...I1.6.....Tg...$ .....t..`p)$.J..T.....P... .#....#-..i.3Z.!...i.RHdR....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAQXnHc[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):	24246
Entropy (8bit):	7.846747278977987
Encrypted:	false
SSDEEP:	384:IbFTdh/uolTu7s3v8qXD/mo101CbF4tGEwS2K7qk6vp7WlDBKCiH5ac1hJ+Xu:IbFhh/uolUs3v8qT+vY4tjgnNx7xJ5ag
MD5:	E45289AF4E26EA5530602CCD3B136153
SHA1:	982BA72AC20A1A4F5EC26DCB92CA4FF954F2B588
SHA-256:	A0BF83A579CCC7E3BD07DE74FCAFBC84AC6CF0C36B4DDE5B3589F899464A56C0
SHA-512:	6193EC145EA9A057C9D399127B780483667FEA59CA0C0C611B3DC4BF1D99595FF4BE472306289364C086A3EAE16D01D7429712B548318E6252F1C703A04964BD
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..2 =r+..Y..N..3h...Z....!A....3..5.P.Lh...m.....W.8`jX.cq,...w..9...#.`.....`E.4lO,(..t..)G.i.a.HdOB.sZ..q.J.&I.A.Z.6X.Pm.5B3..;... ...R=.$Z7t^5.F..k...bvZ..}Dk.H.....fQ..,`....C....S.].3b.D0..b$...P0.....X.....*E)..t....i.=J..@.'..`....$.# ...ZC.c.*.HC...y_4n.....<.E...+...|..#. ...P..wE..).a..].be....k..Y.CA..N1@.. ..f...9....P.....h..h..?.0..d...PWw.(%..<zU"J...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dTzfp[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):	8890
Entropy (8bit):	7.923808661823827
Encrypted:	false
SSDEEP:	192:QnI3wmoo/Jq+krgOtxrcnVskmB7lxED4u+I9ocY5zwX9B:0I33oo/JqqOxrcnVskQK+lpY9B
MD5:	29792D182BA22B3E036424650829BEFE
SHA1:	BB13279B92AD154589A1569CA7AF19474B2FD832
SHA-256:	E6CEE354D756A03B5404D34D7F7433CA55B5D32AC5199A0A508AD3A379AABE06
SHA-512:	F137B17A8DD6783E5906BB8000A54B5FC5769DF5878369A48B5190CFA71392FA0352A4E92EC8F91D2A28BD9C5E977A101CDF0B52FD194ADEA5AB0FA0225CEAI A
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....A..M..P.....T.....@>..yR....G.(..\.jC0.<-cqp.`.1.h.)2.....W....fT...1...Q`.!o..I...ar..{.(1..#.)./|.|.?Jar...(~h$..0.#6./.F.Q T.O..JW.#nH.H.'.`zR..c `.C..#.h..`.....h....U.B.....&2h..}.#..=.",.n..x.(...\.j.^L.<...2...z.Y3U{..zK...1:.).G.W.O+....(.....o....km.R...^2H;..KK...<G....N.h.c.....yY.w.sM.~..y...`....Yh. .\..9....E'$..)..<.....J.(....z*.7K.M..dX.k

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\BB7gRE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB7gRE[1].png	
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	501
Entropy (8bit):	7.3374462687222906
Encrypted:	false
SSDEEP:	12:6v/71zYhg8gNX8GA3PhV8xJy4eOsEfOZbLjz:u8O9A/hSJ9lfkbb
MD5:	1FCA95AEED29D3219D0A53A78A041312
SHA1:	5A4661CCF1E9F6581F71FC429E599D81B8895297
SHA-256:	4B0F37A05AB882DA679792D483B105FDD820639C390FC7636676424ECFD418B9
SHA-512:	7E02CEB4A6F91B2D718712E37255F54DA180FA83008E0CE37080DADFE8B4D0D50BC0EA8657B87003D9BAD10FA5581DBB8C1C64D267B6C435DA48CBED3366CEA
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..RKN.A.}... ...e1(."le.....F\...@.."...|... ..ld.$.(.`..V.0].ghK....]SS...J.I.<@.O.{.....:WB8~....}Hr...P.....`l.N...N.....Z...'.3..;....3.B-....i...L.....b..{... ..Q.... .....L...=.d....n.....&.!..O....W1..."....gm5x....[.C.9^Q.BC.....O...../.(...|.~.0hv..S..7.....YBn..B..o.T<.....|.g&....U.....gm.. .....U..,u..)\$.lN .w]Rm.....OZ.h.....zn.~...A.uy.....,.....3(.....z<....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBkwUr[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):	436
Entropy (8bit):	7.255906495097201
Encrypted:	false
SSDEEP:	6:6v/lhPahm/BBjoPHhOVDqpp05cMxyHtGUmmozY7JE3R+hRMCzRPasXQc01UaVesl:6v/7MHQg25b8Ht3VEMNQ2w5
MD5:	01B5E74F991A886215461BF0057008C7
SHA1:	6A7347C3559814722D7AA4D491A0D754E157FCC5
SHA-256:	DB8A0C0A44AEE824F689A942D99802F95D7950758CB0739C7F179624A592CD51
SHA-512:	17820A7C90B35B0E45D0A07F5445D8C97BFD3098FD9E0F0283CD6CFC1DB2B33C651924D2F04EF398C147CEB8D7DEA3F591DBC19F9039279407C4E4231AC5F57
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....fIDATx.}..M.@.....0...Aa.....#0..."..0....a....<....<....y..qS.....m..k..%.'|.....`....Z.`x...X.....Np..x.....a%(..ab.....=.....j.[...0}.>.O..R~..<@y....nV..:.q.....G.P.e.....?s....i^l.P..5.0....?...&.A.K..|+...X.h)....5K...Zx...[....G...0N<.~PC.@.X.O2..N..x...:?..7.xH.&.....C3..8....Q.*.>...W..~..].U..U>L/....Le&.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\a5ea21[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
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\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cfdbd9[1].png	
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\medianet[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	411779
Entropy (8bit):	5.487169936172669
Encrypted:	false
SSDEEP:	6144:z79kYqP1vG2jnmuynGJ8nKM03VCuPb5XEcJuzYmD:U1vFjKnGJ8KMGxTqYmD
MD5:	CF107E83E7350D805C5A289CF231703E
SHA1:	CE1B53F1280E398305B5B75065CC634DC72A7A8F
SHA-256:	79B0961BBC8CE873BC815645C3C3EF9DA507424767014BFBECDBB204B851DF07
SHA-512:	8AB0C5059067EF942AB8E80EF7D4F15DFE7EF0413A263DD0C193EE0B3BDEAFD0E075635700CB97BD2BDA32ABC96CDB9B77B324BCA8E5C0C5AC7C52822FBA6C51
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\B87Z87FM\medianet[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	411779
Entropy (8bit):	5.487208925807921
Encrypted:	false
SSDEEP:	6144:z79kYqP1vG2jnmuynGJ8nKM03VCuPbLXEcJuzYmD:U1vFjKnGJ8KMGxTkYmD
MD5:	260C4F56FAB255DBCE6B51B3F68AF2EA
SHA1:	9A7EBBDF028BBBCAFC268B06AF8EB28A38A80379
SHA-256:	5DDEED332916A6E6F0CC991F9A852AFB91E60D33E69F3697CDD0B347FCC3B31E
SHA-512:	C2675159FD1D209D45038386021640B6AACCB17D9ACAA945EBDA15393019501DD00D9F137B57D4AAC02F661937D249A7EF8A2518DE048E84C2F029020EF2F1E
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\B87Z87FM\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:inherit;font-weight:bold;text-decoration:none;margin-left:5px}#onetrust-banner-sdk .onetrust-vendors-list-handler:hover{color:#1f96db}#onetrust-banner-sdk:focus{outline:2px solid #000;outline-offset:-2px}#onetrust-banner-sdk a:focus{outline:2px solid #000}#onetrust-banner-sdk #onetrust-accept-btn-handler,#onetrust-banner-sdk #onetrust-reject-all-handler,#onetrust-banner-sdk #onetrust-pc-btn-handler{outline-offset:1px}#onetrust-banner-sdk .ot-close-icon,#onetrust-pc-sdk .ot-close-icon,#ot-sync-ntfy .ot-close-icon{background-image:url("

