ID: 403080
Sample Name: block.dll
Cookbook: default.jbs
Time: 18:45:28
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

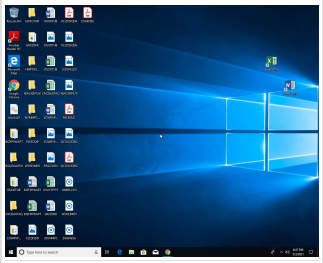
Analysis Report block.dll

Overview

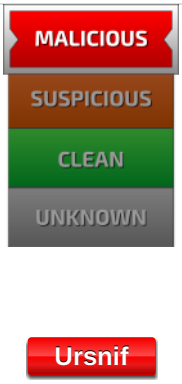
General Information

Sample Name:	block.dll
Analysis ID:	403080
MD5:	5a7c87dab250ce..
SHA1:	554c4ccf2341182..
SHA256:	8a26c32848c9ea..
Tags:	DLL Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection

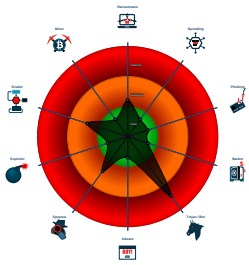


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Yara detected Ursnif
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Creates a process in suspended mo…
- Detected potential crypto function
- Monitors certain registry keys / valu…
- Queries the installation date of Wind…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5720 cmdline: loaddll32.exe 'C:\Users\user\Desktop\block.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4516 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\block.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5752 cmdline: rundll32.exe 'C:\Users\user\Desktop\block.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5592 cmdline: rundll32.exe C:\Users\user\Desktop\block.dll,Pape1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4648 cmdline: rundll32.exe C:\Users\user\Desktop\block.dll,Riverslow MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5856 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6328 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5856 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6452 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5856 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5708 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5816 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5708 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6100 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5708 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6616 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6480 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 1972 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"8oKmD0Ib40VYxHRgT7OnHwlxmK3U2F2Fl3GpR9KrKxvSCrIeiCLZWlQ2QCt+AnP+N5tCnTTv45/b0/D8Eb4xqxiXBnUy/ADWorQScIoNIPfBQqutzO+Ozy/mev4m2eZAuMivS2UNJVH4DVsYsAkGAC4GR+aszytDfGSZp3MklfgRJ6No
j034BrS4tQl5qmeWhJa+Of/CLdmkCwJurSEhMKu3NK7g4EVzni8lIJrDkWNCTaVL4CWXewbAOJFPwh8Y/20KkHTZmVKLmJJRcSj8yyH0avZDtWvJHRDxiI+JYUar2ia3phWwtqVzVhzYzz8aoUVzmlt840TF55o2e8TRUCEZNNmvmluqg
NZzQuNIj68=",
  "c2_domain": [
    "app.buboleinov.com",
    "chat.veminiare.com",
    "chat.billionady.com",
    "app3.maintorna.com"
  ],
  "botnet": "1500",
  "server": "580",
  "serpent_key": "ZQktwkM8O9lYn9oX",
  "sleep_time": "10",
  "SetWaitableTimer_value": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.353402660.0000000005A48000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.353461083.0000000005A48000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.352720988.0000000003D28000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.352839215.0000000003D28000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.352637772.0000000003D28000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 17 entries				

Unpacked PEs

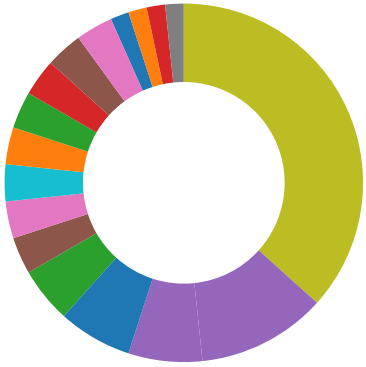
Source	Rule	Description	Author	Strings
1.3.loaddll32.exe.1678d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.3.rundll32.exe.3058d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.6dd30000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.6dd30000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.3f58d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Spam, unwanted Advertisements and Ransom Demands



