ID: 527046
Sample Name: WTXuYxax6d.dll
Cookbook: default.jbs
Time: 10:50:29
Date: 23/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report WTXuYxax6d.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 43
General 43
File Icon 43
Static PE Info 44
General 44
Entrypoint Preview 44
Data Directories 44
Sections 44
Resources 44
Imports 44
Exports 44
Possible Origin 44
Network Behavior 44
Network Port Distribution 44
TCP Packets 44
UDP Packets 45
DNS Queries 45
DNS Answers 46
HTTP Request Dependency Graph 48
HTTPS Proxied Packets 48
Code Manipulations 49
Statistics 49
Behavior 49

System Behavior 50
Analysis Process: loaddll32.exe PID: 6980 Parent PID: 1868 50
General 50
File Activities 50
Analysis Process: cmd.exe PID: 6992 Parent PID: 6980 50
General 51
File Activities 51
Analysis Process: regsvr32.exe PID: 7000 Parent PID: 6980 51
General 51
File Activities 52
Analysis Process: rundll32.exe PID: 7012 Parent PID: 6992 52
General 52
File Activities 53
Analysis Process: iexplore.exe PID: 7020 Parent PID: 6980 53
General 53
File Activities 53
Registry Activities 53
Analysis Process: rundll32.exe PID: 7052 Parent PID: 6980 54
General 54
File Activities 54
Analysis Process: iexplore.exe PID: 7104 Parent PID: 7020 54
General 54
File Activities 55
Registry Activities 55
Analysis Process: rundll32.exe PID: 3684 Parent PID: 6980 55
General 55
Analysis Process: rundll32.exe PID: 6164 Parent PID: 6980 55
General 55
Disassembly 55
Code Analysis 55

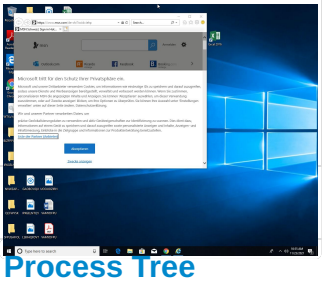
Windows Analysis Report WTXuYxax6d.dll

Overview

General Information

Sample Name:	WTXuYxax6d.dll
Analysis ID:	527046
MD5:	cbe2a109ef92af5..
SHA1:	e71ab85a35df851.
SHA256:	450a436cf830b03.
Tags:	dll geo Gozi ISFB ITA ursnif
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

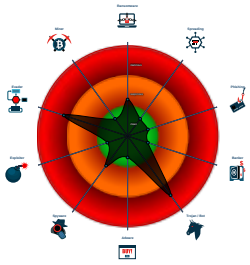
Ursnif

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Multi AV Scanner detection for doma…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- Contains functionality to check if a d…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6980 cmdline: loaddll32.exe "C:\Users\user\Desktop\WTXuYxax6d.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6992 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\WTXuYxax6d.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7012 cmdline: rundll32.exe "C:\Users\user\Desktop\WTXuYxax6d.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 7000 cmdline: regsvr32.exe /s C:\Users\user\Desktop\WTXuYxax6d.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 7020 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 7104 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:7020 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 7052 cmdline: rundll32.exe C:\Users\user\Desktop\WTXuYxax6d.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3684 cmdline: rundll32.exe C:\Users\user\Desktop\WTXuYxax6d.dll,azfdnkcrayghb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6164 cmdline: rundll32.exe C:\Users\user\Desktop\WTXuYxax6d.dll,bngggbakts 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
00000002.00000003.620315557.00000000053B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000002.883888908.0000000004D49000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000005.00000002.884237946.00000000052F8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.613835753.00000000052F8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.612905346.0000000004FD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 67 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.2b80000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.920000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.a60000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.a80000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.regsvr32.exe.4ea94a0.4.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 23 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

Yara detected Ursnif

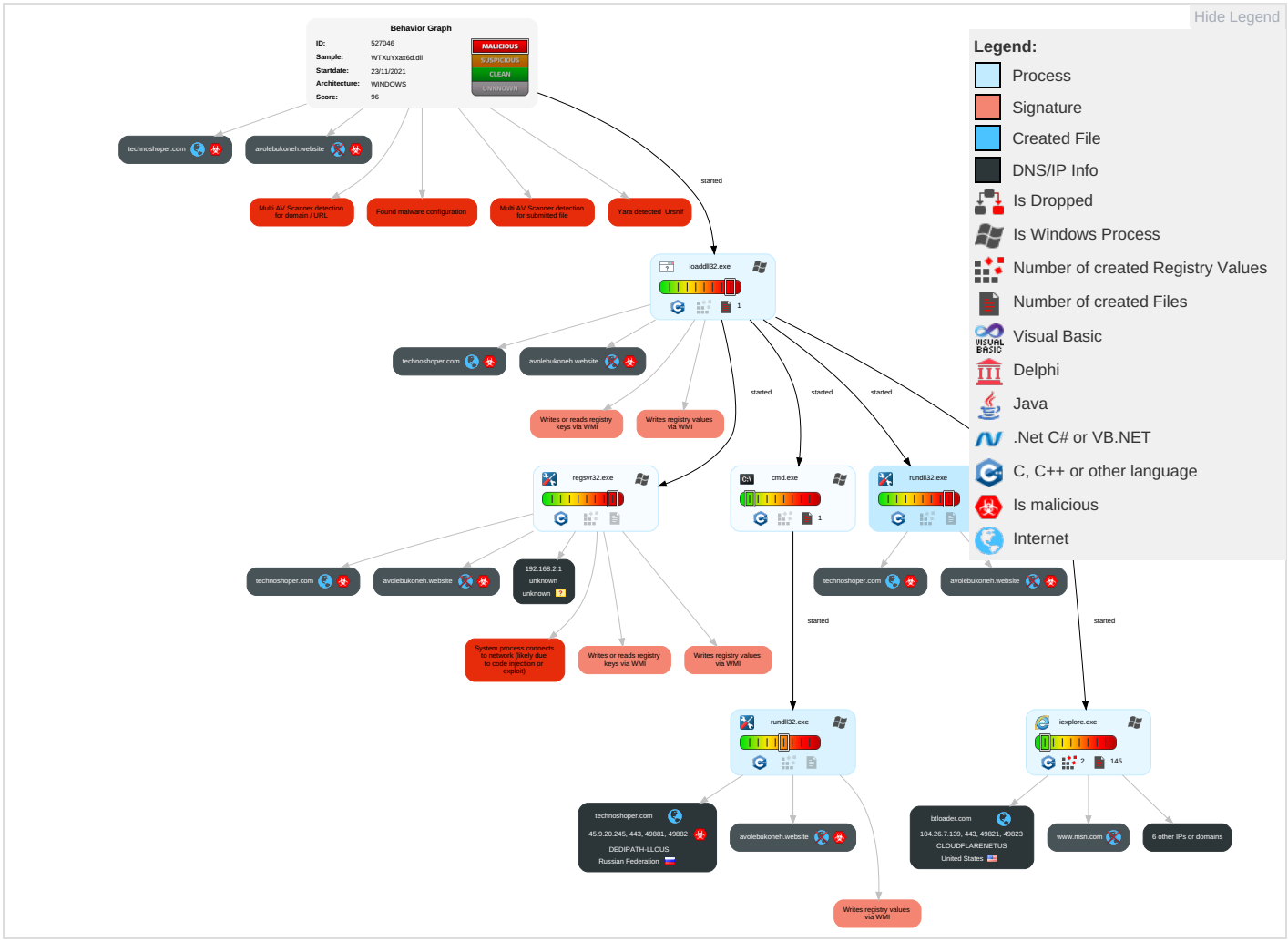
Remote Access Functionality:

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	Netw Effec
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eave Inse Netw Com
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Obfuscated Files or Information 3	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 2 1	Expl Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Information Discovery 1 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Regsvr32 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