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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+cG9saWN5PC9hPjwvcD48ZGl2IGNsYXNzPSJvdC1kcGQtY29udGFpbmVyIj48aDMgY2xhc3M9Im90LWRwZC10aXRsZSI+PHAgY2xhc3M9Im90LWRwZC1kZXNjIj5kZXNjcmlwdGlvb jwvcD48L2Rpdj48L2Rpdj48L2Rpdj48L2Rpdj48ZGl2IGlkPSJvbmV0cnVzdC1idXR0b24tZ3JvdXAtcGFyZW50IiBjbGFzcz0ib3Qtc2RrLXRocmVlIG90LXNkay1jb2x 1bW5zIj48ZGl2IGlkPSJvbmV0cnVzdC1idXR0b24tZ3JvdXAiPjxidXR0b24
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImFsZXJ0ZGlhbG9nIj48IS0tIENsb3NlIEJ1dHRvbiAtLT48ZGl2IGNsYXNzPSJvdC1wYy1oZWFkZXIiPjwhLS0gTG9nbyB UYWcgLS0+PGRpdiBjbGFzcz0ib3QtcGMtbG9nbyIgcm9sZT0iaW1nIiBhcmlhLWxhYmVsPSJDb21wYW55IExvZ28iPjwvZGl2PjxidXR0b24gaWQ9ImNsb3NlLXBjLW9b i1oYW5kbGVyIiBjbGFzcz0ib3QtY2xvc2UtaWNvbiIgYXJpYS1sYWJlbD0iQ2xvc2UiPjwvYnV0dG9uPjwvZGl2PjwhLS0gQ2xvc2UgQnV0dG9uIC0tPjxkaXYgaWQ9Im9 0LXBjLWNvbnRlbnQiIGNsYXNzPSJvdC1wYy1zY3JvbGxiYXIiPjxoMiBpZD0ib3QtcGMtdGl0bGUiPllvdXIgUHJpdmFjeTwvaDI+PGRpdiBpZD0ib3QtcGMtZGVzYyI+P C9kaXY+PGJ1dHRvbiBpZD0iYWNjZXB0LXJlY29tbWVuZGVkLWJ0bi1oYW5kbGVyIj5BbGxvdyBhbGw8L2J1dHRvbj48ZGl2IGlkPSJvdC1wYy1jYXQtZ3JwIj48aDMgaWQ9Im90LWNhdGVnb3J5LXRpdGxlIj5NYW5hZ2UgQ29va2llIFByZWZlcmVuY2VzPC9oMz48ZGl2IGNsYXNzPSJvdC1wbGktaGRyIj48c3BhbiBjb GFzcz0ib3QtbGktdGl0bGUiPkNvbnNlbnQ8L3NwYW4+IDxzcGFuIGNsYXNzPSJvdC1saS1
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQBdIv[1].jpg	
Encrypted:	false
SSDEEP:	384:IY3asYjHnqTeXCnV+vWN8ZiadjNBzJNCGNFq/NFfqoY7mZdd+f0naWx:IdHnmeyI+yi6NB25/NFfbFJnP
MD5:	F4B452436A19591E7C0ED1A7916B9259
SHA1:	5BA326F2E57A89A106689E4EC00B23D30AAA9DBE
SHA-256:	B13869EEC4400F3BDE2DE2F864E786ACC568D413FDA7FC619FC4AF87E6328B5D
SHA-512:	313B26FD6A8C652B5AA50EA698B070D324C7A0B8A202BEF0A1A87EB3ECB633BD0DD9CBD574598F107A4374FCA6FA2ADAB1DC028EC5446EBDD402B044D325F90C
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..:.(.....(.....(.....(.....(.....(.....(.....(.....b..P...1@.(.(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....P.P...(.(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....Z.(.....b...J.(.h.....P...P.....A@....h..#."....1@...(.....(.....(.