Click to jump to signature section

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

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

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:

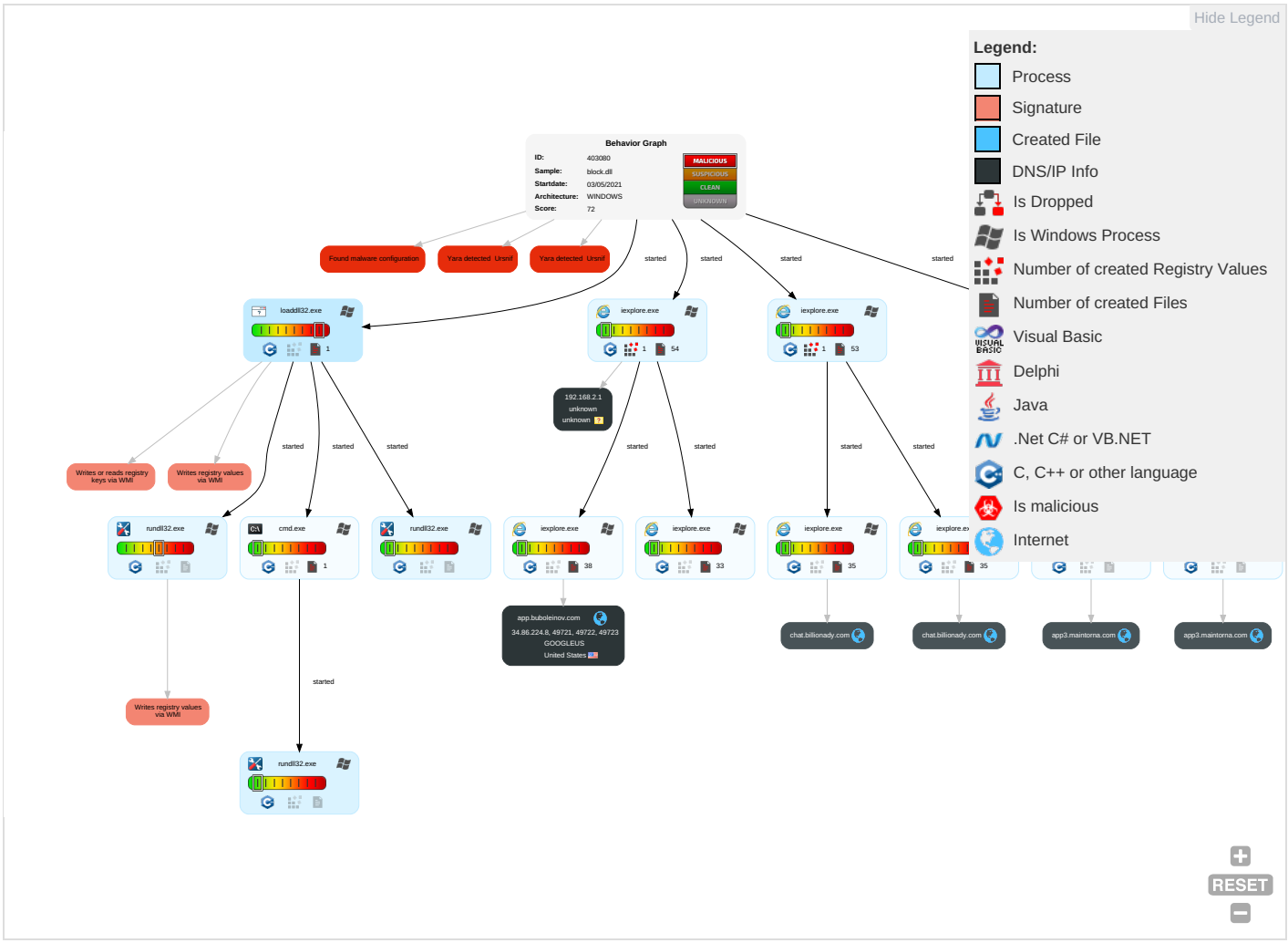
Yara detected Ursnif

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	Rem Serv Effe
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Rem Trac With Auth
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS	Rem Wipe With Auth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obta Devi Clou Bacl
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