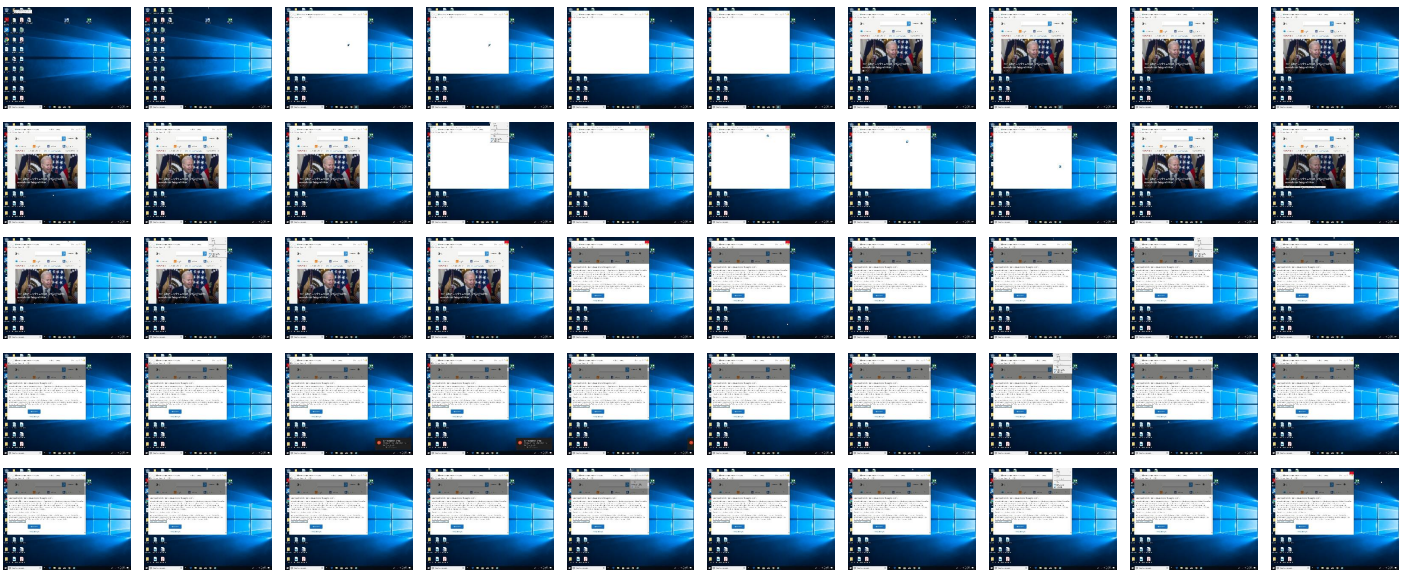
Behavior Graph

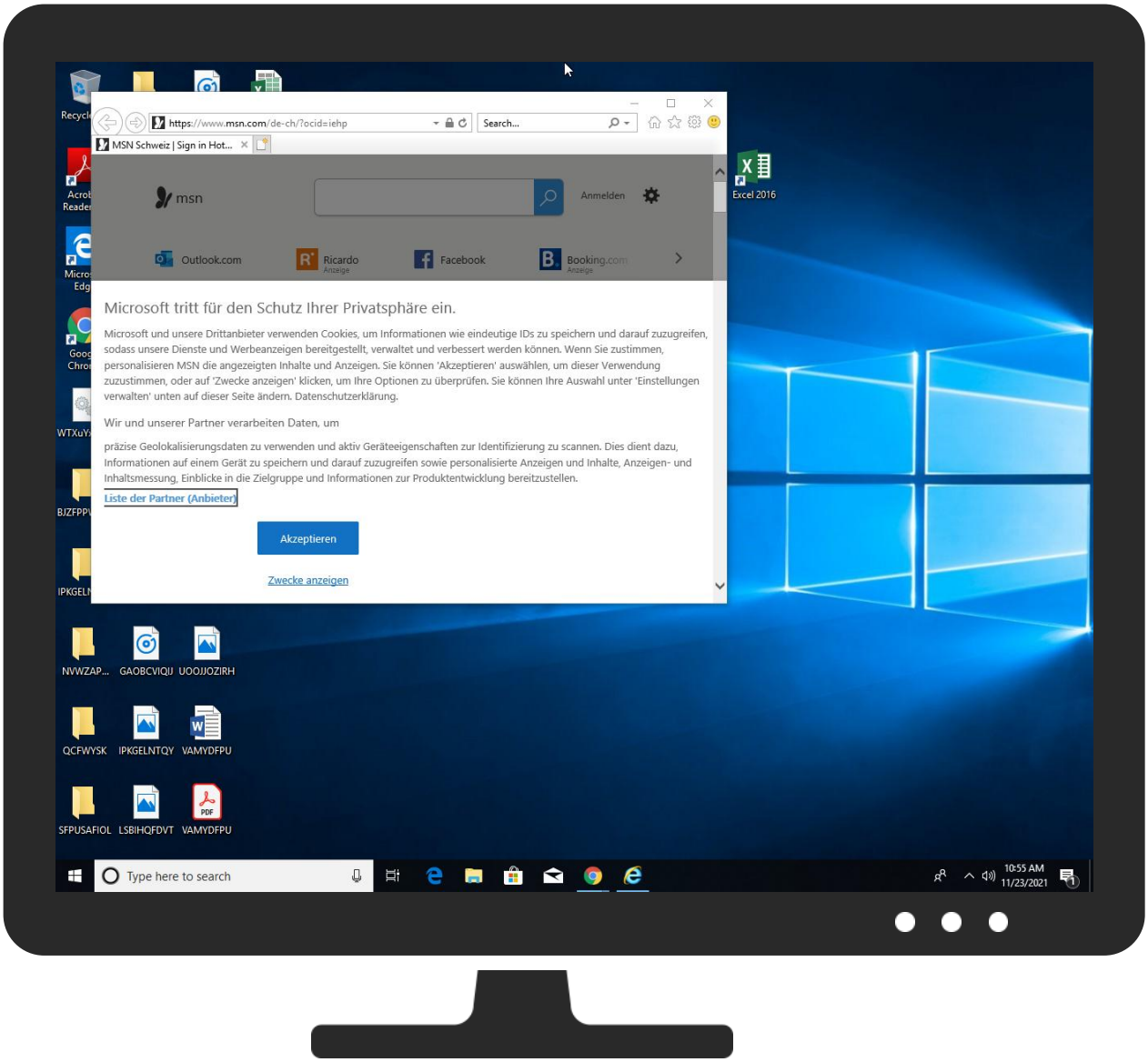


Screenshots

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
WTXuYxax6d.dll	18%	Virustotal		Browse
WTXuYxax6d.dll	25%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.a60000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
2.2.regsvr32.exe.9f0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
5.2.rundll32.exe.2bb0000.3.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.a80000.3.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
2.2.regsvr32.exe.d80000.3.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.920000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.a90000.3.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
technoshoper.com	6%	Virustotal		Browse
btloader.com	1%	Virustotal		Browse
avolebukoneh.website	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://avolebukoneh.website/e	0%	Avira URL Cloud	safe	
http://https://technoshoper.com/H	0%	Avira URL Cloud	safe	
http://schemas.mic	0%	URL Reputation	safe	
http://avolebukoneh.website	6%	Virustotal		Browse
http://avolebukoneh.website	0%	Avira URL Cloud	safe	
http://https://technoshoper.com/glik/qu_2BrFb5C/WnN6ktioLVJSC7NZ8/8U42mL0TVXds/GucNTaVpvRD/cGAaQnoHqkvTq7/u	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://https://avolebukoneh.website/glik/kUbizXMZCF/wcseO9tQzGMWY7_2B/Eo6XsQr55EXJ/TJZ97_2F328/3bdZBpl1pP_2	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://technoshoper.com	0%	Avira URL Cloud	safe	
http://https://technoshoper.com/k	0%	Avira URL Cloud	safe	
http://https://technoshoper.com/Y	0%	Avira URL Cloud	safe	
http://https://technoshoper.com/glik/DGgts_2FWsor6_2F7EcO1Do/0g4WUbLA1T/K9_2Bu0NIeWan9Hma/XZBvL_2BDNj7/jAap	0%	Avira URL Cloud	safe	
http://https://avolebukoneh.website/II	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	
http://https://avolebukoneh.website/l	0%	Avira URL Cloud	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://avolebukoneh.website/glik/pAGZhq9MI53nZ7OH/rIg4LX9fBTj6pjl/8TeMZNhc43A_2FVYsQ/YCg3QZ_2F/BXKX	0%	Avira URL Cloud	safe	
http://https://technoshoper.com/glik/rHKCmFtHVZPPm/wqY5wPH_/2F29vTv7wl_2FGq_2BrLvy6/oSB1MCzJ6Y/1nsQKibmjik_	0%	Avira URL Cloud	safe	
http://https://avolebukoneh.website/glik/oPO1MTCZATyGVB9JDx/_2BxLrMZv/XGH5EgNCAONySOCpr4U_/2F_2FSC6yLxw_2BR	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://assets.onestore.ms/cdnfiles/external/mwf/long/v1/v1.25.0/css/mwf-west-european-default.min.c	0%	Avira URL Cloud	safe	
http://avolebukoneh.website/glik/.lwe.bmp08899	0%	Avira URL Cloud	safe	
http://https://assets.onestore.ms/cdnfiles/onestorerolling-1605-16000/shell/common/respond-proxy.html	0%	Avira URL Cloud	safe	
http://avolebukoneh.website/glik/.lwe.bmp088991256473871MNTYAIDA1010010B	0%	Avira URL Cloud	safe	
http://https://avolebukoneh.website/glik/KwktcAgJA3haqk0/Ms0fL0B4XccTTFIyK9/usG_2BHjp/uyERKVkE6Su_2Fw3uS2y/	0%	Avira URL Cloud	safe	
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	0%	URL Reputation	safe	
http://https://docs.microsoft.co	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	2.18.160.23	true	false		high
hblg.media.net	2.18.160.23	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lg3.media.net	2.18.160.23	true	false		high
technoshoper.com	45.9.20.245	true	true	• 6%, Virustotal, Browse	unknown
btloader.com	104.26.7.139	true	false	• 1%, Virustotal, Browse	unknown
avolebukoneh.website	unknown	unknown	true	• 6%, 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
45.9.20.245	technoshoper.com	Russian Federation		35913	DEDIPATH-LLCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	527046
Start date:	23.11.2021
Start time:	10:50:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WTXuYxax6d.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:	29
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:	mal96.troj.evad.winDLL@17/114@45/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64.5% (good quality ratio 60.5%) • Quality average: 79.3% • Quality standard deviation: 29.7%

HCA Information:	• Successful, ratio: 95% • 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

Time	Type	Description
10:53:19	API Interceptor	13x Sleep call for process: regsvr32.exe modified
10:53:19	API Interceptor	26x Sleep call for process: rundll32.exe modified
10:54:14	API Interceptor	8x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.26.7.139	619b721d39f71.dll	Get hash	malicious	Browse	
	619b721d39f71.dll	Get hash	malicious	Browse	
	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	
45.9.20.245	DAlmS4qg20.dll	Get hash	malicious	Browse	
	2W6FcgEeMy.dll	Get hash	malicious	Browse	
	tebdXHvUhB.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
contextual.media.net	V6oWh8Z20j.dll	Get hash	malicious	Browse	• 23.211.6.95
	V6oWh8Z20j.dll	Get hash	malicious	Browse	• 23.211.6.95
	481DGzXveG.dll	Get hash	malicious	Browse	• 23.211.6.95
	Qf3znUYo2b.dll	Get hash	malicious	Browse	• 23.211.6.95
	481DGzXveG.dll	Get hash	malicious	Browse	• 23.211.6.95
	Qf3znUYo2b.dll	Get hash	malicious	Browse	• 23.211.6.95
	DAlmS4qg20.dll	Get hash	malicious	Browse	• 2.18.160.23
	2W6FcgEeMy.dll	Get hash	malicious	Browse	• 2.18.160.23
	2zTgaLRFkL.dll	Get hash	malicious	Browse	• 2.18.160.23

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tebdXHvUhB.dll	Get hash	malicious	Browse	• 2.18.160.23
	619b721d39f71.dll	Get hash	malicious	Browse	• 2.18.160.23
	619b721d39f71.dll	Get hash	malicious	Browse	• 2.18.160.23
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 2.18.160.23
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 2.18.160.23
	malware.dll	Get hash	malicious	Browse	• 2.18.160.23
	kZ45hWt9ul.dll	Get hash	malicious	Browse	• 2.18.160.23
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 23.211.6.95
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 23.211.6.95
	loveTubeLike.dll	Get hash	malicious	Browse	• 104.76.200.23
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 23.211.6.95
hblg.media.net	V6oWh8Z20j.dll	Get hash	malicious	Browse	• 23.211.6.95
	V6oWh8Z20j.dll	Get hash	malicious	Browse	• 23.211.6.95
	481DGzXveG.dll	Get hash	malicious	Browse	• 23.211.6.95
	Qf3znUYo2b.dll	Get hash	malicious	Browse	• 23.211.6.95
	481DGzXveG.dll	Get hash	malicious	Browse	• 23.211.6.95
	Qf3znUYo2b.dll	Get hash	malicious	Browse	• 23.211.6.95
	DAlmS4qg20.dll	Get hash	malicious	Browse	• 2.18.160.23
	2W6FcgEeMy.dll	Get hash	malicious	Browse	• 2.18.160.23
	2zTgaLRFkL.dll	Get hash	malicious	Browse	• 2.18.160.23
	619b721d39f71.dll	Get hash	malicious	Browse	• 2.18.160.23
	619b721d39f71.dll	Get hash	malicious	Browse	• 2.18.160.23
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 2.18.160.23
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 2.18.160.23
	malware.dll	Get hash	malicious	Browse	• 2.18.160.23
	kZ45hWt9ul.dll	Get hash	malicious	Browse	• 2.18.160.23
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 23.211.6.95
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 23.211.6.95
	loveTubeLike.dll	Get hash	malicious	Browse	• 104.76.200.23
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 23.211.6.95
	data.dll	Get hash	malicious	Browse	• 2.18.160.23

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	RFQ#00439811.exe	Get hash	malicious	Browse	• 45.144.225.147
	iP1ZMsVOo6.exe	Get hash	malicious	Browse	• 45.9.20.149
	jyM8NR8QU7.exe	Get hash	malicious	Browse	• 45.9.20.149
	Payment.xls	Get hash	malicious	Browse	• 45.133.1.84
	VBELHQLOAs.exe	Get hash	malicious	Browse	• 45.9.20.149
	RFQ#00439811.exe	Get hash	malicious	Browse	• 45.144.225.147
	ZrAv540yA4.exe	Get hash	malicious	Browse	• 45.9.20.149
	6Xtf11WnP2.exe	Get hash	malicious	Browse	• 45.9.20.149
	IGG2RkgBzU.exe	Get hash	malicious	Browse	• 45.133.1.84
	EFT-11-22-201.html	Get hash	malicious	Browse	• 66.151.174.10
	Pago de Recibo.xls	Get hash	malicious	Browse	• 45.133.1.84
	M9WBCy4NNi.exe	Get hash	malicious	Browse	• 45.9.20.149
	EFT-11-22-201.html	Get hash	malicious	Browse	• 66.151.174.10
	wj1j21cmxi.exe	Get hash	malicious	Browse	• 45.9.20.149
	DAlmS4qg20.dll	Get hash	malicious	Browse	• 45.9.20.245
	2W6FcgEeMy.dll	Get hash	malicious	Browse	• 45.9.20.245
	tebdXHvUhB.dll	Get hash	malicious	Browse	• 45.9.20.245
	Y5EGM7BygT.exe	Get hash	malicious	Browse	• 45.9.20.149
	KSc3rYBX6Z.exe	Get hash	malicious	Browse	• 45.9.20.149
	BVxT3jA2K0.exe	Get hash	malicious	Browse	• 45.9.20.149
CLOUDFLARENETUS	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 104.21.71.149
	Ozmxatmtnyjmmnespgaqcxwhfqpufmkzto.exe	Get hash	malicious	Browse	• 162.159.133.233
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 104.21.71.149
	iP1ZMsVOo6.exe	Get hash	malicious	Browse	• 162.159.129.233
	VDnn1698j5.exe	Get hash	malicious	Browse	• 172.67.188.154
	TEiwRyJ2v1.exe	Get hash	malicious	Browse	• 172.67.188.154
	Ozmxatmtnyjmmnespgaqcxwhfqpufmkzto.exe	Get hash	malicious	Browse	• 162.159.129.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	T0wxwBjIdR.exe	Get hash	malicious	Browse	• 104.21.62.32
	jyM8NR8QU7.exe	Get hash	malicious	Browse	• 162.159.134.233
	sBz6zVtsB1.exe	Get hash	malicious	Browse	• 172.67.188.154
	THUAN PHAT - ORDER CF005548 - #U00e9tiquette DHL3Y53479213784593234.exe	Get hash	malicious	Browse	• 162.159.134.233
	DHL express 5809439160_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment Slip.xlsx	Get hash	malicious	Browse	• 172.67.205.83
	20002.xlsx	Get hash	malicious	Browse	• 104.21.62.32
	FIAA PO-200036452676.exe	Get hash	malicious	Browse	• 104.21.64.38
	New Orders.exe	Get hash	malicious	Browse	• 104.21.19.200
	YPJ-76577.exe	Get hash	malicious	Browse	• 104.21.19.200
	inter snake.exe	Get hash	malicious	Browse	• 172.67.188.154
	0PBOMB3aN9.exe	Get hash	malicious	Browse	• 104.21.88.245
	VBELHQLOAs.exe	Get hash	malicious	Browse	• 162.159.134.233

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	V6oWh8Z20j.dll	Get hash	malicious	Browse	• 104.26.7.139
	V6oWh8Z20j.dll	Get hash	malicious	Browse	• 104.26.7.139
	481DGzXveG.dll	Get hash	malicious	Browse	• 104.26.7.139
	Qf3znUYo2b.dll	Get hash	malicious	Browse	• 104.26.7.139
	481DGzXveG.dll	Get hash	malicious	Browse	• 104.26.7.139
	Qf3znUYo2b.dll	Get hash	malicious	Browse	• 104.26.7.139
	Clti.xlsx	Get hash	malicious	Browse	• 104.26.7.139
	Vernon.xlsx	Get hash	malicious	Browse	• 104.26.7.139
	Activation Online Mail.htm	Get hash	malicious	Browse	• 104.26.7.139
	Renee.schneider.html	Get hash	malicious	Browse	• 104.26.7.139
	DAlmS4qg20.dll	Get hash	malicious	Browse	• 104.26.7.139
	2W6FcgEeMy.dll	Get hash	malicious	Browse	• 104.26.7.139
	2zTgaLRFkL.dll	Get hash	malicious	Browse	• 104.26.7.139
	619b721d39f71.dll	Get hash	malicious	Browse	• 104.26.7.139
	619b721d39f71.dll	Get hash	malicious	Browse	• 104.26.7.139
	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

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\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):	5.1927425956439235
Encrypted:	false
SSDEEP:	3:D9yRtFwsx6wmxvFuqLHIfiAANEJGX7T4mEYldufUXVlNROqSmfRKb:JUFkduqsiAANEIXH4mE8dufEIOwb
MD5:	97D066790F446B2355842BDC31161621
SHA1:	79B67BB9C6CAAF003EA680A2A6709433CA6C1B32
SHA-256:	F13D8638250DE1808D29F92C6B80F79DDF12C78A875577C87BECBC47B5F47377
SHA-512:	C790616D0277A5017FF26E416A87FE216C22BC69F99C6224CDAAB9364B571546D994EEBE1426C5E81E928AF9B7F62C1FCFCB494CB48E743ADBE25444B9C7A985
Malicious:	false
Preview:	<root><item name="BT_AA_DETECTION" value="{"ab":true,"acceptable":false}" ltime="1230238320" htime="30924955" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5EF2C13C-4C8E-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	1.9065712172685974
Encrypted:	false
SSDEEP:	12:rl0YmGFLQrEgm2p+IaCyJBMu/GgCF/nlWrEgm2p+IaCyJBMu/GeF8Mu0G77/Mu07:rJQGW/4h+WGW/4hj8hth69lW/Hw
MD5:	A7191FCBA7354DF63848F0E32E44E3B5
SHA1:	CBD943E767E2A9158615DEF6B6D28E3CE3E21143
SHA-256:	4D16881E8A8F181F7CB39F490E5B2548FD6A2E395409E081C4D38D4AF1F8035C
SHA-512:	F21B5449868E60D6BC7D2A85A68DD001B2B798B1FC5CC41F8604480B143E372802F47E6C591AC692FE03AA7E9FFFD96B18634B80B2068AA3B5194A07F0F5C028
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....t.0.....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.P.c.H.y.X.o.5.M.7.B.G.Q.5.e.z.0.u.y.0.k.l.g.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5EF2C13E-4C8E-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	330752
Entropy (8bit):	3.59886128947096
Encrypted:	false
SSDEEP:	3072:hZ/2Bfcdmu5kgTzGtlZ/2Bfc+mu5kgTzGt5Z/2Bfcdmu5kgTzGtfZ/2Bfc+mu5kn:Iz3M
MD5:	F9F14BC733510635E8DB74A98E2766D6
SHA1:	FA81A1035CE77D6B7B663C58AD1797828D5D556E
SHA-256:	A0B2AD31B993E2675CF243039790059BA739A4DFD32757A289B06E51614C00E1
SHA-512:	AA631E62C24848235EC85010B5F110CB4A0D66BF328AD9302ECCDFDF7FEC371B5CDB50FE6674A1A09A6EBAB5218362DFF3DA7B93430068EDAF761111F74251 C
Malicious:	false
Preview:	.....>.....E...F...G...H..... .....R.o.o.t. . E.n.t.r.y.....p*.^.....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):	358
Entropy (8bit):	5.0970008444066845
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc41Ep/VoIoUBtTD90/QL3WIZK0QhPPNbVDHkEtMjwu:TMHdNMNxOEpdoIoUBtnWimI00OVbVbkt
MD5:	B1F3FAC4DE3508CF9AAE72B9A1D8954C
SHA1:	EB9655A1ECB9D5318595DD148D6F408A8A4477BA
SHA-256:	B64E776FCA454B340ECF26C3ABFE078D9BDD53BDDE029F1DF54187FFD323D3E2
SHA-512:	AD0D6D8309FC9CEB8E31FA8DF5019BDE71D79EE884C27D0A32FD2D76849C77CECFC7511CE577FFDAA15F5FD9FF3CA017BB4638092CC972079229A0A05839F C8