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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\AAQTNpF[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):	19533
Entropy (8bit):	7.957635016532373
Encrypted:	false
SSDEEP:	384:+se+XaO+HFe+APb8Ekg/5TT3Z7+hRmQ73stDgU/XfR9wkaTlZcNmM58:+F+9+APb2+5TNQ7ct5/Tw7lZcNmM58
MD5:	D61E35515C7D557038A8665509304921
SHA1:	5613E3B44907BAF1A7E07A94EFE8E43953B8FA86
SHA-256:	7BB82EC8C12377DC2485B83B0BD2A71B6CD511593456AE4CE360D60EC507C027
SHA-512:	0CA6A919C6AF1D4B4B822A0C24AE81423E0CF65C22FD16AE1E9C6769C5C46C1C62348A1DAB89C05F9E08DF15F80AA4B2678BC9F854C864631E5AE48949453FA
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...#H..r3.;.'?O.j!.Q.b.....[<.q...}:....[....G...O....#.{.]Ll.k".....\....k<...?.O\.....o#O6.w<....^?AP6W.....+.L.....A-.i.....s.T..l,;.."^..P".E.3$....S...&...$.....l..e.q.9...:/}.i.).3A..<.m.w.....~C.&7._...&Th.cl....c.....tH.Q\rF[.Z.Iq.n.mT.p<...w.y4...bm..3s..X..Q....r....pW..?.a+..Z...#..w..gl.=.kN]....4..Ag../C.S./.1...C.....I.....0.0...<...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQVPm6[1].jpg	
SHA-512:	1BD59BED9431C26C14AA4545A6B459680BBDD855E20CE1FE2A5BD4B861DAA793CA9FA6EAF96F353099440E80DD2046E54577DD0B329C45B8EA5FE13CB08B67D0
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.....?....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\NUEPGTR9\AAQWUGg[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):	18255
Entropy (8bit):	7.962015651735258
Encrypted:	false
SSDEEP:	384:Nz4xw4e6tJpm5mi+3bypKLOLlvnRxFdQ1a0JBzU2:NMjV45PCy9lvRZQ15Bp
MD5:	4A81A5224693344F8A3ED08E527D13DD
SHA1:	A238470F528B17C72837CC56D6C27E11B9BCDD94
SHA-256:	59FF579660EE9F0DC93BA5DEFA14CA890E02BC49CFBBB3DCD9C24F15209D8FC0
SHA-512:	4AFD90BE51CBDA5D400CD713C2DCDD714F34E1B62BF27657FBE81E543C3563ED499DD279FD1552F07A8507A04866C8B2EEE1BDA063995A26A213C75636844F8
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..1D.c..X...b=....q.d..\.4X.W...G..-.$.Ji'..}...h..F..j. ...%....Ii...W.#.j.....G.i...^...s.....~..;.... W+...k.....n8.=.....Gt.....=.35..I3..S[.?..8...c....Q..:.....?..f...?R1.....Q*.E"AH..!.@h.....H:P...1...Hc...@(..#.....@.).%..1...L.....?.eG.u...W.e.v.x.w7.....z.X..q.z..G,.WS)-...>}.DO..t.?..V.-F...W.GL.5.?.P1...&...U.....h.I..Ha..&....D..:...S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQXdUx[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):	7039
Entropy (8bit):	7.862175001949922
Encrypted:	false
SSDEEP:	192:QoXHtL+y0q0rIhnrTImqBUfdeXYkN3517BIihbv:bX0y0Hrcn3ImbqYy3517BIi9
MD5:	DC4833176AD98C9F455000BA323C8164
SHA1:	E96798AFBD6E81E377DD05A16487ACC3B47EDB77
SHA-256:	6E5082087DAEF009086494CC78025B5FAF70932876670368B82DA6C057702138
SHA-512:	89E57A0FB5F0C8DAEB7CB560164B0DDE439D1A55ABADBF46933AAD541CE092CFED1006AE7DDA0D5EC5E1CCA071273842AEEC1BD03EDED91AAAA36703BB29EABD
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..6.r.".5.:7.0h.~d.."..... .....`>G.M...I#....].a^Iz..M.....P!.d.p>U.%.uD.4.....ns...(...X....d...jC...\P...\P.@.(.....P.b..R....1..U.<.9v.!.qn.n8&.W.._B.....6>...rU..A..'.R.....@.S....@.}...1...v....I.a..n.{6@.$....w..1.E...Q@..d1...H..T...C...b..P...P...LP0....J.....q..U.<.9....Z.....w.3.....(...o.x*..w...+...?*g.}M].Cf.....5..(...../x..t.C)....#0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQXfSR[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):	2975
Entropy (8bit):	7.846293289939557
Encrypted:	false
SSDEEP:	48:QfAuETA+TFZm0vNoFScHHcYXyVpQQO/x5EBCvPJpxfew3QlCtu3b93iC0GI0GJz:Qf7E5FZm0+zHcJ6Dr/PZfeytuI0GJz
MD5:	30761D078158E7FD375C861443C708F3
SHA1:	8B4AD8475EBDE11B020FD2A833C6F7BE2D67F4AA
SHA-256:	7A818CC492B99DA8F9E1DBC054EFA96F1EFA04D53DF09F26EAECDA7FFAE5F130
SHA-512:	49D30255D57E6AEFD9725A4AD675951B93696EB9D401DDB16ED237951149EDC363D77D5DF5D974365BFAB167A1BDC5458EEF25B37A4BBCBB52934DE55E8CD38
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQXfSR[1].jpg	
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..y.h8<..E.4~...g_..5+tc.6g.#...\.|....>il-w$...X.US. ...n...,H..0....."U...r.z.y...Ur9Lo.#..r.`.2,...e.2i1.....H...1..&B...5+..<.V.C.<.....S.6..l..r..Q.tUX.. .2....s.l...C.oa.....7.O.5/a.]....I.:...zr..)..]Fm..@...PN....88'.C.5.....!..i.....W0<X..k...;~bG.r.H.{.?.&....F.=.\.E.:....p.qI...r...b....0.F~s...IZ.;..6..K.?.F?.K.4..y#)..T...V..6.(v.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQXi93[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):	9964
Entropy (8bit):	7.9450142588571175
Encrypted:	false
SSDEEP:	192:QoHmdBrFRl2fQ9TNQT0t66OnVXWJTbvbt7u9kqtj/Uqd+:bHmd9FRlMQhNQQtg2Ekqtld+
MD5:	79BA33C5F507F380A0CC346486310DB4
SHA1:	59C4262BA33D880CA585E21B741F3CF6AA9B70D8
SHA-256:	B035C393E27BF0D748A55CCCF90F9FA479068778FE744D4D24E81ACA1A1A19ED