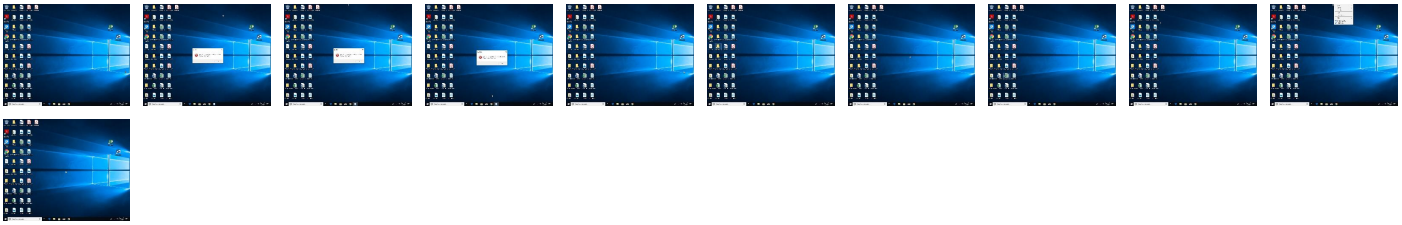
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.33d0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.loaddll32.exe.12e0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://app3.maintorna.com/cDNEPwBarUn/ROJH1XYkRfSClQ/qONBPlQo8FxG6mQW9Ogcz/u7mo1Dj2PullrRPq/bR_2BFpPLx7OhU9/HJBhAhHBzmstPPDOE1/w6ebBa_2B/KX_2BOm6FIW3gd6Bvbnj/Sh9h8HN_2BONCwGgPQr/IY0nkmO9u18wIpqrmMTW3z/GWi0vHa3h_2Bj/6IH92Uhj/Iom39I56_2BMfY2_2BRDxU0/VfXOZ9_2BQ/hDbFynpSdJTA10_2B/DTN9zUXGBVIL/6pinDdbjTIZ/J8liN5BZT7oU_2/FDetd44m1Cdm74WjgwpWw/7RPnYCrU0gXGaG9w/dolpQdALprU5fVz/g9lnmYz4c/oMbk6u	0%	Avira URL Cloud	safe	
http://app.buboleinov.com/zWr7XKiLQ_2F3QZ2bR/ZuzwfgbmQ/mjgvv5jUliwpj1wMmSf1/mVwZRrRJ02ozj18W4CC/_2FqTc0J0ACZs0Zo0yB15V/UkO_2BhXUEjqi/ylcme0uu/h88DPxTz52fwzk2KiAITqAX/y1YkE9ueOd/NzFODbcfeCN_2B548/9jGMMg_2FjQB/TCcN38_2FLI/w78Mf5LsU18OtD/O9ldbealz2YOBBV9govEw/if1bIKJhIzR9fYIT/Dva1E7_2F2LcgBj/3WJFp2Il273lx9FN_2/B45JK5S6v/rZZWdDOKWu65eMI2rNKK/RAsOHyLCy3eKhZf_2Fm/CD_2FuANPfLuHGjULRoA2Y/Paqy	0%	Avira URL Cloud	safe	
http://app.buboleinov.com/zWr7XKiLQ_2F3QZ2bR/ZuzwfgbmQ/mjgvv5jUliwpj1wMmSf1/mVwZRrRJ02ozj18W4CC/_2Fq	0%	Avira URL Cloud	safe	
http://app.buboleinov.com/u9JBOXOyCt1J/Cqk3pF0_2B2/evko0P1iOLkfYu/tE8kijPwXl6fpTUvGY0L0/uKSRiZsz1TrV	0%	Avira URL Cloud	safe	
http://chat.billionady.com/1Z7Zv_2Fo_2BBI/5yyu9xO7U6xQJUAU9LBdU/_2BZsJzv4AW1v4_2/FuBHkCgtXKYNI2J/fjLUpx4yvdGQ9xBWU8/nZ2UCR2Fn/6_2BJUjWbSDTFYEq01IK/G2MuJJozgl6fI_2Bxi6/8WHocMwy1m3c6beo7EybdT/0fZNT0A7jOYrz/ZJgKKaGn/V_2Bc6nIeAMBXcBQSTKS3tl/dRpB7HoFuq/5r0h_2Bic5oCoaHxQ/GZIQmnaYFeN7/lgmkXjg8R1P/o6CJiUeiWxo9TA/Om1BRSx_2BLEYhxw_2B1w/ztx7Xd1V_2BwFgLL/5ttSiFJbfjzPnDR/nMd_2BdWk4HTz_2Ftn/Va7N0lfshKE/mKz	0%	Avira URL Cloud	safe	