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x5cea86ad,0x01d7e09b</date><accdate>0x5d098694,0x01d7e09b</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.137422073511568
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4fLGTkpaO6TD90/QL3WIZK0QhPPNbkI5kU5EtMjwu:TMHdNMNxe2kpa7nWimI00OVbkak6EtMb
MD5:	8B35A6C01C00BC38EFCA757A160B2E30
SHA1:	F3BDBAF90522F5CC5D6016A4D5E609CBE5B97836
SHA-256:	16F77854E3DBC6831657E31C9022B4D531D5283FEF93390A4B71CBC0CFF9C94D
SHA-512:	FDF08DA827A5775558CE078D1C952AFC16BA0612F07DBBD01E4E0B72201DCB2BE0D9D4097A66837325CE216552FF0F8EFC214DCD91D3AFB383C47295CCD591A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x5b317322,0x01d7e09b</date><accdate>0x5b507290,0x01d7e09b</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):	362
Entropy (8bit):	5.11461645242108
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4GL1e+FR2TD90/QL3WIZK0QhPPNbyhBcEEtMjwu:TMHdNMNxvL1e+/2nWimI00OVbmZEtMb
MD5:	4498C163B7201DC686B564823A2560B4
SHA1:	957994F82B8714D568FE72D8B479F1F2D4359F3D
SHA-256:	68E651B999E0D3C8C0296536AF9FC1483D7AFBFF7565F5F680F0E20AC06EDA1D
SHA-512:	79A49770C9CD56A2FCE8EF42630440168A15AE4AAE3A1EE3AC6E8B237A896B561451D8E25375515774C68863EB91A3C74EA9ABC2EAE4DD15B9EFF8BE75A1BA0C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x5d2883df,0x01d7e09b</date><accdate>0x5d405a1e,0x01d7e09b</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):	352
Entropy (8bit):	5.107217072236228
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4JuBnotTD90/QL3WIZK0QhPPNbgE5EtMjwu:TMHdNMNxiVtnWimI00OVbd5EtMb
MD5:	48CF4F5B7D7AD1490C663CA70A4C8E51
SHA1:	A0514DE8485EA9215E5625D1D30128F0FDF0C609
SHA-256:	A3CB4A5AA29D72BEF68F9B033CC17F0C6255F793DA917A22CB0674B644223167
SHA-512:	66BF8EF55B701DC7E6628AE8A323636E0A56B903367986CDED7C995A4F32BEB3AB4B8FEB3BCA03CA45BF808F3462D7D001E6F0B08A24ED76555F3B5C9E7D985
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x5c0f2e19,0x01d7e09b</date><accdate>0x5c5b78e6,0x01d7e09b</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):	358
Entropy (8bit):	5.1228504566378605

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4UxGwe0KVTD90/QL3WIZK0QhPPNb8K0QU5EtMjwu:TMHdNMNxhGwYnWimI00OVb8K075EtMb
MD5:	C6B6BC244C99F61BABCE2FBCB22E64D9
SHA1:	35A3081339A890731A22CB85DDFE5D4DC528B323
SHA-256:	BEFD9D0864A11740FD1D2194421C6EA1B231F667F602F240F45B1AB2C0423DD0
SHA-512:	FB00C826781DB7370F2C1A0059C5BE1248B0BEC93648A7953ADBB11A7336265E8DDC5F68148D9C1D91B3FF78CCF53D45A71F66A62B8D5A6F7642E72AB2BF11C A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x5d6da6d7,0x01d7e09b</date> accdate>0x5d8ca4fa,0x01d7e09b</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Y outube.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):	356
Entropy (8bit):	5.081707677158787
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4QunT7otTD90/QL3WIZK0QhPPNbAkEtMjwu:TMHdNMNx0nTktnWimI00OVbxEtMb
MD5:	47652013AFC9AF67190B37EB614D396C
SHA1:	C51501AC8B9CEF00D071F79E4CD282D716D6BB4D
SHA-256:	3AF31E81025325A3632FB3E16B9C8DC5682F93DC5855DC430A3F02B1DE861D57
SHA-512:	EA8D363513CA0A607616EEC8B9B943CD746D2C84E9CBB620358EB41BBB1B7F2C37C17FE8E7D71EF44FF1839DD109F3576CF2A21DFA97EB5F8A56DFE7E7A815 F3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x5cb613fa,0x01d7e09b</date><a ccdate>0x5cd510d6,0x01d7e09b</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Re ddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.15587133580377
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4oTMKg5WTD90/QL3WIZK0QhPPNb6Kq5EtMjwu:TMHdNMNxxMVcnWimI00OVb6Kq5EtMb
MD5:	0EB17AA2E180F04788F785319FC39B4C
SHA1:	2248ADB5B5FE871D76E86773E8FD163AE17CF4CA
SHA-256:	258975832AD973D8DC8314326734FFB84E3375CF48009530E522D2BAEC9C4030
SHA-512:	56204FCEFB628C2B7A0A161B0C08034811F0244073574B6E1C11D6464D2DE4964A60C75B1C79DD50022BCE14688FB08AD2D4153224A6282C618CC3C8B851FD2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x5c781627,0x01d7e09b</date> accdate>0x5c971518,0x01d7e09b</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\N YTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.11597956611254
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4YX2nxbCR3+tTD90/QL3WIZK0QhPPNb02CqEtMjwu:TMHdNMNxcVCRGnWimI00OVbVEtMb
MD5:	AD6D14E1F6A7EAB6D68C17CB61A79D32
SHA1:	9C00B35B4962FBA3522CA4984A835ACFC52FDB4B
SHA-256:	0B97A3543161D5EAC060D387075AB6C6298C2DD0FDCDC45066BACFA6D6BD2770
SHA-512:	35EACE8ECC26E15D1A1E5D6C7CD7D331B6ED28084053C2153C479267E785CC916F30CC7C9578C16E259ECBB9629083BCF7526FA4E1592309161D3F0C8574E4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x5b7697ab,0x01d7e09b</date> <accdate>0x5bc2e279,0x01d7e09b</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):	356
Entropy (8bit):	5.109820030314615
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4In1Mb3UBtTD90/QL3WIZK0QhPPNbiwE5EtMjwu:TMHdNMNxfnm3YtnWimI00OVbe5EtMb
MD5:	38BA1865E79F13A9C6144FF8805DAC18
SHA1:	A7FB833B9D86256754C01619C379BD9000A86300
SHA-256:	E83FD15047BD1631464CA165C076679E74EF52B207D974DCE1508DDCF7EB3E49
SHA-512:	A01720EC47223E0B36EFD56B3E67C3771D3AB77527853A33A7E9A407502DF489A500CAF7C963798F77ABCAA99FF714F6C02B0255AF09C664C1E1AB6750EEEA5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x5bd858d8,0x01d7e09b</date><accdate>0x5bf75616,0x01d7e09b</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\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	21318
Entropy (8bit):	4.109053117861958
Encrypted:	false
SSDEEP:	96:yQQQQQtzS29dcBUXqYkE1fwDzXrzS29dcBUXqY:bzSAcBykEBczbzSAcBq
MD5:	AFAFED39473C261B5057A5DADAB60447
SHA1:	4646A2A85D04594044597A771FE5912685023281
SHA-256:	D87F66224329BD8EED915F49DAA1F5A7B13984A941E3D7FA1586CE164CDC7112
SHA-512:	81B24BECA1D93E4EEF591EFD1A9A5AD27D96B4B355DCEA8E4A6F3B192F50E133B8934F4FA3B67C2A5774178AA770D7BD2CDE029088C4A5E75A38DCA2B3ABD466
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"""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\4996b9[2].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 45633, version 1.0
Category:	dropped
Size (bytes):	45633
Entropy (8bit):	6.523183274214988
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
Preview:	wOFF.......A............................,....OS/2...p...`...`B.Y.cmap.............G.glyf.......,...,0..Hhead.......6...6....hhea...,...$...$....hmtx............($LKloca...`...f...f....maxp...P... ... .name... ....IU..post....... ... .*...........I.A_.<........... ....d.*.......................^...q.d.Z...3.......3.....f.............................HL .@...U...f....................... ....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.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\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\55a804ab-e5c6-4b97-9319-86263d365d28[1].json

SHA-256:	886E0D5D43DFB17D92EB8C5C80AB0671ED9DE247EC4AD9D71B358F32F7613287
SHA-512:	97FA869A8BE850E759BDB5AAA0E850B787358CC4EED55796F6B51D1AFD5B6B25CF7A6FAC5FCD67AA9588876F208D40449ED94886046177B6FEAA083743B01696
Malicious:	false
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":true,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","gb","ws","gd","ge","gg"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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..$....`.....c@O..|b.....r..... m.....o.q}...}...?,.M.Go.....0J.*..E....j#}....'..d.....y....Ex.....NV"+G.cs.....;...+.V..."....w...W...@..$..rI_..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...IXdSg.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\3Y2ADQKS\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:	dropped
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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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.'cGl.&....y[.p6..8...L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAQVPm6[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2403
Entropy (8bit):	7.807847874907652
Encrypted:	false
SSDEEP:	48:QfAuETAzOifN8pL/nF/TFZoTy7zOWk0ljjGzRi3wWLtWOqO+zgtO:Qf7EwN8tndAW7zI0l0SRnqO+zgtO
MD5:	10BDCE1F28F778B6F7C76D396A88A0A3
SHA1:	705B774818562E65F4C0DC64A08D8D1E38932772
SHA-256:	EB966433ADA42DEA9BE343ECAFA32C13851D1ADAF91734E0697D96AE3B876D0A
SHA-512:	1BD59BED9431C26C14AA4545A6B459680BBDD855E20CE1FE2A5BD4B861DAA793CA9FA6EAF96F353099440E80DD2046E54577DD0B329C45B8EA5FE13CB08B67D0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAQVPm6[1].jpg	
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......K.d..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....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\3Y2ADQKS\AAQVTlD[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:	2F85B52188672BB53F92C7B80A8F2E3B2B31D0E6F99A3CB4D5D2C89A5F414CCC697DD6709689E619126902E6D0F7CB7866C8A2B3E6EECA8D3319F438DBBF85 3
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO........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\3Y2ADQKS\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:	0AF8BE812D1A05915C06EE377AD3CEB7C612A699238A3FDB07326FBDDD6E3539E8AC8FA643485383644FB67D1F284B0F52E81DCE75591D14CC5EFE950B798B 2
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?...&....~Z.@.......Z...@.b..(.sO. PR7`l....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\3Y2ADQKS\AAQXmCn[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):	2053
Entropy (8bit):	7.7444838178786135
Encrypted:	false
SSDEEP:	48:QfAuETAChSTvvelFjDyUJRN5Hi/cqYmOJA+wUqFWnu:Qf7EA+VT2nCJfZqAu
MD5:	BCF5C7A113C8BBAB535EDF9CCBE6490F
SHA1:	C55BB801302CCE7ED433F2EC82F65E473EE27377
SHA-256:	AE2DCD9205699F2D0A913DDC97A8B702E3A29555F2C1604B4A76C2BB18A8ACA8
SHA-512:	ACE81D2D98AF4523D24607CFAF48226F1E24CF50F886C48CCEFCF1D9F65A799FF8E3F5B5ACAD3716FEAA0490CB56543406C5C95A72903D86D2900910CC3240
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......K.d..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?.._..s...GyO........P...c.....F...Q.gc.5H...s..?.R$E.;...8...!......].o.zFj\.Y..N.#5.Hv%M>...*y...4k.....K.|...:....9..Z_..9O.`..g'... ..c..?..Z.;0.W.y })..)*iR7R.q.#.......v;........3..#.....W..Q.QH..O.......qe..%>V.CM.}.O.S.b..u...?Z|..7.Fo.q.....X...x.\.u.-........1wZvat/.f.us.Qf.B.....'....ngo..>.....|..Q.G4P]..%.....t! F.?.F4{@.......i{F.....U..sH......+......E....Hbc..O.U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAud6Gv[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	356
Entropy (8bit):	7.101459310090333
Encrypted:	false
SSDEEP:	6:6v/lhPahmpAKG4NDBbCySVUc3/qF9Hio9hbifyZQw+bS2LblMid1Rc9ruhiFp:6v/73bCLVYHio9h8kQw+7BMW1W9rAir
MD5:	A94D5FFB98CBCA323E6AEA6A826B9ACF
SHA1:	D4F20C419292258A27A06511955A02400C767723
SHA-256:	7527C0E97B871894A7AC475D714D51E82F51BB965848DCD03657B12D5808BCAB
SHA-512:	D2B0D68C085457161F612B50508548D9FD6F7F48DE74AEC8009C65375A0CF0D58469BC8B93AC2705B4AB4A0F0D3FE07E8207500AD896FFC676D7D50649643A7E
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...j.A.....A..y..X....$.E.'.b.:.h!.bc%...:.FlD..L.@:...F...o...u..+.>nvf..v..n.;08..<.,C....-|A.x.D1.Mx....B.R>.....3..d@.... %....v.Z...5.C....3@.a.[..iku.....%.(....p.h..m.](..s>F.&...q.^..dH.....0<a1...4. .z.Q.@<W...,...4..?M.b.....@{X..L..x...|:.B..B..K...j..k6/..LE@....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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+l9ocY5zwX9B:0l33oo/JqqOxrcnVskQK+lpY9B
MD5:	29792D182BA22B3E036424650829BEFE
SHA1:	BB13279B92AD154589A1569CA7AF19474B2FD832
SHA-256:	E6CEE354D756A03B5404D34D7F7433CA55B5D32AC5199A0A508AD3A379AABE06
SHA-512:	F137B17A8DD6783E5906BB8000A54B5FC5769DF5878369A48B5190CFA71392FA0352A4E92EC8F91D2A28BD9C5E977A101CDF0B52FD194ADEA5AB0FA0225CEAE A
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....A..M..P.....T.....@>..yR....G.(..\.jC0.<-cqp.`.1.h.)2.....W....fT...1...Q`.!o..I...ar..{.(1..#.)./\|.?Jar...(~h$..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\3Y2ADQKS\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:	modified
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\3Y2ADQKS\BB1ftEY0[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.316910976448212
Encrypted:	false
SSDEEP:	12:6v/7YEtTvpTjO7q/cW7Xt3T4kL+JxK0ew3Jw61:rEtTRTj/XtjNSJMkJw61
MD5:	7FBE5C45678D25895F86E36149E83534
SHA1:	173D85747B8724B1C78ABB8223542C2D741F77A9
SHA-256:	9E32BF7E8805F283D02E5976C2894072AC37687E3C7090552529C9F8EF4DB7C6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1ftEY0[1].png	
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\3Y2ADQKS\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\3Y2ADQKS\BBXXVfm[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):	842
Entropy (8bit):	7.712790381238881
Encrypted:	false
SSDEEP:	24:03eeNY8QugsamcgusRa+4Sm81pdhTaXHir8L:0fNY8QuosS+4SmetsL
MD5:	4F44C5854D2A321DE38DDA7580D99D2A
SHA1:	637217CD4AB94060B945D364D6AD80BB173F41B7
SHA-256:	77E9AF4EF4CEC6BAE0181D3173577BE0488DE8DB5FA71D2E5C7E05B5D5D27565
SHA-512:	AC46863DDFE68156E7D76DDE08C299459B8C01CD8B2DB9DB5C3A4434D5CF34F6162556A29EBBCA401810ED5AD5F9BE57090E819DDED688EE7C36D179A1FBF F6
Malicious:	false
Preview:	.PNG........IHDR.................a....pHYs.........+.....IDATx.e.Oh\U......2.....65...\...].,ZT...Z(...U.....t...P.P..P(.n.Vl.JA......%3...h.i&3y/.z........}.;.|.<.J.6.fcr:LZ-..+...(...Pp.......,y..= ..D.....V:...Q,....r...5.hI[.a..A.....93.K>.st.........Dq..&....2)..bl.Y.........,_..4Ag..s.(l?A..>..m.M.W..O...C....f.....r.^;<...r...n.....9.....t..<.I.r|.....|1?S.|.....#0..O@.6=}.....q.^..N X.9*.Gh..Q.!i6...A.,..&.5+...o...dod...J.....D'CS:...../...:.....X|..zH....$#}5K..x^.-.-.X>@.'.W .+.~./..z.o_H.~IF.f.o.}[,.eh,=.....W-....Tf?.........t5$~b...Pgq..6..o}9v..'.....KJ.I.| MT.....d..i..7..^.....i2....I..W.X..a.].V...UWf...fd....=.1~K....[.dX...dV..J.....eL....O.....R. .T._.wGr2...W.x. .W.....I....4X....Y~.$.c...v\o_^...S.....O.z..gV.T.............x...{..7..3i.@%... ..IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBZbaoj[1].png	
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:	D0FBCC60FCABCCF01B13735903BEE75C4843688C8208D9B7D51D47AA7B6DC6B00ACDAB83116238F8D5FC9405B96B5DFA7BD66390F8A1D8E4491BAB81D18D1F0
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\3Y2ADQKS\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:	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\3Y2ADQKS\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\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\iab2Data[1].json	
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\3Y2ADQKS\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):	5.4871296565633285
Encrypted:	false
SSDEEP:	6144:z7hkYqP1vG2jnmuynGJ8nKM03VCuPbpXEcJuzYmD:Y1vFjKnGJ8KMGxT6YmD
MD5:	AF670B889B9B543EBEC77183AC70A006
SHA1:	05785425B9FFD0051FA7BA32BA796A75A987B3C7
SHA-256:	E01C5E5D99FFEE14D97AA6CCB277A118244F658DA0ED9CE718CD4391F6242125
SHA-512:	776CC310FF36AE506C766FCDECD4DF676C5B2F18EA9077BE774656FD4AE4C08880FE70ECE44E4D60AB6E11E762AEB8B3A7D83CBAAE1440D08FEA414288B37C5
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\3Y2ADQKS\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):	5.48713787053686
Encrypted:	false
SSDEEP:	6144:z7CkYqP1vG2jnmuynGJ8nKM03VCuPbGXEcJuzYmD:j1vFjKnGJ8KMGxTvYmD
MD5:	957EAAA9298DF60EE861591FA19C218F
SHA1:	A1207DA877214336D58A1974B2F143462B75C41D
SHA-256:	427264BFF78795AFC64316B20F3A4BAEB135AA192043A2DC7D95CC9421150236
SHA-512:	61714C26AD46F375CCA4A5A02AD6428E81F499062F8E8741B7128794D77A995CEE7B761599B02BE7A22BEB971271ADA10F70D1D05346683979B4A677862D63FE
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\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\otCommonStyles[1].css	
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\3Y2ADQKS\otFlat[2].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+PGRpdiByb2xlPSJhbGVydGRpYWxvZyIgYXJpYS1kZXNjcmliZWRieT0ib25ldHJ1c3QtcG9saWN5LXRleHQiPjxkaXYgY2xhc3M9Im90LXNkay1jb250YWluZXIiPjxkaXYgY2xhc3M9Im90LXNkay1yb3ciPjxkaXYgaWQ9Im9uZXRydXN0LWdyb3VwLWNvbnRhaW5lciIgY2xhc3M9Im90LXNkay1laWdodCBvdC1zZGstY29sdW1ucyI+PGRpdiBjbGFzcz0iYmFubmVyX2xvZ28iPjwvZGl2PjxkaXYgaWQ9Im9uZXRydXN0LXBvbGljeSI+PGgzIGlkPSJvbmV0cnVzdC1wb2xpY3ktdGl0bGUiPlRpdGxlPC9oMz48cCBpZD0ib25ldHJ1c3QtcG9saWN5LXRleHQiPnRpdGxlPGEgaHJlZj0iIyI+cG9saWN5PC9hPjwvcD48ZGl2IGNsYXNzPSJvdC1kcGQtY29udGFpbmVyIj48aDMgY2xhc3M9Im90LWRwZC10aXRsZSI+V2UgY29sbGVjdCBkYXRhIGluIG9yZGVyIHRvIHByb3ZpZGU6PC9oMz48ZGl2IGNsYXNzPSJvdC1kcGQtY29udGVudCI+PHAgY2xhc3M9Im90LWRwZC1kZXNjIj5kZXNjcmlwdGlvbjwvcD48L2Rpdj48L2Rpdj48L2Rpdj48L2Rpdj48ZGl2IGlkPSJvbmV0cnVzdC1idXR0b24tZ3JvdXAtcGFyZW50IiBjbGFzcz0ib3Qtc2RrLXRocmVlIG90LXNkay1jb2x1bW5zIj48ZGl2IGlkPSJvbmV0cnVzdC1idXR0b24tZ3JvdXAiPjxidXR0b24