SHA-512:	01B927B27860B1B22E755851860BD527D7BDB9F43F753AC71BA9C18A459D10ACE45452C31A76CA2A6BF5C6AD4153A361D0960A19C5947175393C276A8E9EDFD
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.....?..._+.N.j%.....C.s@.2.....*..cV.Ms.V6....m.9..Y6...[....#...Vr:.....r..G5B`8.0 .u..oL.b...y.X.6.|R..sZ..|..9...`f.j...-...).Hd.-Lw.(N...G-VV~Et.,..5.GTK...*lhV.N.d.H9.F3,.....b-.i6J.!R..qE...I.k..n.zf...b`.r.F.E..V...Eip[..d.,.i.....m.....I.`..7`...*..G.w....&.....|..g..O1.#*O.mV.LF.....R.....f.].en.^/..5|...R...g8.)KSH&.....H...1LR.D.85.6]..+.:...p9.9D.Ey..P.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!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\NUEPGTR9\AAQXICQ[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):	16517
Entropy (8bit):	7.957170522681704
Encrypted:	false
SSDEEP:	384:+jUWRBBZwZSAJ1xYvFfc8UfVqJzxdMf2GVFOWpYs:+HBIZIvyffVqZg2a
MD5:	4C86E76D5B3D7AE230557D78CD9DD92D
SHA1:	DBD89515A3C0FDBC09072423FE11E6FD7D2BB990
SHA-256:	ED75246170D091F80398921F19EA76600BC9EF8E74C54F140CD39888BCCAC42A
SHA-512:	A04F17D2ABE02890A1431868D65525A628619B2EEFF046CAD65EDA5222F1C98C27049122495A891C49F126D61C31CA52A455C692C083EC676F8D062083570B28
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..yd..%+..3.q.jw.^#...Xm.6.(..E..'-8..3.MBv1G#..`U}>.kc9y.....RpF*...n.nm.<....z...5.....{yp-.....Bzj)j..X..y.l..v...l.4...l....i...n....].Y..q.N..k...\...F..$....i#&.2Z.Y...ARO..\u.\._b..L./.....N6...,.c..(..d4....,.X.';...R.ts]..<.....S..%..RV....q].{.:.[.....C.....r...w-....lR.!.r..Y..%.k0....d..t4s...k.....#....Ji..i.Z....LQ.T...(Hm.....Z.m ..4..hp.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAQXpWY[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):	10993
Entropy (8bit):	7.768964926797329
Encrypted:	false
SSDEEP:	192:Q2un6W/1VOOxpBa9//8L7Wq7mqc6su6oTNIBsSJ2Ou8bRKWIzVGlua/4RFmGo5k0:Nu6y1VOOvBa9//q7WfVPfJ2Ou0KW4VqJ
MD5:	0AB9DEE3575FB357533FD36C8E24642C
SHA1:	CEBDF8E3B885EFE9936968F1ABA68E3A171AE810
SHA-256:	2A9459A553FEA91BEC5DACDB6D178FA7E8B68AA94CD318568EC8FA2F068FD33B
SHA-512:	2B43261C4884B6076D3480FDA8899E326493D1ABAA69D81B4E66456E5402E73A62445540F5022AC61202C7BED225FB1B1DF069616D9F1350417EFCF758DABBD0
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.....?..+RE.....(.E...P.@.....(.P.P.@..@...`%.%!..%.%...P.P.HbP.@.LbR.....% ../U.(.h.S.....).).(.....J.(...4.(.P0.B..%.....@!....La@.@.@.@.!.H.....P...Z.(.....(.....P.@..!..4.....!....q.O1?.E.a.l..<.....Gwo).J..f.....)...C@..@.1.@.R ...A@.@.(.....Z.J.(.....(.....J.J.F.y. 2.E.....K.I..\l3.#g>....F....J.R...Ph...__..%..9.E.bX...~T.r.5Rb..k.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAzjSw3[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):	587
Entropy (8bit):	7.531438372526454
Encrypted:	false
SSDEEP:	12:6v/7r+k5j60/BRFEAYagzKQkIr76mpc0hneR2bHVkKPVXwZzv8gXAtz:GNO050agzTkVmpc0xguPViO
MD5:	2DF6E53A33E3D7D2E401F9FD0B723221
SHA1:	C2E3B5A6FF363BBD31CC6E39CEEC10B67BBBB9E9
SHA-256:	3484DE1DF304502392D694F16B843B7E1FF5C3F2FF88C6BCB30B195F34F8AEF3
SHA-512:	70A4CBD0A3BB14584F9D528CE87F69DE5CC10366BDEDB3B568E63411280C7D7B4900EC8101AC87774C9DACCBB9F1A8D989483A5CDFBD382FE814F1F181601E 1C
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...Kh.Q...lf..(*.....M.....PQ....QA..nD.."n.....4.`K...&.M.D..X...jH.4Nc..:0.{.....suv...G_.VI.3.w*k.cd.v....J.i..t.R.zd_..@..C.....$..J...5+...U/S.....k..:....1...!%..g.T...<plv...)Y....;..uq..(..b..X_...]=..K.[...\[.....r...`G.u.....{..n..._.....u..E.~..!f%.'..>..2ZZ...u.....>....8.w...t.Fi.W....l.~%h....h/.{.K#91 EGx.SGjUq...<.....0...c....P.h.....^G...%..S]..P...c.j..r..{.0x"#k.q..45.....r..E...k...)..y?|.-y..}.D`..`J?.u.}...sH....E.\2r.s~b!@a."........E...Hv.....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:	EBBF357EF6B388E4BD1B261D51DE923D15DBF3AC4740874BEBDEF336BB8133C3B63AEA9D8D95D2D1A044F6E43B7DD654586661462C9239E4FFA6B8328E6B49 A6
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. ....l.o...s....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1ftEY0[1].png	
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\NUEPGTR9\BBVuddh[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	316
Entropy (8bit):	6.917866057386609
Encrypted:	false
SSDEEP:	6:6v/lhPahmxj1eqc1Q1rHZl8lsCkp3yBPn3OhM8TD+8lzjpxVYSmO23KuZDp:6v/7j1Q1Q1ZI8lsfp36+hBTD+8pjpxy/
MD5:	636BACD8AA35BA805314755511D4CE04
SHA1:	9BB424A02481910CE3EE30ABDA54304D90D51CA9
SHA-256:	157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3
SHA-512:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C1 3
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....P..?E....U..E..|.....|...M.XD.`4YD...{.\6....s..0.;....?..&.../. .....$.\|Y....UU)gj...]..;x..(.."..$l.(.\.E.....4....y.....c...m. m.P...Fc...e.0.TUE....V.5..8..4..i.8.}.C0M.Y..w^G..t.e.l..0.h.6.|.Q...Q..i~.|...._...'..Q..."".....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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\NUEPGTR9\BBZbaoj[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):	351
Entropy (8bit):	6.901959384450008
Encrypted:	false
SSDEEP:	6:6v/lhPahmlVPGiBERRpXw0kdFA2ykO2tWNNClAukllbp:6v/7fB0RpXw0otykOhNN4kll1
MD5:	34B5D386B790631BCF4E193D22CCD4A7
SHA1:	E65C95C426A4430A96782CE1B9156C2DDDF8807F
SHA-256:	6FA5E53DF07126D22CF60FA1DBCF537FE1F82F26520738317CB0086CA923AD44
SHA-512:	D0FBCC60FCABCCF01B13735903BEE75C4843688C8208D9B7D51D47AA7B6DC6B00ACDAB83116238F8D5FC9405B96B5DFA7BD66390F8A1D8E4491BAB81D18D1 F0
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.cy."....B.^.V....[30.....G.....8...4....P..x.....U.9..`...6~.^...g630...1L.F.4...O..w....r....A.@.`..+.....0}p...@....+.1...0..t.E. ../....S.a... y..@.?/.c@.6.K.....`..,!. P:..._l.n...0...|..n.`.....`..r:.0...r.!.a..W..7.30r.....G.1.2........i.$..`5..B\b.#zL..r.8....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\checksync[3].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\NUEPGTR9\de-ch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	79097
Entropy (8bit):	5.337866393801766
Encrypted:	false
SSDEEP:	768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B
MD5:	408DDD452219F77E388108945DE7D0FE
SHA1:	C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7
SHA-256:	197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385
SHA-512:	17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB1B
Malicious:	false
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\NUEPGTR9\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
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\NUEPGTR9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otSDKStub[1].js	
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","L I","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMi gratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknow n",o[o.BannerCloseButton=1]="BannerCloseButton",o[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otTCF-ie[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	103536
Entropy (8bit):	5.315961772640951
Encrypted:	false
SSDEEP:	768:nq79kuJrnt6JjU7cVbkhS/G+FBlTjmSmjCRp0QRaPXJHJVhXKNTUCL29kJlXYoXY:49jht4bbkAOCRpl6TVgTUCLBX10UU/px
MD5:	6E60674C04FFF923CE6E30A0CD4B1A04
SHA1:	D77ED2B9FA6DD82C7A5F740777CC38858D9CBDDD
SHA-256:	48221F1DE0F509D6C365D9F4BA1D7DB8619E01C6BC4AC8462536836E582CDC66
SHA-512:	62F5068BDEDBA361DAD0B50B66F617A2A964B9D3DB748BF9DE29C4F6307B1891AF9A4D384F3CEB25C77B62D245F338D967084301391A41BAB9772E2632B36B9
Malicious:	false
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\tag[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
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\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\2d-0e97d4-185735b[1].css	
Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expected semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weight: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:	22994B9288054B22B49A9D439F5DF7A4DBA4507DCA56F20BF222113AA60544E374DEF9FCBCB214DF0684DA68A3550898CCB5B47EAA57C20FCC52BDC735653E4
Malicious:	false
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("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 null";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="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\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:	EC89E47D9C49DB7B5E8E5388A29C5F1C5424C0293DC972D9878A332C58A0174F083BACAC07574A761844E5CD6A2E33BF4648B92DB7494129DDA4CC11FEBDAC8
Malicious:	false
Preview:	......JFIF.....\`.\`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP\`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO...}........!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\AAQWMEO[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):	5361
Entropy (8bit):	7.631706376909551
Encrypted:	false
SSDEEP:	96:QfPE9XBPmRNRKv4F/4EhHID3SKzDJwxsmkXmfPy9GIbH:QngXBurRKvi4Ex8ZXmC9Jj
MD5:	D2AB80E95424DB27C031732565C4C485
SHA1:	DBC3CF5514FC9896B0E91FC536C025EA303B27C2
SHA-256:	533E7D8170EDE67A61DA30BC7887989F9E569D02ED85878BFE21BF1F2498B8FD
SHA-512:	4686F34493CD65021D690A56E478BD472D73AB648AC56FDCE85280A6CE38FD4384F4AF20E0962C17C74450036E06EE98D55A27268A1238573E3B86BB59B18ABF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQWMEO[1].jpg	
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..Z.^.....zP.@.4.P.@.....@.....P..@.h.....h.'..L.....2.$A....@!....L..@.8..4....@.v.....''..x..4..d.....LP...(...f..@.@.=h...@....h.1.@...Q@..@...@.&.....h..h.O...s@.....:P.w..`b....Q@...P...(.../J.(.....P.@..4.....L....f....-...R.....t.g.....G.....6.fz.bsL...z;._.G.....N..:\..*.P...:@a.>...K..G...s.V.6....H.....b.....(.'&.....h....M.8...h...4..h.E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQWZ1M[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):	7739