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\otPcCenter[2].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": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUtaW4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImFsZXJ0ZGlhbG9nIj48IS0tIENsb3NlIEJ1dHRvbiAtLT48ZGl2IGNsYXNzPSJvdC1wYy1oZWFkZXIiPjwhLS0gTG9nbyBUYWcgLS0+PGRpdiBjbGFzcz0ib3QtcGMtbG9nbyIgcm9sZT0iaW1nIiBhcmlhLWxhYmVsPSJDb21wYW55IExvZ28iPjwvZGl2PjxidXR0b24gaWQ9ImNsb3NlLXBjLWJ0bi1oYW5kbGVyIiBjbGFzcz0ib3QtY2xvc2UtaWNvbiIgYXJpYS1sYWJlbD0iQ2xvc2UiPjwvYnV0dG9uPjwvZGl2PjwhLS0gQ2xvc2UgQnV0dG9uIC0tPjxkaXYgaWQ9Im90LXBjLWNvbnRlbnQiIGNsYXNzPSJvdC1wYy1zY3JvbGxiYXIiPjxoMiBpZD0ib3QtcGMtdGl0bGUiPllvdXIgUHJpdmFjeTwvaDI+PGRpdiBpZD0ib3QtcGMtZGVzYyI+PC9kaXY+PGJ1dHRvbiBpZD0iYWNjZXB0LXJlY29tbWVuZGVkLWJ0bi1oYW5kbGVyIj5BbGxvdyBhbGw8L2J1dHRvbj48c2VjdGlvbiBjbGFzcz0ib3Qtc2RrLXJvdyBvdC1jYXQtZ3JwIj48aDMgaWQ9Im90LWNhdGVnb3J5LXRpdGxlIj5NYW5hZ2UgQ29va2llIFByZWZlcmVuY2VzPC9oMz48ZGl2IGNsYXNzPSJvdC1wbGktaGRyIj48c3BhbiBjbGFzcz0ib3QtbGktdGl0bGUiPkNvbnNlbnQ8L3NwYW4+IDxzcGFuIGNsYXNzPSJvdC1saS1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\otTCF-ie[1].js	
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\3Y2ADQKS\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\9QTQHWWN\17-361657-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F
Malicious:	false
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.localStorage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c.data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("office")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-dependent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\3b2da2d4-7a38-47c3-b162-f33e769f51f5[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):	57130
Entropy (8bit):	7.972544093187763
Encrypted:	false
SSDEEP:	1536:QJ9TCFUuyDdm0zK2fGLjdI168M/sl784yc0:QJ0iuygvdI168MkJr0
MD5:	96DD9EF9AA1A32C776DCAA965D73693E
SHA1:	AF469E1E176BA11FC764249C220BD5D9A5EC386A
SHA-256:	18F9C8D9EDC05867956862BB066F4C779415A7B20F86BB0A6F4E9DC85E4F94DC
SHA-512:	7A508FB623EC1707BC27B13B983BE20A861A2E75188BFD0EAE4987953582D1F0395B6C249AEFD1B70C94A84766D3AC0122FFB030C2AD969A429D2A032BFED58
Malicious:	false
Preview:	......JFIF.....C.....C.....,.,.."..K.....!.1.."A..Qa.2q..#.B.....R.....$3Cbr%..S..&Tc.....A.....!....1.AQ.."aq.....#2B....b..R.$3.Cr..%cd.....?..r..A4eT8.s.Q\..=.#....zP[.O..D0R..[p.Jl^8.....c4..0....r.{v..=.....k.!.2,)...6.I..9....g[M:d.E...}o...Q.^...HC.Fb....<. <..$...Q..`...n.%..t..4~tp\.YJb.29*..<.V.r2.>...4....#....KK$2)..Wr.\|.O..\|m`9...:.J.Z..0...$.....,.....U..4."#....R.....1.fRd..>....|.g<lKdz.nx%N...pH$~..}...[.qO>.+{.$.....~.~.....$..p.....t.....8..}..KIw....U.n$.StjS$..3.G>.h...@.RW;w..H...*.....A...H...R.`z..G g#?..;wS..."..!;...@\|....q...c...G..N....\|pQWN.O.H...7+}...8.....0$hB....F..H%.#..$.r8.]`.o+..9.m.....Nq..t!...F..'p@.A.o.W..dt.....<d...B.3...y$..'..g..o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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+Jly9XD5hb6Fg9a6: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.....Sl%.WX.q>..8.....Z.V.n.U.....\..... ..7....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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\9QTQHWWN\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\9QTQHWWN\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/WYqU9m8LaBIIJcv1DAKvA4IFE4JN3QNr:IUEz+UbKa8ZQQptpedAWp8LaCHg1DAed
MD5:	F2186DFE6F4836465043A993391B84C5
SHA1:	C595247171C1DD8D73429B0C58773C5E177106C5
SHA-256:	710EFEEA80DBB97B005C47E34341F00ABCD3345A5756EC967A6D1D6D06094B22

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAOdxvW[1].jpg	
SHA-512:	21E86B092676E1EAE42E18C680D176A045E8158CE8386DB7D8624B7D3C70E9A018C1992FCAB22A6FEBF824445BF1850E7E98BFB4AECDA769ADA52356DFCF43D3
Malicious:	false
Preview:	.....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..pn..+1..(...P1.L..s.4..1@.8^2h....2)J...P"0..@.c..g<.!<..)..BW.J.."Xm4..0.....4$..z.C+mL.....*..6.?. <.....4. .Hb(.&8....=..1..*....A4..(.2.....HT...5.p.....{.E.4.p.....L.....{P....+HBc4..8.3I...y.S`d....7.k.U....B.....^(..h...H.m;..c...@..1@...B.@.Bc....p....4.}(..H..:S@.#..4...!...P!)..T.i..M..M...h..a..1.c..n(.....H...<?..1.....!...S.`8.1.J.1..0..h.H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\9QTQHWWN\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\9QTQHWWN\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\9QTQHWWN\AAQVtAu[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	19353
Entropy (8bit):	7.759923173787334
Encrypted:	false
SSDEEP:	384:IWHFoJoL9JdqB+osyLtr3JN5rSwxi55JPZZQDm0tHelvTCn:IWHFsyTdltpTdhivJBZH0t+FS
MD5:	E816AA08895A8364BBBFE53AD815ED4E
SHA1:	17B84C624BA2CDBD33D301A55A91582BDB7AF63D
SHA-256:	F800A4F3965D72E5926E78D37DD60DA9C5B5CC6C4C03C615DE4D6E20C56D1036
SHA-512:	7BCCBE050D366D53B5F6D79F085E666799170B0CA4B143F2125A2563D4A81C6392CB2494DAF1CB416FAB0950FF59879A8FF49996E6F0486FA38BB2F4EC703B05
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\9QTQHWWN\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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..9I....9].Z..g[.(.....4_...ED.C:*..y.G&....v9....k./..np}.V..s4=.....$.:..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\9QTQHWWN\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:	42C0009CC3295F4B9CF46C3D0D2ECFF55DF3B3F701B270AD77BB96DDD39B13C9129994AD4F6C4AE41741B4BBC9BDFBE0BE73047CF0ABFD1DB7D11258F020F5C
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.bi.G2.r.k>t+.W....r..+.V.8.z.Rj....-.*.$?M..$a#eMf.H..)&.(.Vq.=...._}EtD.....-..4Q.....D..y..._.....u.a...Z.....=.4....vY...C.=.M0Q..@.(.....5.BI*.>f.zf.v)+...`...|..fr.....!.r.C..d..#.66.<f.2\K(...3'.ATH..0Fh.RK.[.H...X..{w...c.@.....$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\9QTQHWWN\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAQWZxV[1].jpg	
Encrypted:	false
SSDEEP:	192:QoSUS/VsG2/4T+Gw5jNczWdgNMvaMrs83NlX0dXPj/IqRQmbHOBKewFh+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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO 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\9QTQHWWN\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, 311x333, frames 3
Category:	dropped
Size (bytes):	22049
Entropy (8bit):	7.947759500276846
Encrypted:	false
SSDEEP:	384:NgPTAqVEC7Rr4dL/Wx3LJ9cTIPEW5Nq46cBl123BE7n4VsL/BmaGm00RjJ3sB:Ne/RMdbWxF9cksJ41BUu8GDzGmtRl3o
MD5:	7F0F570ADBA884F69FF642A783D388DA
SHA1:	997F55B58F750C4393C212FDA9579D2A5CD0C19E
SHA-256:	7FCA36CB92AE7D8E7BA3D1F05428CE2C2A12FBD3391543A9FBECB6E9553820F1
SHA-512:	3FDBFF139A0A2F96C24716C1712B6B7B18F7D59F74C37ADAB102B8FDAB19864D6C11DD3E8E0537DB494F882AB1D457B3359609A7D36F1FD7537FAA611D94513
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..}..b.<.Te.....?.....$y.%...jzTj..hL...Q.FT..".[.....-.....<1...@...@.....D.....R%.In....w?g....K]I.we.....4.K.`.....H.}H. .*...@ ,..S@.Jv..'...73n.b.#.i.K.....;H8.1.Rw.....8=sC|..d.3....U.,..Vs.Q.Wts...bj&.. ..."t4....#KK\F.H.g..._.1u"...=A..-ON1....q....o.G...@._,.\x.....q*..V.Z..7EM.Q...9O9.".lu(.'.VC1 \....Kc...f..fK..E-_..B...o..@".....)..1@...4...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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:	8351DAE3BD697AEDDEC0E52858CCDE313B9013530BA80B4AB23D6CCD8B4F766685101F6956189EC5281A6116AF40D9B5B6C0CD2AB00223C4D36D950E52EBF3 1
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...[..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$2 D.*.,...U.]H..M.....5!.....1@..p)..q@..q..Q.....&.4..ER.P>Z.....R.I....E ....@.....h.#.MK.5S..$;.b..'SR.L.eM.p.E...SAq.R.\6R.\UN1.v...qN.q.)X.J...&+..b...;..I..@.v..\]..V...d T.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\9QTQHWWN\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAQXfYg[1].jpg	
SHA-512:	E0CF4117DCB1AC66791CB4858833FF3FC156DC4BF4F19ACF1DFDB08A89D5AB87BBC9DAF4E4B8F563CCEF41F9056DA4BD355A0875AB49BCDFB020599D3EC4 A0E
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....TM..h.....@.....i3..Mj.|.Rf.$..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.H I..'S..@V...H....H%...j.U....*9u..U...]f.#....S(.....}....s.q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAQXfgx[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):	25676
Entropy (8bit):	7.959854408609341
Encrypted:	false
SSDEEP:	768:NQb01Ys+VK07GvLWvCcXQg2NhUGlnManN1ekVWOnI/:NL1Ys+Q07Gviv7Xqv97eKWOI/
MD5:	0EDE139669D625C1BBA5E1ADEF41DA11
SHA1:	21CD4D848F8E376047E7D2383CC21FF848DD0F7A
SHA-256:	6CB1AFFD42AB2196C8DC2411F3BFE5C2D3B26BC2C3BDCA5B8E224E5659B9DBCC
SHA-512:	FC00DD6E41EB758BB483EB31545A322F33DD76EDFA24BDC15FB12248CD568825E1B794F3C3AC76503551E6D6D88C9852CF8365CAE5795C9FAA1CFA28DFC315 DC
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..... .....?.....h.....P.@.....H...b..S.m...@...\P..@.....P..P(.....!.h.B..q@.(..P!B..p..(.....h...J..(.qH.\U.1L...1@.(.....b..P...1H A..1Lb.@.b....]..P.....]...h..h..i.P)...B.@.....pZW.v.p.....W.B.....h...W.....&(.....b..... .1...1H...m.B.....!.h.v.1.h.v...L....P..HB.@.....h...W..i\..E.\R.....)\....\R.....\.-..... ...b....1@.....h..H...C....i.v.`...(Zc