Entropy (8bit):	7.8917224240630945
Encrypted:	false
SSDEEP:	192:QnzE08Kde5QNFNYNcJpmW+s8H3hukp9PjbLSJ/Ke+LAd4:0QtKo5EFN2H5s8R7D2n+ky
MD5:	1A479FFC8FFF606EEFF33B77B5AD4FE2
SHA1:	936A50CE46BDB97401EC42CE5A1A0C55C4217E7D
SHA-256:	2B040973AA9764F4FF32A1CF464718B90ED88C17E4922D2BBF8B52B3B8B4B1C5
SHA-512:	7F9006686901173A526264BDED166E53A6612313F136E517D19F40D0E961E392E085499CAD0344E9B7CE052C1FF8A4C3048ECD5842C8A8936626DC94A304FEE6
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...nX....._.V.".4.....j.I:(c..n.e.Y.,.....{.5#....^...{.....L.....&(....c...&..UB.....G'.?LR..irp.I..=.....&&:.Uh..P....E.X.t.../.*n.....}.WC%.....]....z.t.cY.....Z.....V....d.....X]..e?....a.h.....y...rO..h.@4....s.....Fx..~c.i...!..,.QK...t.....Z.t...c.x.....G8Xi.=._.....,E...ZM...q...p...W.U2.....s..}.o.....X>.7....4s...LzI.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQWjrc[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):	11022
Entropy (8bit):	7.929252269200777
Encrypted:	false
SSDEEP:	192:Qo/Xc/PrcIzJo/VAAeoUUHMLRJIL0IKq8u8zrNhBi0kd56MJ0HEmcKnpSl:b0HrLzJ8V9xUUHMNLUE3ev0FcKp0
MD5:	A8F1522207E7A4B6B1BE14CA553BA958
SHA1:	D74B26A2AB2DCD6376A53E442C98C6A10B9F9367
SHA-256:	122785C75649FFBE9F7A89562EAA5C2E03DF71876CEE274697D2645595B21003
SHA-512:	7C957D99A7725F874B9AD2F01380D9111C868B46E850B8588BA5A3BB7A057FF22F71D0B3C50708DA4C63978223A0CA18FAF9D47D84CF95C075998E5B99AAA2C
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....F.7...H.....id...z.J.a.W..[.wU.jz%.2.O[i..G3O)...=.....\P.@.M.....4.1.....+...H.....4.z.}.0..}..D.)\.F{Q.....d....V.....u;UC.....*...2&.5.....3...D.DR}Y..k.!,J."..t..Y.;.7E.K.....A..9...2....\.;J...q.....EC(b.).Z@!.....w(Cw=.....0...Q$.'U..e.....(IQ.y.....j.%....O.....P.h.i".....h...Q.b.....D.....@.2.q...nF.R;...3.....>....s@.].....(.s.=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQX9oS[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):	20704
Entropy (8bit):	7.824227947010682
Encrypted:	false
SSDEEP:	384:IcNUwfHORaOwUjJDXoEyvXpAgg1tZMfXXc2UpF44fAzkJC2w0sRl9UQuU/:I6HGaOwlE6XV6tZMfc2aAn59LT
MD5:	33933640C045C8E307527A705B5D2F29
SHA1:	9AF39C6CEE50571E737CA3667727C77D98846E8E
SHA-256:	38DBAA7E434412E3AFEEFBC05B70CFE6F873D568DCA59BAF8714B0D0FADC0A06
SHA-512:	8351DAE3BD697AEDDEC0E52858CCDE313B9013530BA80B4AB23D6CCD8B4F766685101F6956189EC5281A6116AF40D9B5B6C0CD2AB00223C4D36D950E52EBF31
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.....?...[..3.l..?....f.....a...M.bT9.D.Jb..P...&..p..v%...@...*nU.3zQp.d.N.9A.B0..1v.`..@....OZ@J.h.H.).DX.M...CC#.j@P.94$2D.*,...U.]H..M.....5!.....1@..p)..q@..q..Q.....&.4..ER.P>Z.....R.I....E ....@.....h.#.MK.5S..$;.b..'SR.L.eM.p.E...SAq.R.\6R.\UN1.v...qN.q.)X.J...&+..b...;..I..@.v..\]..V...dT.w.....c.1..V...N..qL..>sR....h.\P....b....I@y.C.....zt.@<..Cb..9..qL.c.T.d.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAQXaYx[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):	10712
Entropy (8bit):	7.721470271044596
Encrypted:	false
SSDEEP:	192:Q2uWqZ80U96yf7WFlPe+KxfZdp8xtVVX6ZC4+0H1RVh4xGlrpuivaQp2M:Nhj0uDs4fWVAIL0/DKGlOQ4M
MD5:	B3A7E0CF05B54D9D0A57316B06B4B275
SHA1:	A42D27642EF8AA6443F54C23B45528784058FA4D
SHA-256:	1EB659DFC3117684152CA6DD5932207F9ECE079B88AB77D3024BE2C890C10E1E
SHA-512:	F29692943A88E7F118426469EBAE1821E8C19F246ECD429C9665D6909216A7F28162E8F9EF593B7F7DC79BAAECA48E3E1540F608349AC34A0FF36B4258836166
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..i.P.@....L....@.h.(.....4.(..E.X..P.@.....@.@..!.....}(.....@.@..%...P.@.@..%.MH.....@.L.<P.@.@. ...@.L....X..P.@.i.R.....1@..%.1....z..@...p}{..}.%.&(.1@..%...P.@.@..%.K@. .....P.H.....L....U..&....(...(.....P.P.@a.2(.?.>.2....a.s@.@.@.@.@.....P.@..>.....S.(...4...R..0..@.O.(.Z.(.E.(..@.i.R.....b.....A.....7...(.M.%.....@..%0...3@..'z...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.7122174073593905
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:	619b721d39f71.dll
File size:	134656
MD5:	5adbb59a4def2a9bfd37e3e0aebbed1d
SHA1:	5a64fc794c133a525ea70e06ce335a7b238db2f4
SHA256:	e5ddae0f09c15a7eaebe71a0ccfcb83ccdd629760b612fffaab46d9a4260e662
SHA512:	623a3c92b47e4448fe8042e3bbb2956fd795553d84cb6a45c883814fb04717481df8b5fed3b693186b56fb742ee87b82840b6c88d5cb1215975e52dd6b26569d
SSDEEP:	3072:LvOaXNXxXqpTzj3Ec0dFP37Gw4nsGyTbP0/8WukDtY:znQzq7esGyXPJMDtY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100020d1
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:	0x619A5AC7 [Sun Nov 21 14:42:15 2021 UTC]

General

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	0xacb8	0xae00	False	0.609846443966	data	6.59578540229	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc000	0x140d2	0x14200	False	0.651021447981	data	6.20313332211	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x21000	0x13a8	0xa00	False	0.137109375	data	1.83776567302	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	0xda8	0xe00	False	0.771484375	data	6.43638670581	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 11:37:25.544626951 CET	192.168.2.5	8.8.8.8	0xe72a	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:40.702986002 CET	192.168.2.5	8.8.8.8	0xe958	Standard query (0)	web.vortex.data.msn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 11:37:41.865154982 CET	192.168.2.5	8.8.8.8	0x511d	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:49.962747097 CET	192.168.2.5	8.8.8.8	0x5c38	Standard query (0)	assets.msn.com	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:57.183243990 CET	192.168.2.5	8.8.8.8	0xc934	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:01.374361038 CET	192.168.2.5	8.8.8.8	0x751e	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:02.264033079 CET	192.168.2.5	8.8.8.8	0xe937	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:03.909246922 CET	192.168.2.5	8.8.8.8	0x7f5c	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 11:37:25.563970089 CET	8.8.8.8	192.168.2.5	0xe72a	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2021 11:37:40.738867044 CET	8.8.8.8	192.168.2.5	0xe958	No error (0)	web.vortex .data.msn.com	web.vortex.data.microsoft .com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2021 11:37:41.884275913 CET	8.8.8.8	192.168.2.5	0x511d	No error (0)	contextual .media.net		2.18.160.23	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:49.984325886 CET	8.8.8.8	192.168.2.5	0x5c38	No error (0)	assets.msn.com	assets.msn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2021 11:37:57.204243898 CET	8.8.8.8	192.168.2.5	0xc934	No error (0)	hblg.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:01.395544052 CET	8.8.8.8	192.168.2.5	0x751e	No error (0)	lg3.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:02.286330938 CET	8.8.8.8	192.168.2.5	0xe937	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:02.286330938 CET	8.8.8.8	192.168.2.5	0xe937	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:02.286330938 CET	8.8.8.8	192.168.2.5	0xe937	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:03.928791046 CET	8.8.8.8	192.168.2.5	0x7f5c	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - btloader.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49805	104.26.7.139	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-22 10:38:02 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 10:38:02 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 10:38:02 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: 1168 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=O7OmytPUbmst2uj2RPkJHsBBZ9Sj7EQhwN9Et1hjO4Y7iHTbLwdlMR4CIgadFJDoKLPbvIbthnLPFCcJBKD2MbPVh3hrGjV9iwCXDsxkBoCoFdRQfFCfA3Afcc9prg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b2186a10b666937-FRA
2021-11-22 10:38:02 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 10:38:02 UTC	1	IN	Data Raw: 29 7b 69 66 28 61 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 22 47 65 6e 65 72 61 74 6f 72 20 69 73 20 61 6c 72 65 61 64 79 20 65 78 65 63 75 74 69 6e 67 2e 22 29 3b 66 6f 72 28 3b 63 3b 29 74 72 79 7b 69 66 28 61 3d 31 2c 72 26 26 28 69 3d 32 26 74 5b 30 5d 3f 72 2e 72 65 74 75 72 6e 3a 74 5b 30 5d 3f 72 2e 74 68 72 6f 77 7c 7c 28 28 69 3d 72 2e 72 65 74 75 72 6e 29 26 26 69 2e 63 61 6c 6c 28 72 29 2c 30 29 3a 72 2e 6e 65 78 74 29 26 26 21 28 69 3d 69 2e 63 61 6c 6c 28 72 2c 74 5b 31 5d 29 29 2e 64 6f 6e 65 29 72 65 74 75 72 6e 20 69 3b 73 77 69 74 63 68 28 72 3d 30 2c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 61 6c 75 65 5d 29 2c 74 5b 30 5d 29 7b 63 61 73 65 20 30 3a 63 61 73 65 20 31 3a 69 3d 74 3b 62 72 65 61 6b 3b 63 61 Data Ascii:){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;ca
2021-11-22 10:38:02 UTC	2	IN	Data Raw: 6e 64 43 68 69 6c 64 28 65 29 7d 29 7d 76 61 72 20 75 2c 61 2c 64 2c 62 2c 6d 3b 75 3d 22 36 32 30 38 30 38 36 30 32 35 39 36 31 34 37 32 22 2c 61 3d 22 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 64 3d 22 61 70 69 2e 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 62 3d 22 32 2e 30 2e 32 2d 32 2d 67 66 64 63 39 30 35 34 22 2c 6d 3d 22 22 3b 76 61 72 20 6f 3d 7b 22 6d 73 6e 2e 63 6f 6d 22 3a 7b 22 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 74 72 75 65 2c 22 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 22 77 65 62 73 69 74 65 5f 69 64 22 3a 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 35 32 22 7d 7d 2c 77 3d 7b 74 72 61 63 65 49 44 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 69 66 28 21 65 7c 7c 22 6e 75 Data Ascii: ndChild(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(!e||"nu
2021-11-22 10:38:02 UTC	4	IN	Data Raw: 65 49 44 3d 6f 5b 6e 5d 2e 77 65 62 73 69 74 65 5f 69 64 2c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 29 3b 74 7c 7c 28 28 6e 65 77 20 49 6d 61 67 65 29 2e 73 72 63 3d 22 2f 2f 22 2b 64 2b 22 2f 6c 3f 65 76 65 6e 74 3d 75 6e 6b 6e 6f 77 6e 44 6f 6d 61 69 6e 26 6f 72 67 3d 22 2b 75 2b 22 26 64 6f 6d 61 69 6e 3d 22 2b 65 29 7d 28 29 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 74 61 67 5f 64 3d 7b 6f 72 67 49 44 3a 75 2c 64 6f 6d 61 69 6e 3a 61 2c 61 70 69 44 6f 6d 61 69 6e 3a 64 2c 76 65 72 73 69 6f 6e 3a 62 2c 77 65 62 73 69 74 65 73 44 61 74 Data Ascii: eID=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,websitesDat
2021-11-22 10:38:02 UTC	5	IN	Data Raw: 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 7d 2c 61 2b 3d 74 7d 29 7d 76 61 72 20 64 3d 74 5b 65 Data Ascii: trunc(100*(+o+0)),max:Math.trunc(100*(+o+0+t))},o+=t})}var l=t[0];if(null!=l&&l.bundles){var s=o,u=1-o;Object.keys(l.bundles).sort().forEach(function(e){var t=l.bundles[e];i[e]={min:Math.trunc(100*(s+u*a)),max:Math.trunc(100*(s+u*(a+t)))},a+=t})}var d=t[e
2021-11-22 10:38:02 UTC	7	IN	Data Raw: 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 76 65 6e 74 28 22 43 75 73 74 6f 6d 45 76 65 6e 74 22 29 3b 61 2e 69 6e 69 74 43 75 73 74 6f 6d 45 76 65 6e 74 28 74 2c 6e 2e 62 75 62 62 6c 65 73 2c 6e 2e 63 61 6e 63 65 6c 61 62 6c 65 2c 6e 2e 64 65 74 61 69 6c 29 2c 77 69 6e 64 6f 77 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 61 29 7d 66 3d 7b 7d 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 69 6e 74 72 6e 6c 3d 7b 74 72 61 63 65 49 44 3a 77 2e 74 72 61 63 65 49 44 7d 3b 74 72 79 7b 21 66 75 6e 63 74 69 6f 6e 28 29 7b 72 28 74 68 69 73 2c 76 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 65 2e 6c 61 62 65 6c 29 Data Ascii: ocument.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(e.label)