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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:	E3B0FF068E7C903C4D06FDDE07288F4121ACF1A24E59067AB65FCB1C94DF66FE6E5246BDB3098E4EA80B380CFB5ABF38AA6AAF6A0175C94FC3421CA30E4CB BD8
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..|.+.N].S..p...$.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._.*...l1.6.....Tg...$ .....t..`p)$.J..T.....P... .#....#-..i.3Z.!...i.RHdR....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAQXnHc[1].jpg	
Preview:	.....JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\9QTQHWWN\AAzb5EX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	322
Entropy (8bit):	6.966129933463651
Encrypted:	false
SSDEEP:	6:6v/lhPahmKxf8jCAw4DGQJe1kvnxIekdOgcKOtQExGTFDDv4bp:6v/7IxkjyzQEyaI1QmGTlW
MD5:	89E1141C659F2127DD80809F71326697
SHA1:	3262110C91000071FDBB0D33893EC1EC8026ADEC
SHA-256:	98763AAD3E2B7507E7729711ACD2DACCBD56164FE6DDB10410047B212275C279
SHA-512:	1D32DF0DB191F0A3FA152BC47F5F463234224F215A283A26E4EBAF95095A0977ABF5B9D9804FA4DDB276CA8DAE2865789802BB8A18B02B232A9DBB22D5F19E49
Malicious:	false
Preview:	.PNG........IHDR.................a....pHYs.........+.....IDATx..=..@..C.....K..`-(.`...vb.....vV...`g.!D.....!.....7..../Qg.Z...Y........c....t.......c..).....)@.:.....8..t1{P_\.1..3Ao.....A].....5G _.....\5..x5R.....'...VS.....|.`...~.....+....H^..1E^...0.,').....qJ8!..D.!O}.i1..E(....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB7hjL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	462
Entropy (8bit):	7.383043820684393
Encrypted:	false
SSDEEP:	12:6v/7FMgL0KPV1ALxcVgmgMEBXu/+vVIIMhZkdjWu+7cW1T4:kMgoyocsOmIZII+7cW1T4
MD5:	F810C713C84F79DBB3D6E12EDBCD1A32
SHA1:	09B30AB856BFFDB6AABE09072AEF1F6663BA4B86
SHA-256:	6E3B6C6646587CC2338801B3E3512F0C293DFF2F9540181A02C6A5C3FE1525A2
SHA-512:	236A88BD05EAF210F0B61F2684C08651529C47AA7DCBCD3575B067BEDCA1FBEE72E260441B4EAD45ABE32354167F98521601EA21DDF014FF09113EC4C0D9D78
Malicious:	false
Preview:	.PNG........IHDR.................a....pHYs.........+.....IDATx...N.P...C.l...)...Mcb*qaC/..]..7..l...x.Z.....w....._....<....|.........."FX.3.v.A.............1..Rt...}.....;....BT.....(X.....(....4...-...f ....0.8...|A.:P%.P..if.t..P..T.6..)s..H..~.C..(.7.s>....~...h..bz...Z.....D4Vm.T...2.5.U.P....q.6..1t~.ZU....7.i...".b.i.~...G.A!..&..+S.(<(...y._w..q.....Q.l..1...Tz...Q...r.............g...+.o.]. ..J...$.8:.F..I.....XT..k.v....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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\9QTQHWWN\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\a5ea21[1].ico	
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.@lA.,>\.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\9QTQHWWN\cfdbd9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
Preview:	.PNG.....IHDR.....U....sBIT....|.d.....pHYs.....~.....tEXtSoftware.Adobe Fireworks CS6.....tEXtCreation Time.07/21/16.~y....<IDATH..;k.Q....;.;..&..#...4..2... ..V,...X..~.{..|.Cj.....B$.%.nb....c1...w.YV....=g.....!..&.$.mI...I.$M.F3.}W,e.%..x.,..c..0.*V....W.=0.uv.X...C....3`....s.....c.....2]E0.....M...^i...[..]5.&...g.z5]H....gf....I... .u....:uy.8"....5...0.....z.....o.t...G.."....3.H....Y....3..G....v..T....a.&K.....,T.\.[..E.....?.....D.....M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P.....9.....yI.<...9... ..R.e.!`..-@.....+.a..*x..0.....Y.m.1..N.I...V.'..;.V..a.3.U....,.1c.-.J<..q.m-1...d.A..d.`.4.k..i.....SL.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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\9QTQHWWN\checksync[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):	21717
Entropy (8bit):	5.305602492520896
Encrypted:	false
SSDEEP:	384:fuAGcVXlblcqnzleZSweg2f5ng+7naMnpuZOrQWwY4RXrqt:A86qhbS2RJpusrQWwY4RXrqt
MD5:	677C48207F5A13E6D6DADF30D2D6C52B
SHA1:	10BCE9871F228CA247E92B0A6366D5FE2A4426C8
SHA-256:	16872C9C9305146F1665B47C30EAF0AF695450B80E6B659781C71E3B45526027
SHA-512:	7C35E7BE4917DEF18676DCD367EA060F9073A093D9B66D6104784845E8B3AA3C14846F617661384E9A4F07E9FE149156A0C54DBF1030CBB4ED972CAF5F115CF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\checksync[4].htm	
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\9QTQHWWN\otSDKStub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19145
Entropy (8bit):	5.333194115540307
Encrypted:	false
SSDEEP:	384:7RoViYMusfTaiBMFHRy0I2VMwG4JRuIKBf:7aViMsffBMnktf
MD5:	0D2A3807FB77D862C97924D018C7B04C
SHA1:	9D17F3621001D08F7B98395AC571FC5F6CDA7FEF
SHA-256:	75DE71E7FEAC92082AF2F49B7079C0B587B16A5E2BB4DABDA7E7EB66327402FB
SHA-512:	409ABCD5E970CAFF9F489D3E7F3D9464B2C5189118D2D046CA99E42CEC630C2C65B30397B8A87C3860E3426CF9F7E0A5F86511539CA9D9AEDA26C74CA90559
Malicious:	false
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,A,b,y,v,C,I,w,S,L,T,R,B,D,P,_,E,G,U,O,k,F,V,N,x,j,H,M,K,z,q,W,J,Y,Q,X,Z,$,ee=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknown",o[o.BannerCloseButton=1]="BannerCloseButton",o[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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:	9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929ED
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\G62TDH9B\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:	204D9F37932441E64BF8E19AEE91EFFB8077C1CC4EF95A0F28B83254073EFFEF218DCCD4F032412257F3E9AE1764E41495CB96BFA620AF348E39AF54A3B47FEE
Malicious:	false
Preview:	......JFIF.....`.`..... ..... .'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..e.[yv..W.t....%...i...TXlL..Ph-.F.Vm.....v#...b..%....M.. .J...[.....q.iB.3.....i.D.....r....'&e.b....ztS..D....u.g(.Z...Y..5.).I.F...OZ..L.b..}.....)..#...9.t.)B...l.\'.....J.....I..-,IA..NMjf.#....Y4.....7<..Wm'.....R..f..tk,.AZ{K.....Ukjf.....J.a>e..a..t..!0G.i.`....s.h..HA@.v)...0....4^.!..[.}..yS].kX.>ddA..G".e..].Ww1J.l'..s.)."..~..]Y>...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAPf39f[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):	21120
Entropy (8bit):	7.657084465552846
Encrypted:	false
SSDEEP:	384:lkoXrGGh1zUezyvAKAAIpqOzmY20Yi0kfBtpookcOk:Idbjh1tPFwY2YfBtRvOk
MD5:	CC5B6CF2CB727C318006F2BCD1CF1F99
SHA1:	C453B022FEE212111E60C3EF7A81BB31B3F80DE1
SHA-256:	DFB4510B79EB2FFAA39962D9EFB59EA31C4184FD17DAD6E7F3FA9E9AA1D18282
SHA-512:	9D15447F3C18EF2F45E7F2F536A26C0AAC1B1AAE077D887A08C0F76036FC8D3F446CBD2B99203A7ABD5F461D2036EF523669563444A3BAD82CD378F77ADFEAF28
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..k....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....i7d4.F99...$.4.lpAA7.....AA@....JCDjv6;.qveI].V..@....P.@....P.@....P.@....P.@....P.@....P.@....P.@....P.@....P.@....2...4R.c....<.f.....;..@%=.8...*.o.R.d84>...A@....P.@....P.@....P.@....P.R. Vs}.a..).-.%R2c.(...4.a4..4.Bh...).!.['tc%f:.!@....P.@....P.@....P.@....P.@....P.@....P.@....P.@....P.@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAQUJZI[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):	7740
Entropy (8bit):	7.867130092982425
Encrypted:	false
SSDEEP:	192:QnJL+PfG/LdRLMU7dXdk4M7nVN5TCqKK84AUt2izEaie:0ZwUdR7ZFM7nJC48le2SEk
MD5:	274A0211B41581B887A9FF0CCA73056E
SHA1:	5F918E12FB3B45A3866613181F001A2F580001F9
SHA-256:	B95146E9728AF0BAAB9A93116CA3F3C8555AA9806EF3D602E827753C597652DC
SHA-512:	9E913EF8527F0C71210D3878A5587A3404BFB8BC1E0EBECA731123160F0071F781EDEEDA1BD762C14037178779B769998F4E8B3D81BA0FFB5A7F2F76929B76A6
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....@...!r}h..>.....x.....\|.....".c....I.....o.....:.]...@....h.....1..qBI..z.J.bo...F.?.@...P..I..C..:.J.=....{.... .....6O.._:O.._:O..<.?.@.....5...@..'...|.?.h..y..h.....C@..%.....3..C@.....7S..C@.....:.....3@..@..@....h..8..T<P.....B...Ph..3\N..y..Tw...i...TY.Wid.%CmA.4(.Y"Q&...[Aa..;^FQ...Ud.e./ .ty3$...a..x?.J..Z..k.....Wn.R.h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAQUhxV[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):	3440
Entropy (8bit):	7.8771377943394105
Encrypted:	false
SSDEEP:	96:Qf7EpeefVR/HLcAAdyL9Vk6zLsb/xEQVNCAwC:Qjoz7/4YBVpLk/6i
MD5:	D26619CF3169E821297EE102E7D96B1B
SHA1:	BD465B42A72D9246C8705497C29E94C3F47D54CB
SHA-256:	D6245338DFC32E90EC7EE3CB9FF46E9D41714C7810CEEB4A405D1EA35B3FF023
SHA-512:	25FA3524B1D29092752AEC16F5B00522C818D5B5AE8E40C8CB9D38373702ECB87BD1403A441C6787216D824DD37DAD255D7EDC0B833BC000F7FF9A0A97B2BFB
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..L.....".28A.8....z.....H9^..5].r.<.@...ps..m.>..K.|.....|.U...s..>.V...:.#wQ..p3.y.Z...q".M.Y..\...9.i/1.b..h.....9..7]J.-..a-.L.S+3.....S.%.....7....d..zpG.@..wv.m=.....~p.....p...x..i....g....t._..F..../.....l&%^f....\.F..;...3.....zdR..L..^/9.F9.*..Q.^.*6.....Ae.m2.....}...U.5..Os*.....zNWEZ.n....b.|..y.._.)o. .....^X8b8=....O[..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAQVisl[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):	14964
Entropy (8bit):	7.941983454156354

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAQVisl[1].jpg</th></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:+zdmhu5Qh+5MHuHNAVl4/OhDfl2JfVTQKyNm1:+zohiFwyc4/sD1VD1</td></tr>
<tr><td>MD5:</td><td>2BE803200F26BFCA3AB0E566192076F5</td></tr>
<tr><td>SHA1:</td><td>6F53E2EAEBD6BB251AD7EA4F09911F4527D19C76</td></tr>
<tr><td>SHA-256:</td><td>2E02E936341BE9CE0FAD85856F56718098B617A2AB227F736A3E969A891978AC</td></tr>
<tr><td>SHA-512:</td><td>76CB524F8750828B20D10152D064E45E7A1B1497BB9D28DAD31E68B5466C7D549D75C0C970EC906F9C481F8E2B8A57EC5F2E3FD9473768256FE8BEA67376FC1</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO.......,..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..v......(..Z.5*..O".*..S.V6py.......J|..>.......*...%..f*y.+.Op.i./'9.p.4a.J...)61w...(.&K....hA.......2.....B.....";>.Zi.&}....S,..........gS`<br>..].~.9..Vf.9...=...'?.9.CC^Q......f......>....F..W.M.......v...s..'..U.d.,..@}.K.........u.)%.qH....#.C...<A.>.+.......S...Y.7LM6.9`xeo...c..\].o....]...#.EE......x.K.\..ra_...s:..R..9..OQ.b...-
..U@fuP.!.i0$..@,..[-.e[..........5.,.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAQW0Fs[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>2196</td></tr>
<tr><td>Entropy (8bit):</td><td>7.799560401503644</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>48:QfAuETAQgh/boT8B8nC/6gVTzeIA8phYvzJrikCr9KJKqm5sLQ:Qf7E2h/MTRC/6mPCZCBKJjOMQ</td></tr>
<tr><td>MD5:</td><td>43B1E133700A65EF28BA0599062D2704</td></tr>
<tr><td>SHA1:</td><td>B853984965EE3ACB0924580E8A706AA971A8A5EC</td></tr>
<tr><td>SHA-256:</td><td>E90243483DCB75142ED2D6CA34804B2F005416AD471F456FC3DF88B2E69083C5</td></tr>
<tr><td>SHA-512:</td><td>A78E4743CAE5DA55EB88B19D59363AAF4DAB05E9A210C26D9FAB550276EB86B448F63385486D2A272FAF27F366ED9A78E41B175C69167020E89958645788D193</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......K.d..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..d`....2..F..i..M....H.Fr..,&.nL.\{.L.P..$M..2~.X..u..3.ml1.).b..^.....fU.-.P...".Q.?1.ERFnE.....;E..9%?...:h.K/.....5B"..........bu.<br>..O....+.RI.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.&</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAQX4Y6[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>11545</td></tr>
<tr><td>Entropy (8bit):</td><td>7.834731011869194</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:Q2oVv2S9MP6iXJdxLEYaz5LHR1nXj1q5t3bbXBDW5vu0/bX0foFvCI4:NoVv24WjxIY4HnXj1MZRdOX0Q9C/</td></tr>
<tr><td>MD5:</td><td>CFABB2D22F889DC7DDB35C01B116107A</td></tr>
<tr><td>SHA1:</td><td>8371C17F1F6F35488A3618E17EEF94CAE5963584</td></tr>
<tr><td>SHA-256:</td><td>EDAD410223A8911F6F7AA702945AB856A10D930E00011D5E14CCAC7E049A25F9</td></tr>
<tr><td>SHA-512:</td><td>CEF30993C812935C49AE3EEF0303BEFD9EDF23F4256B7ED249BA534D3CDCB81DEAAC69DBA7B86E7BB019C404BE15EF86DA471AC54B2918AA88AE4EDF2B35
90D7</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......M.7..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..k..86...iQb....B ..Nyj.p..CQ.......wb.K.<..[.q......Qpr.......&..2..=.z.T....5..>.....R.P.?k>.>.......as..K.<..Q...9.....a.X...#.\..
.H.p..Q...yw&.P'..1.9P{...#.....M.8c.X5.Z...R...6.O-....KF#.F.b%.:..e.H\...a#..=....T....(...>...\9E]2..>c.h.RO..n~Ja..O..|.......#..i.*..V. F(.T/. ...c...B.....(.!E.\.......y..@Y.....:P; 4.;
G.@..*.a.~T ..g.....Np?*.C.<P...^......3..</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAQXaYx[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 310x166, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>6913</td></tr>
<tr><td>Entropy (8bit):</td><td>7.804453728675494</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:QfPEiEv/BqVcbl9wDRr41m0n47ROQIIPPm4bEq7BT9UoEukvmt/rYd0f/cZ:QnxE3BQd9rIm0gIIGYLBT9fkut/rY2cZ</td></tr>
<tr><td>MD5:</td><td>B01320ECD9A78047BFBD22F65074EAA0</td></tr>
<tr><td>SHA1:</td><td>FBF809124993916E529E838F25DFD6D293BEDDFF</td></tr>
<tr><td>SHA-256:</td><td>64D7F79A978C30CC66893C4434BC523388C7A9DF089E795C8549D5F04F36FDE6</td></tr>
<tr><td>SHA-512:</td><td>F2B324B3FF8909CF5D0B43A654E9C7CDEBA546A477610534A61165CF93F7365D430223DF8B6CA578A3003F4B01ECF7CE50C983C78CCE0D269CA9C0E3176657F</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAQXaYx[1].jpg	
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..:`-.....!o.h.(.....(.....).P.f..i....4...f..@.;R....`...%.....N...78a....Z...4..@.@.....n.....k...v.....Fl+..xb.....i...(.....4.f..`.....f..f.....%0..(..... ..2(..../.(...2.....J.(.(..h...F$iX...#...?.v.....X<..t'...._...._p.....4.f...3@.h.....L..(...&h...%.....E.O@....@....b..(...&(..H;..q.@.`.Q.zP.@.@.@.H...@.....#$..w?JM...).Gh.4.....+..<...8K.].^..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!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\G62TDH9B\AAQXevg[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	12126
Entropy (8bit):	7.945197487897491
Encrypted:	false
SSDEEP:	192:QojRJN0D37cpItLy/vhNWN0jOv7QaeDPhM+xbBiKLZHx7bYfKdohw45mxNVv7M6n:bjRJNAjyJEvEj58KNR7whwMmxDMaYU
MD5:	549D7502E6B50302E7B7451DABF61781
SHA1:	87949284AB340C839F895F33BCD7ABE6ED992637
SHA-256:	904790AB667AD93D7F07BE7B90FD02EC0CF09F9194A78C0F52DBFC704FC49C7D
SHA-512:	E68451666915C21C9C8B254B1292D8702F7813D3496251998A7AC2EB5F0403E05A316221EC14F82E2A7A15CF2C58BC26CF94A942DC99B29498237F5291B1107B
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....`W.....Y."O.2@zR...Jv.f}.`..u.P...z...k.F.....}./.vS..ZKc..G@F..R2.|.)...8.....@."......2.6r>...=2hn._..l%g..0..r.C...f=....`..{V.L.Q$7..F.....0t.n.n.Bm.<G../Jw.*E(5'f!.q..P....2..hr$...D.r..N.c{ !r..2....#..i...4.yA.R.. O\P.@..@..7.+....1....C...l .A..bP...+jQ.>.....c..9...Fh..u../b....+..r'..D..x.(.l~\.LE..@.E.....L"G.m<..Ke$A.....>..[*.7.Wl#..y=..C-...M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAQXf3x[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):	15421
Entropy (8bit):	7.938798835151617
Encrypted:	false
SSDEEP:	384:NNQYoyZatW3tUuKEqY5GDZBEK0aflClgebIdApdd:NNQYPlQY5GDrE7Eag0IdApj
MD5:	AA8EC32FFDEC3C9E845264897B2C563B
SHA1:	31CABEECBFE771AF7583891F81B4E51C1FC7987B
SHA-256:	35EF5EB79DAD38112E7E7FDF50E2E2F063092974C4B42CA35355F0DF01BFB3ED
SHA-512:	18832CFA4700F1669204501A774ACD732331C31003892931D380D4108DA562EE6594B207FC807A63D793D99F262816FB233C5FE33EB5DABAED7EAFC4FE2BB766
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAQXf3x[1].jpg	
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..dh0....z....@...H.....!jC.:..2.Bc.&(.E...*]...e.2}.P....+n.B-..D..NzC*...H..S..f..A.H.b.....R1.S@,..1o..jX.../&.-.....+DK4..D..."...5%...x.2..8.L.!.&..i....3. ,'J.K...@.#....).1..b..(.OJ..s.M&Q./.5..:....lj..o<U.F..N~E!.q.H..S..P"ATH.LB1.4W..RQ,T..}..#.....e#....e!l.....D.N..Z.pt.IZ.(..9.c7.$...m@.JC%.(.. ...:U".50D-HcGZC$Z.IT!h.P.zP.{..H..a..2.....n..sT....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!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\G62TDH9B\AAQXmH5[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):	8812
Entropy (8bit):	7.785286756347677
Encrypted:	false
SSDEEP:	192:QthUlXi/hR29b3Uk69XXhOK6MJKJK6asmgMua2m7pi/UL9qE4/TP/:+hdhcj6nhXu1Mn7oUL9C/b/
MD5:	636EE718D1D2A584B802B7B2FF118A8C
SHA1:	EBFB0494723731690DCD6ADEAF8C46F6A703A7E7
SHA-256:	9F49793042FEFF2190C920E2648838C78FB4C84841F1D38497213F58033BE011
SHA-512:	AF70F5C92B9AD59F0221E9F6B5896D3A9D7708FEB833839AF8339CB24764A853A545E344C89932D15FBA70895B0849C34D89867E017454B6D45B07A45842F77A
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...]@8-.(Z.P...h.....m.....@...]...(..@...6....e....6P.....l..e.&..6.....m..h.6..6..m...@...B(....b.....- .-...@...(....@....(...a..\P... .).b..S.q@. ..(...Ha@.....`%...J.....@..%.%.4....L....Q@.(.h.E./z.Q@.@...Z.(...(..!.....A@....!3L.4....4....4.3L...&h....&..4....&....nh.....(a@....5.(j.]..n..n...@...]....@...\...0.u.. h..@.\....0..82(?Z..<7.S.s@.h...A..L...@...3@...Bh.3@.h.(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\G62TDH9B\AAQXqrn[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):	31173
Entropy (8bit):	7.932533282363292
Encrypted:	false
SSDEEP:	768:IVoG6/tet+zsLEx/cYs5sq2bKU+zdNvgVB/X:IVp6/tesaEdbsOq2bKUmdOVZ
MD5:	3B0190D7BA95CFE173567A1A35347439
SHA1:	27D8E7272A958939F4B97A61163B70677C2B188E
SHA-256:	FC37F8281C32BFC0C9CB8D388717F6E99624CE66436CDAAD97FDCA65D3D15AE7
SHA-512:	6EB821D20CED51C73BB99ED3714E2A58D80A5C4D74ED351813BD4EAE661BAE200AE40946B2ADE11622A44D05B57FB35E01469E82904D66BE732E41D761AA71B
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.....?....(.....(.h.h.....(.....5.[.....>I.....@....{E.6V.{.....f...I.5.Y%?;g..3..1@.<....i.....N..w.....s.}.;..)v...i..x.Wr..=.Ji..77.a).e<qT.On...K.....<.T{P"KMRG!$9..J..W4.....+..XLsH.....M..m.5&....."...K....m.....s....HZ.@.....T.....SOa.s#..u*.pA."....(.q@...1@.@.....(.h.h....&..%.F....g.zP.....K.....Q....T.Gq.i..P.....#,O.....Y.w..H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB7hg4[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	470
Entropy (8bit):	7.360134959630715
Encrypted:	false
SSDEEP:	12:6v/7TIG/Kupc9GcBphmZgPEHfMwY7yWQtygnntrNKKBBN:3KKEc9GcXhmZwM9LtyGJKKBBN
MD5:	B6EA6C62BAEBF35525A53599C0D6F151
SHA1:	4FFEFB243AAEC286D37B855FBE33C790795B1896
SHA-256:	71CC7A3782241824ACDC2D6759E455399957E3C7C9433A1712C3947E2890A4D4
SHA-512:	0E4E87A66CF6E01750BC34D2D1EC5B63494A7F5C4B831935DD00E1D825CDB1CFD3C3E90F29D1D4076E7F24C9C287E59BE23627D748DB05FB433A3A535F1154
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..QKN.A....(..1a.....p...o..T...../.....$..n\...V.C .b2.....qe'.T.1.1h8./.....$:Y6...w}_>...P.o$.n....X,<...R..y....$p.P..c.\.7..f...H.vm...I.....b..K..3.....R..u...Z'.?..$.B...l.r....H.1....MN).c.K1H.....t...9.....d.$.....:..8..8@t._...1.".@C....i&Z.'...A1...!....R....}.w.E4.|_..N.....b...(.^.vH.....j.....s...h. ..9.p!.....gT.=B.|..,=v.....G..c.5.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C13
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....P..?E....U..E..|.....|...M.XD.`4YD...{.\6....s..0.;....?..&.../. .....$.|Y....UU)gj...]..;x..(.."..$l.(.\.E.....4....y.....c...m.m.P...Fc...e.0.TUE....V.5..8..4..i.8.}.C0M.Y..w^G..t.e.l..0.h.6.|.Q...Q..i~.|...._...'..Q..."....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\checksync[2].htm	
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\G62TDH9B\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\G62TDH9B\otBannerSdk[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	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\OTUW0Q90\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:	43CF44624EF76F5B83DE10A2FB1C27608A290BC21BF023A1BFDB77B2EBB4964805C8683F82815045668A3ECCF2F16A4D7948C1C5AC526AC71760F50C82AADE2B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\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\OTUW0Q90\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\OTUW0Q90\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:	A6834B4CA196B46432AA31C5A5F0EC16E41852C2A2D7D09C3374CC942795DC4A0A958C7DC72DA6FFFB6A437462AF67C75FC01FFABFC9565A7EACB0C9F9DE2B3
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...]....4K.T.bcpM....*S.&.j.P....(..h.v...P....c..;.P!....!v...P!Yp(Bd{y. .@.m10.@.m.&.....p.0...\P0....CB.(....C..c.Hc....@.(.).Hc....I...H..)..).x...).....I..R.@...@...\P.....@...p.Lx...b.(@8S....@..-.(.A@.....Z.(.....@..F.5H.4.E11.(..h.Qi.1.i.pJ.v...h.6.1B..pC@..s@...0%T.....S.....LM..LP ...(.@...@.P1v.).....P.....HhxZ.....).....$..C.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAQQSrK[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):	11692
Entropy (8bit):	7.94273146239602
Encrypted:	false
SSDEEP:	192:QoIjrMQW4oH2FsVg+A0nZJNQeO7QD6jzBWVvEvosc/p43G7pVBkVUmLm07ksmWmB:bIjrMQfo0oxA0ZweOUpvsOy2/qVUmLml
MD5:	20D4519FB505B36BE4DE67E3263C1413
SHA1:	A73956576096046A20F059FE6A4C2AB07BD3E27D
SHA-256:	43EB91494B152806DF501FFE317ACFEC63B085CA16FBC379B0EE49023581CD77
SHA-512:	AC69E84B8C6B86C7866BB7FCA01ED9EA0B67352682AB2FD6A6DD8707120CAE4263E284731DAE0F76785B5211C4E48B324ECB9BE75AA0294B2F0A9FF8C67958F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAQQSrK[1].jpg	

Preview:

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO...}.......!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..:..\s....z`P...#4...8....z..s.@.x..'8.@.....>......e.Q.j?vH......{..z.7=M ......$....Jb.08....r..<.....;+....$..R.p...f.omBV.....Px>
.D.1=z..a<.@.>.....=.....].u"...f.....C..=..A+...1...{....R.......=. .@.O"..;........vT....d.O.SM.b.-n\....e....!..JHl...)..9`;u..B.Q.....Q.....r..#..D..&...E.4....3........2.....o.......8..I...'....N?:.`......
@.x. ...K.P.3.i..Wu.HV..a{.5.k

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\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:	EC89E47D9C49DB7B5E8E5388A29C5F1C5424C0293DC972D9878A332C58A0174F083BACAC07574A761844E5CD6A2E33BF4648B92DB7494129DDA4CC11FEBDA/ C8
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?...M*.(.!..V`.>o..;.[a.B.....F...$.....Us.ME..J.lV.h.,..........(.n....cz."..A(...yu.....c.FJu.U.....Q......d....ws...8....&s..Oj.?~...m,R..I/.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\OTUW0Q90\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, 311x333, frames 3
Category:	dropped
Size (bytes):	11822
Entropy (8bit):	7.8289572737659165
Encrypted:	false
SSDEEP:	192:Q2X49PzpHHPI+EfUJt4d2RssaboN5VRbxYi7wJmGok4qc1/CYtK2ebMPJ:NX4RFPI9dqZlq+wJuIesRAh
MD5:	635D2E812B29FE98B0D2159D0ABE2453
SHA1:	963026C35E7C7FFFB0F0C052F2E91BF6F15DA195
SHA-256:	5243A76E4EAF7EF8A5D4C72FDD3BA4E48FC7875B986BCE757C146C24FF6C4E72
SHA-512:	FC6CE7BD1169FBEA0AF45E03AE564AAFDEC51DA7914BE7FA9CC8104E841ECFE9A08340D1A978FAC6D783A4CB41EA66B1248157215D143E279A1C6E8809D0F CE3
Malicious:	false

Preview:

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..z.J.3@......@.@....@.(.h`6..P........(.q@..&h.s@.(.E.;4..0...\....J......J.r.... .@...C....L..@...J..J.....@.y.....Z@4............(..
.@.4....b...(..@.=)......&h....@.4.P....@&h.A.....`.(.....P.@.....J.Q@.@.J.i.@..:..@.@.....<P.P..I...S@.F;..@......^.........<.@5....P.(.A@.<P..@....1@.@...........C@...\....Z.(...
..........o4.$q.....8.u4.....+.. ..d;~.......h..t.N>.b&..E.].~..d.....m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\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:	E8E1C93F9114DFF133A8CCA08D8FA10870E7550193377C4A069EBF625B4803FBA6121563B5470FDA5498BF3E96ECD52C02354D2B1002CD0F3D115261EA1ABF7I
Malicious:	false

Preview:

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..W...V..,~.y.Wh..B*..#l.&N.z..G9..Km.m(......K..f..@j..2.&.b..4...h.0h..../../jk....v..G...7......e.kBO.3.S....d|..R1.q@.4..@..3`.89...
[...a.k".M.,.j.M.H...\.W)Dd..9S.hLM.....)...%fF.#4.....'h............L.14.....H...q..q.Y..&...Z..^G..9<S...+.._7#...NBE5..H\`.T.B..XP...{.\j.."....B(........[.t...].e..R1J.@.....@.@?z.Z...d
'.B(9.@....`......6MWAu)H..vg5.d0&.0p...V$.H.p......d.a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\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, 311x333, frames 3
Category:	dropped
Size (bytes):	11524
Entropy (8bit):	7.853199656109683
Encrypted:	false
SSDEEP:	192:Q255QcmmWT3NeMr8Su3KTBwYP5HTHnSyRzaHbxzdFlyUi2JmJwRd2bxUdgRhCyq:N55QWWxFoXPYFH3ROBpyUiAuYdixUgR+
MD5:	184A58668CF5B11BACAA18CA15D4B08D
SHA1:	F5F9515D2792A83933D3A781A0282791005D3A90
SHA-256:	5C71A4888CFD8F6E5A2422852B21D7E3BBEEDDEF6656C9B7FCFBAA7DAE35C3BF
SHA-512:	33CC28FA94C100216D061D01E4379AD5E60C05CA99E3E4A9AC4788831E96A4EBC84792D1096180A4C9C60A54E5514E801F6796FF63441B239930E9C5D3834CEE
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....a.$}._.....5>.....L...(...4.P.@....P.@....P.@....."....Qq.M...y..`..b.....f....a.u.....n..0Xi.Z9.a...Q...nOj...M.Qp.^.w.<.....T.a.3... ...L.O$.....4...jw..Op.g.....4.....y...T.ba!4..BE1..}(..o. ....p....;._.{Qp..n}..X>..K.,.i...V...S.c...4...>..K.9C.^.....I.G0r.D...a.q.FlZv...5...+..t5.,....;.2.. ..C.h.7.S@....w..!j.7P....>..M.... 4....@..yk.a@.W.....E..E.....`...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\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:	37AAEA107ABDEF120CD2C6230B7EA207A3FD7EC109006EDC8ACA0B5580E062E67DA22EC8B5F413F319B743BF1A967AA66FD5A76E3D9E077CE407B052D5D8E E7C
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....R1. #..0..I..R.....LA@.m....'e.zPH..?.....c..4...#&.g.i..a.(.E.|.....@.)..Z.<{...h...X..J,.I....`.....=(...1.@.....u."....s.0$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\OTUW0Q90\AAQXgGS[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):	7672
Entropy (8bit):	7.899724287113537
Encrypted:	false
SSDEEP:	192:QoHqdeF0SalNmFwy9VM0IbyMp7GTFbXcF3zH:bHdF0SeNny9KWM1G5bgDH
MD5:	BBB780E441A64C9C3E02355A7E40B10F
SHA1:	994374DF769B6C987EED7D8A66CE2871F29B064E
SHA-256:	869D76A392E2C5496B20C1B256CFC23E26FC0F6B58B0025BC98ABD86DF29040F
SHA-512:	ED2CE8A2A2BE163EBDA4A745901AB8F695DB0391FA4DE1FA7710914BAE676DFAB66D710863B5D14507927FCA720B6787F6315F199ADD122BFFA77C0E01336D9 2
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.../)9.Y.P.$.`,x-....M.,.....,F".Vi~y9.....@.4..3...(.....`.%..K(i9.....;..j....I.....L(?^I.r.ZE.o.Z3..0.YT.R)k.z..4.[.C.....^J.U...Q T..n.L.V...-...Q&L...&.....k.-.....h..O.Cw.m.. .....7.. _..hH....=.i.t...P[..`9c.v.S.~..Xc..fG!@.l..l.:...j..K.....}..Jqw%.....x,...z._...AhZ.o#.O)...p.?.....1 ..*...H2.T.t' .....K.....E..S9TdRW.F.e;.e.)T..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAQXqYx[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):	33189
Entropy (8bit):	7.9490548374961

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAQXqYx[1].jpg	
Encrypted:	false
SSDEEP:	768:IBeUnZEbQqvWzovQqABKM2KC0ODo7QZjZs9QsHPH6q3gmDNyzqBHj:IBTnWbbOzovQXKZKBOD6RPGm5
MD5:	24B9CB95258C67508D049AD4C96763A7
SHA1:	1545F2FDEF85CECF7C4415A167D8EE0343B770D3
SHA-256:	49C4D4C97D5F9B910C5E60B7532B3C1C7F867D3AE39C2A2C9C99ABA85CF5C34B
SHA-512:	3071ECFEDB1E35D49AAD1174C3B13DC1EBB4DBFD38EB1B3165624A47F9ABC850976D2BF5F71631F0C44F2108DCE5FEA99D210CBAFAA6677F9C4A1C2CA885D66A
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.....?.....@.b<S.-.....R....R.!:8.*.,.&.....66D.Z...k.A.....*..=2.b.U.....3..(@y.j.Wz..H...`u.....F.m.....26.....a2:..-".N_\+u*....0...R..<..oZHsf.z.7....+.../.@;...`/...p@'..)..q.D7..r>.....|.....a.%.{.}.S.r.AK+P.{.....)..B.:t.h.n.O5.D\Y.....F...).y..z..Cs.*..T...d.1.@u~...(.Cb..>..FA.}+.6.0{.w....6....5...ko,.:....w4H..~\7..F...C[..6K.5.fm.c.<..#.....K0....5.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAycUpK[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):	279
Entropy (8bit):	6.585816958592039
Encrypted:	false
SSDEEP:	6:6v/lhPahm1TutaSP91hccpL3fHL5FlzNua5GVp:6v/7XSxFQcZ3f9rUa07
MD5:	D63AE2349294868B3EC2658627995955
SHA1:	E96A4ECB7E48AAC4355BDC28F12DA4C334AD2E20
SHA-256:	12D743416FD1041E0D34C45732DD577A39CD218B65E3F39BF43F2277EE7E6553
SHA-512:	4885F0BA41A6B9E0B14F588B6451C83B08ED2094247EE2160EAD9FB79D9A6474B7EF4DFFCA468845BD9DB27A66231833A9F94E62961975C55B12F3ACB9399C1A
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.c....?.....`...k.?3.]..W..w..g..b.z.(..^...d...BQ..8.....?..(..lo.....E.....|.,. .\....gb.=..Ze0..A.....s...`M....ZW|.`@1..J..x.(.:...|....y...XH,..*....&-.a...8.B.8..A.....S.Mn.....d30Y.Uw....IEND.B`.

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.138662325535767
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:	WTXuYxax6d.dll
File size:	125952
MD5:	cbe2a109ef92af54de51a534980151a7
SHA1:	e71ab85a35df851229f87fde059ad35ed167bdbc
SHA256:	450a436cf830b03533a2ce0d8d40724d61c8b0e5f8164413c05d2c870b4ba8eb
SHA512:	c30e3d42ed63a1327088111cc7ad3baa11149d5a9c9b7778a7561bc67a38c07be01978654128f29486c595441cc13a82ceaf6026ec9b04bbf5e2f1fd01c06020
SSDEEP:	3072:FSGsYBXQAs5JLGk+9wDTXSH1/FKBl0C7p+1mwu/:FELKkOh4B2Cd+Tu/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100071f1
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:	0x619A563C [Sun Nov 21 14:22:52 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	4c89e39b5ebc619c69b957c6b4f65780

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xfdd8	0xfe00	False	0.686069758858	data	7.13842205011	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x11000	0x95e6	0x9600	False	0.670651041667	data	6.50007500448	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1b000	0x6994	0x4200	False	0.885002367424	data	7.5794714709	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0xf8	0x200	False	0.3359375	data	2.51977440023	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x23000	0xe68	0x1000	False	0.716064453125	data	6.24269223414	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 23, 2021 10:51:36.761096954 CET	192.168.2.6	8.8.8.8	0x2273	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:51:42.627621889 CET	192.168.2.6	8.8.8.8	0xb094	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:51:43.641735077 CET	192.168.2.6	8.8.8.8	0xd93a	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Nov 23, 2021 10:51:49.603517056 CET	192.168.2.6	8.8.8.8	0xcbe0	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Nov 23, 2021 10:51:50.182585955 CET	192.168.2.6	8.8.8.8	0x5b22	Standard query (0)	assets.msn.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:51:53.210439920 CET	192.168.2.6	8.8.8.8	0x37cf	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Nov 23, 2021 10:51:59.316274881 CET	192.168.2.6	8.8.8.8	0xc8e4	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Nov 23, 2021 10:52:20.899028063 CET	192.168.2.6	8.8.8.8	0xf03b	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:43.953464985 CET	192.168.2.6	8.8.8.8	0xfcde	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:44.298163891 CET	192.168.2.6	8.8.8.8	0x8bb6	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:47.325711966 CET	192.168.2.6	8.8.8.8	0xa6c6	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:54.386729002 CET	192.168.2.6	8.8.8.8	0xf1c2	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:54.933254004 CET	192.168.2.6	8.8.8.8	0x76e0	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:57.756691933 CET	192.168.2.6	8.8.8.8	0xd7f5	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:04.584307909 CET	192.168.2.6	8.8.8.8	0xd5e9	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:05.181210041 CET	192.168.2.6	8.8.8.8	0xa9bd	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:07.959935904 CET	192.168.2.6	8.8.8.8	0x52c4	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:15.200695992 CET	192.168.2.6	8.8.8.8	0xe1de	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:15.647783995 CET	192.168.2.6	8.8.8.8	0xa6e4	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:18.801898003 CET	192.168.2.6	8.8.8.8	0x45ea	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:25.476068020 CET	192.168.2.6	8.8.8.8	0x808b	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:36.076216936 CET	192.168.2.6	8.8.8.8	0x992a	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:36.809657097 CET	192.168.2.6	8.8.8.8	0xb0be	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:37.067101002 CET	192.168.2.6	8.8.8.8	0x9a5b	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:40.575599909 CET	192.168.2.6	8.8.8.8	0x27de	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:46.143867016 CET	192.168.2.6	8.8.8.8	0x6ea8	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:47.428843975 CET	192.168.2.6	8.8.8.8	0xec77	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:47.528775930 CET	192.168.2.6	8.8.8.8	0x758f	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:51.183243036 CET	192.168.2.6	8.8.8.8	0xdd02	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:56.538692951 CET	192.168.2.6	8.8.8.8	0x89c2	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:57.601921082 CET	192.168.2.6	8.8.8.8	0x34eb	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:57.770467043 CET	192.168.2.6	8.8.8.8	0xfa5f	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:01.542634010 CET	192.168.2.6	8.8.8.8	0xa433	Standard query (0)	technoshop er.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:08.000895023 CET	192.168.2.6	8.8.8.8	0x4166	Standard query (0)	avolebukon eh.website	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 23, 2021 10:55:08.252931118 CET	192.168.2.6	8.8.8.8	0x9a71	Standard query (0)	avolebukoneh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:12.061213017 CET	192.168.2.6	8.8.8.8	0xab20	Standard query (0)	avolebukoneh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:18.446316004 CET	192.168.2.6	8.8.8.8	0x364a	Standard query (0)	technoshoper.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:28.780441046 CET	192.168.2.6	8.8.8.8	0x3eb5	Standard query (0)	avolebukoneh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:29.643714905 CET	192.168.2.6	8.8.8.8	0xb825	Standard query (0)	technoshoper.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:30.182122946 CET	192.168.2.6	8.8.8.8	0x932d	Standard query (0)	technoshoper.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:33.765352011 CET	192.168.2.6	8.8.8.8	0xe690	Standard query (0)	technoshoper.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:38.797801018 CET	192.168.2.6	8.8.8.8	0x74db	Standard query (0)	technoshoper.com	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:39.938874960 CET	192.168.2.6	8.8.8.8	0x114d	Standard query (0)	avolebukoneh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:40.500597954 CET	192.168.2.6	8.8.8.8	0xfb82	Standard query (0)	avolebukoneh.website	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:44.059487104 CET	192.168.2.6	8.8.8.8	0x7e9e	Standard query (0)	avolebukoneh.website	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2021 10:51:36.780513048 CET	8.8.8.8	192.168.2.6	0x2273	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 23, 2021 10:51:42.662647963 CET	8.8.8.8	192.168.2.6	0xb094	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Nov 23, 2021 10:51:43.664618015 CET	8.8.8.8	192.168.2.6	0xd93a	No error (0)	contextual.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Nov 23, 2021 10:51:49.626315117 CET	8.8.8.8	192.168.2.6	0xcbe0	No error (0)	lg3.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Nov 23, 2021 10:51:50.203742981 CET	8.8.8.8	192.168.2.6	0x5b22	No error (0)	assets.msn.com	assets.msn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 23, 2021 10:51:53.231761932 CET	8.8.8.8	192.168.2.6	0x37cf	No error (0)	hblg.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Nov 23, 2021 10:51:59.341965914 CET	8.8.8.8	192.168.2.6	0xc8e4	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 23, 2021 10:52:20.920825005 CET	8.8.8.8	192.168.2.6	0xf03b	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Nov 23, 2021 10:52:20.920825005 CET	8.8.8.8	192.168.2.6	0xf03b	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Nov 23, 2021 10:52:20.920825005 CET	8.8.8.8	192.168.2.6	0xf03b	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:43.977089882 CET	8.8.8.8	192.168.2.6	0xfcde	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:44.321031094 CET	8.8.8.8	192.168.2.6	0x8bb6	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:47.348301888 CET	8.8.8.8	192.168.2.6	0xa6c6	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:54.408608913 CET	8.8.8.8	192.168.2.6	0xf1c2	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:54.951196909 CET	8.8.8.8	192.168.2.6	0x76e0	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:53:57.780173063 CET	8.8.8.8	192.168.2.6	0xd7f5	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:04.604422092 CET	8.8.8.8	192.168.2.6	0xd5e9	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2021 10:54:05.202909946 CET	8.8.8.8	192.168.2.6	0xa9bd	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:07.980220079 CET	8.8.8.8	192.168.2.6	0x52c4	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:15.225646019 CET	8.8.8.8	192.168.2.6	0xe1de	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:15.668725014 CET	8.8.8.8	192.168.2.6	0xa6e4	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:18.823904991 CET	8.8.8.8	192.168.2.6	0x45ea	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:25.496202946 CET	8.8.8.8	192.168.2.6	0x808b	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:36.097043991 CET	8.8.8.8	192.168.2.6	0x992a	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:36.829816103 CET	8.8.8.8	192.168.2.6	0xb0be	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:37.100219011 CET	8.8.8.8	192.168.2.6	0x9a5b	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:40.596667051 CET	8.8.8.8	192.168.2.6	0x27de	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:46.166496992 CET	8.8.8.8	192.168.2.6	0x6ea8	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:47.453711987 CET	8.8.8.8	192.168.2.6	0xec77	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:47.549573898 CET	8.8.8.8	192.168.2.6	0x758f	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:51.203574896 CET	8.8.8.8	192.168.2.6	0xdd02	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:56.558392048 CET	8.8.8.8	192.168.2.6	0x89c2	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:57.621939898 CET	8.8.8.8	192.168.2.6	0x34eb	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:54:57.791332006 CET	8.8.8.8	192.168.2.6	0xfa5f	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:01.562652111 CET	8.8.8.8	192.168.2.6	0xa433	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:08.021049023 CET	8.8.8.8	192.168.2.6	0x4166	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:08.274789095 CET	8.8.8.8	192.168.2.6	0x9a71	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:12.081146955 CET	8.8.8.8	192.168.2.6	0xab20	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:18.464086056 CET	8.8.8.8	192.168.2.6	0x364a	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:28.800038099 CET	8.8.8.8	192.168.2.6	0x3eb5	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:29.661693096 CET	8.8.8.8	192.168.2.6	0xb825	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:30.203749895 CET	8.8.8.8	192.168.2.6	0x932d	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:33.785058975 CET	8.8.8.8	192.168.2.6	0xe690	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2021 10:55:38.817606926 CET	8.8.8.8	192.168.2.6	0x74db	No error (0)	technoshoper.com		45.9.20.245	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:39.958785057 CET	8.8.8.8	192.168.2.6	0x114d	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:40.519731998 CET	8.8.8.8	192.168.2.6	0xfb82	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)
Nov 23, 2021 10:55:44.079997063 CET	8.8.8.8	192.168.2.6	0x7e9e	Name error (3)	avolebukoneh.website	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - btloader.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49823	104.26.7.139	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 09:52:21 UTC	0	OUT	GET /tag?o=6208086025961472&upapi=true HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: btloader.com Connection: Keep-Alive
2021-11-23 09:52:21 UTC	0	IN	HTTP/1.1 200 OK Date: Tue, 23 Nov 2021 09:52:21 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: 2524 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=9tSAb0qJURYPecAhlFR31D6V6y8WmhJzLk8VfHiSNkRpSqrAmbscXgsKaKrnCtvFLCUzBqyaSc4Zf2PiJnHT0KlTY%2BKTDKJYBXZwDIJFJJqAUSxjWMdQXoP31%2FEliw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b298113fff92b1e-FRA
2021-11-23 09:52:21 UTC	1	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 6c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 74 72 79 7b 72 28 6c 2e 74 68 72 6f 77 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 72 28 65 29 7b 76 61 72 20 74 3b 65 2e 64 6f 6e 65 3f 6e 28 65 2e 76 61 6c 75 65 29 3a 28 28 74 3d 65 2e 76 61 6c 75 65 29 69 6e 73 74 61 6e 63 65 6f 66 20 63 3f 74 3a 6e 65 77 20 63 28 66 75 6e 63 74 69 6f Data Ascii: !function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(functio
2021-11-23 09:52:21 UTC	1	IN	Data Raw: 6f 6e 28 74 29 7b 69 66 28 61 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 22 47 65 6e 65 72 61 74 6f 72 20 69 73 20 61 6c 72 65 61 64 79 20 65 78 65 63 75 74 69 6e 67 2e 22 29 3b 66 6f 72 28 3b 63 3b 29 74 72 79 7b 69 66 28 61 3d 31 2c 72 26 26 28 69 3d 32 26 74 5b 30 5d 3f 72 2e 72 65 74 75 72 6e 3a 74 5b 30 5d 3f 72 2e 74 68 72 6f 77 7c 7c 28 28 69 3d 72 2e 72 65 74 75 72 6e 29 26 26 69 2e 63 61 6c 6c 28 72 29 2c 30 29 3a 72 2e 6e 65 78 74 29 26 26 21 28 69 3d 69 2e 63 61 6c 6c 28 72 2c 74 5b 31 5d 29 29 2e 64 6f 6e 65 29 72 65 74 75 72 6e 20 69 3b 73 77 69 74 63 68 28 72 3d 30 2c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 61 6c 75 65 5d 29 2c 74 5b 30 5d 29 7b 63 61 73 65 20 30 3a 63 61 73 65 20 31 3a 69 3d 74 3b 62 72 65 61 Data Ascii: on(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;brea