Timestamp	kBytes transferred	Direction	Data
2021-11-22 10:38:02 UTC	8	IN	Data Raw: 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 7c 6c 67 65 20 7c 6d 61 Data Ascii: entEnabled="true"==localStorage.getItem("forceMobileContent")||p.mobileContentEnabled),p.websiteID &&p.contentEnabled&&(!(n=/(android|bb\d+|meego).+mobile|avantgo|badaV|blackberry|blazer|compal|elaine|fennec| hiptop|iemobile|ip(hone|od)|iris|kindle|lge |ma
2021-11-22 10:38:02 UTC	9	IN	Data Raw: 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 28 30 37 7c 31 32 7c 32 Data Ascii: z)|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(07|12|2

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 576 Parent PID: 1000

General

Start time:	11:37:19
Start date:	22/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\619b721d39f71.dll"
Imagebase:	0x960000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
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: 00000000.00000002.838163135.0000000001100000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.838084722.00000000010F0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5708 Parent PID: 576

General

Start time:	11:37:19
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\619b721d39f71.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: 5308 Parent PID: 576

General

Start time:	11:37:19
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\619b721d39f71.dll
Imagebase:	0x1a0000
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: 00000002.00000002.839159615.00000000031D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.839120739.00000000031C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 984 Parent PID: 5708

General

Start time:	11:37:19
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\619b721d39f71.dll",#1
Imagebase:	0xd40000
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: 00000003.00000002.839122166.0000000004CB0000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.839163812.0000000004CC0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: iexplore.exe PID: 4404 Parent PID: 576

General

Start time:	11:37:20
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:	0x7ff7f2b30000
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: 5180 Parent PID: 576

General

Start time:	11:37:20
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\619b721d39f71.dll,DllRegisterServer
Imagebase:	0xd40000
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: 00000005.00000002.838215057.0000000000CE0000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.838316194.0000000000CF0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: iexplore.exe PID: 6204 Parent PID: 4404

General

Start time:	11:37:21
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:4404 CREDAT:17410 /prefetch:2
Imagebase:	0xb90000
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: 6268 Parent PID: 576

General

Start time:	11:37:25
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\619b721d39f71.dll,ajdpigjhocqby
Imagebase:	0xd40000
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: 6368 Parent PID: 576

General

Start time:	11:37:29
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\619b721d39f71.dll,arjmszzymit
Imagebase:	0x7ff797770000
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