Timestamp	kBytes transferred	Direction	Data
2021-11-23 09:52:21 UTC	2	IN	Data Raw: 61 70 70 65 6e 64 43 68 69 6c 64 28 65 29 7d 29 7d 76 61 72 20 75 2c 61 2c 64 2c 62 2c 6d 3b 75 3d 22 36 32 30 38 30 38 36 30 32 35 39 36 31 34 37 32 22 2c 61 3d 22 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 64 3d 22 61 70 69 2e 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 62 3d 22 32 2e 30 2e 32 2d 32 2d 67 66 64 63 39 30 35 34 22 2c 6d 3d 22 22 3b 76 61 72 20 6f 3d 7b 22 6d 73 6e 2e 63 6f 6d 22 3a 7b 22 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 74 72 75 65 2c 22 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 22 77 65 62 73 69 74 65 5f 69 64 22 3a 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 35 32 22 7d 7d 2c 77 3d 7b 74 72 61 63 65 49 44 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 69 66 28 21 65 7c Data Ascii: appendChild(e)}}}var u,a,d,b,m;u="6208086025961472",a="btloader.com",d="api.btloader.com",b="2.0.2-2-gfdc9054",m="";var o={"msn.com":{"content_enabled":true,"mobile_content_enabled":false,"website_id":"567173 7388695552"}},w={traceID:function(e,t,n){if(!e|
2021-11-23 09:52:21 UTC	4	IN	Data Raw: 62 73 69 74 65 49 44 3d 6f 5b 6e 5d 2e 77 65 62 73 69 74 65 5f 69 64 2c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 29 3b 74 7c 7c 28 28 6e 65 77 20 49 6d 61 67 65 29 2e 73 72 63 3d 22 2f 2f 22 2b 64 2b 22 2f 6c 3f 65 76 65 6e 74 3d 75 6e 6b 6e 6f 77 6e 44 6f 6d 61 69 6e 26 6f 72 67 3d 22 2b 75 2b 22 26 64 6f 6d 61 69 6e 3d 22 2b 65 29 7d 28 29 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 74 61 67 5f 64 3d 7b 6f 72 67 49 44 3a 75 2c 64 6f 6d 61 69 6e 3a 61 2c 61 70 69 44 6f 6d 61 69 6e 3a 64 2c 76 65 72 73 69 6f 6e 3a 62 2c 77 65 62 73 69 74 65 Data Ascii: bsiteID=o[n].website_id,p.contentEnabled=o[n].content_enabled,p.mobileContentEnabled=o[n].mobile_content_enabled);t||((new Image).src="//"+d+"/l?event=unknownDomain&org="+u+"&domain="+e)}(),window.__bt_tag_d={orgID:u,domain:a,apiDomain:d,version:b,website
2021-11-23 09:52:21 UTC	5	IN	Data Raw: 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 2b 74 29 29 7d 2c 6f 2b 3d 74 7d 29 7d 76 61 72 20 6c 3d 74 5b 30 5d 3b 69 66 28 6e 75 6c 6c 21 3d 6c 26 26 6c 2e 62 75 6e 64 6c 65 73 29 7b 76 61 72 20 73 3d 6f 2c 75 3d 31 2d 6f 3b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 6c 2e 62 75 6e 64 6c 65 73 29 2e 73 6f 72 74 28 29 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 6c 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 69 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 73 2b 75 2a 61 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 73 2b 75 2a 28 61 2b 74 29 29 7d 2c 61 2b 3d 74 7d 29 7d 76 61 72 20 64 Data Ascii: ath.trunc(100*(+o+0)),max:Math.trunc(100*(+o+0+t))},o+=t}}var l=t[0];if(null!=l&&l.bundles){var s=o,u=1-o;Object.keys(l.bundles).sort().forEach(function(e){var t=l.bundles[e];i[e]={min:Math.trunc(100*(s+u*a)),max:Math.trunc(100*(s+u*(a+t)))},a+=t}}var d
2021-11-23 09:52:21 UTC	7	IN	Data Raw: 20 61 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 76 65 6e 74 28 22 43 75 73 74 6f 6d 45 76 65 6e 74 22 29 3b 61 2e 69 6e 69 74 43 75 73 74 6f 6d 45 76 65 6e 74 28 74 2c 6e 2e 62 75 62 62 6c 65 73 2c 6e 2e 63 61 6e 63 65 6c 61 62 6c 65 2c 6e 2e 64 65 74 61 69 6c 29 2c 77 69 6e 64 6f 77 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 61 29 7d 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 Data Ascii: a=document.createEvent("CustomEvent");a.initCustomEvent(t,n.bubbles,n.cancelable,n.detail),window.dispatchEvent(a)}f={},window.__bt_intrnl={traceID:w.traceID};try{!function(){r(this,void 0,void 0,function(){var t,n,o;return i(this,function(e){switch(e.la
2021-11-23 09:52:21 UTC	8	IN	Data Raw: 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 22 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 4d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 29 2c 70 2e 77 65 62 73 69 74 65 49 44 26 26 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 26 26 28 21 28 6e 3d 2f 28 61 6e 64 72 6f 69 64 7c 62 62 5c 64 2b 7c 6d 65 65 67 6f 29 2e 2b 6d 6f 62 69 6c 65 7c 61 76 61 6e 74 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 Data Ascii: ContentEnabled="true"==localStorage.getItem("forceMobileContent")||p.mobileContentEnabled),p.websiteID&&p.contentEnabled&&(!(n=/(android|bb\d+|meego).+mobile|avantgo|bada\/|blackberry|blazer|compal|elaine|fennec|hiptop|iemobile|ip(hone|od)|iris|kindle|lge
2021-11-23 09:52:21 UTC	9	IN	Data Raw: 76 29 7c 7a 7a 29 7c 6d 74 28 35 30 7c 70 31 7c 76 20 29 7c 6d 77 62 70 7c 6d 79 77 61 7c 6e 31 30 5b 30 2d 32 5d 7c 6e 32 30 5b 32 2d 33 5d 7c 6e 33 30 28 30 7c 32 29 7c 6e 35 30 28 30 7c 32 7c 35 29 7c 6e 37 28 30 28 30 7c 31 29 7c 31 30 29 7c 6e 65 28 28 63 7c 6d 29 5c 2d 7c 6f 6e 7c 74 66 7c 77 66 7c 77 67 7c 77 74 29 7c 6e 6f 6b 28 36 7c 69 29 7c 6e 7a 70 68 7c 6f 32 69 6d 7c 6f 70 28 74 69 7c 77 76 29 7c 6f 72 61 6e 7c 6f 77 67 31 7c 70 38 30 30 7c 70 61 6e 28 61 7c 64 7c 74 29 7c 70 64 78 67 7c 70 67 28 31 33 7c 5c 2d 28 5b 31 2d 38 5d 7c 63 29 29 7c 70 68 69 6c 7c 70 69 72 65 7c 70 6c 28 61 79 7c 75 63 29 7c 70 6e 5c 2d 32 7c 70 6f 28 63 6b 7c 72 74 7c 73 65 29 7c 70 72 6f 78 7c 70 73 69 6f 7c 70 74 5c 2d 67 7c 71 61 5c 2d 61 7c 71 63 28 30 37 7c Data Ascii: v)|zz)|mt(50|p1|v)|mwbp|mywa|n10[0-2]|n20[2-3]|n30(0|2)|n50(0|2|5)|n7(0(0|1)|10)|ne((c|m)\-|on|tf|wf|wg|wt)|nok(6|i)|nzph|o2im|op(ti|wv)|oran|owg1|p800|pan(a|d|t)|pdxg|pg(13|\-([1-8]|c))|phil|pire|pl(ay|uc)|pn\-2|po(ck|rt|se)|prox|psio|pt\-g|qa\-a|qc(07|

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6980 Parent PID: 1868

General

Start time:	10:51:28
Start date:	23/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\WTXuYxax6d.dll"
Imagebase:	0xaa0000
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, Description: Yara detected Ursnif, Source: 00000000.00000002.880807454.0000000001AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.701819091.0000000001AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.702016309.0000000001AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.701985470.0000000001AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.702307918.0000000001AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.701915707.0000000001AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.880442482.0000000001299000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.701957231.0000000001AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.746687116.000000000186D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.768852725.000000000176F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.878853677.0000000000870000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.701777888.0000000001AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.702038882.0000000001AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.724522780.000000000196B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.878927946.0000000000880000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.701868957.0000000001AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.879009895.0000000000920000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6992 Parent PID: 6980

General

Start time:	10:51:28
Start date:	23/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\WTXuYxax6d.dll",#1
Imagebase:	0x2a0000
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: 7000 Parent PID: 6980

General

Start time:	10:51:29
Start date:	23/11/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\WTXuYxax6d.dll
Imagebase:	0xe30000
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, Description: Yara detected Ursnif, Source: 00000002.00000003.620315557.00000000053B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.664565353.000000000513D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.620214841.00000000053B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.642767964.000000000523B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000002.881549232.00000000053B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.620265495.00000000053B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.620243933.00000000053B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.620142786.00000000053B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.620475830.00000000053B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.620285363.00000000053B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.881330354.0000000004EA9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.620302187.00000000053B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.686987362.000000000503F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.879036722.00000000009F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.620184852.00000000053B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.879010768.00000000009E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.878979369.0000000000990000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7012 Parent PID: 6992

General

Start time:	10:51:29
Start date:	23/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\WTXuYxax6d.dll",#1
Imagebase:	0xb50000
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, Description: Yara detected Ursnif, Source: 00000003.00000003.612905346.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.612880805.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.612995967.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.613174085.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.879831053.0000000000A50000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.879916049.0000000000A60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.635568127.0000000004E5B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.679769381.0000000004C5F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.657340118.0000000004D5D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.879772547.0000000000A40000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.884432102.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.884087885.00000000049A9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.613014620.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.612932234.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.612953290.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.612852123.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.612982412.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 7020 Parent PID: 6980

General

Start time:	10:51:29
Start date:	23/11/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff721e20000
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: 7052 Parent PID: 6980

General

Start time:	10:51:31
Start date:	23/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\WTXuYxax6d.dll,DllRegisterServer
Imagebase:	0xb50000
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: 00000005.00000002.883888908.0000000004D49000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000002.884237946.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.613835753.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.881014887.0000000002B80000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.613794834.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.613948347.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.613862631.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.613818747.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.613737711.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.658506384.000000000507D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.879852238.0000000000B40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.636697378.000000000517B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.681026277.0000000004F7F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.613707607.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.613851431.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.613762692.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.880994352.0000000002B70000.00000004.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 7104 Parent PID: 7020

General

Start time:	10:51:32
Start date:	23/11/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:7020 CREDAT:17410 /prefetch:2
Imagebase:	0x1050000
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: 3684 Parent PID: 6980

General

Start time:	10:51:36
Start date:	23/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\WTXuYxax6d.dll,azfdnkcrayghb
Imagebase:	0xb50000
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: 6164 Parent PID: 6980

General

Start time:	10:51:47
Start date:	23/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\WTXuYxax6d.dll,bngggbakts
Imagebase:	0xb50000
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