http://app3.maintorna.com/cDNEPwBarUn/ROJH1XYkRfSClQ/qONBPlQo8FxG6mQW9Ogcz/u7mo1Dj2PullrRPq/bR_2BFpP	0%	Avira URL Cloud	safe	
http://chat.billionady.com/1Z7Zv_2Fo_2BBI/5yyu9xO7U6xQJUAU9LBdU/_2BZsJzv4AW1v4_2/FuBHkCgtXKYNI2J/fjL	0%	Avira URL Cloud	safe	
http://chat.billionady.com/hPJ75Rz1l0Yg172f0/W92Rc6NrZORu/agJ84T4GWPF/71Su9Jrd5ILrko/1XWo5CLa_2Bx1ycL2fXGF/76IsZupbi6IIlogp/P_2BrqGlfT6Z_2F/9HIF9QL_2Ffn95EjHz/EKpbgAout/m_2FkBfNGzNFhXOxCcqe/1zQKvOOwqE_2B22qrZS/vj3rmMMb_2BsLkd2AZhDC4/602lvjtm6dYcP/dyzgfgBT/A_2BC4eofqol5orEsMEQPWe/zZ6Swnuj_2/FM3kwbNjGbF9dztKO/5Sul25wMK_2F/fSrDDmSQa3P/LwvXQje5tWHJ24/YCtfl_2Bd9Wgni_2B/yKHW	0%	Avira URL Cloud	safe	
http://app3.maintorna.com/6r_2FD5QsDWTjJjwzHfBaL/2HYJ2K06UlseV/lZ1msT18/ny_2FHLDol8VG6VjuFqLZ26/y1nZ	0%	Avira URL Cloud	safe	
http://app3.maintorna.com/6r_2FD5QsDWTjJjwzHfBaL/2HYJ2K06UlseV/lZ1msT18/ny_2FHLDol8VG6VjuFqLZ26/y1nZcgTjUQ/HL5YV0taxU5zFMebw/ouCjKnY1SB67/bctA52f0140/sHpnVH95T_2Fuj/QLIAvGeVws2XTmrrXV3BZ/psxvZSZg2i7jPF9N/caz3S5QCjepHp3W/l6q5V6Mw_2BHygdAjz/QFWLuSVDY/2iEYyTYQm6wj63ekurFy/nVWvwQ5A_2FY6vAZ0b2/ysxli7hdttfqNZtbDq2s51/_2FLPh7LrbbPo/JhDaZ4qW/MGAYB_2BvyA3HE7Ywiz/pWy	0%	Avira URL Cloud	safe	
http://chat.billionady.com/hPJ75Rz1l0Yg172f0/W92Rc6NrZORu/agJ84T4GWPF/71Su9Jrd5ILrko/1XWo5CLa_2Bx1yc	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
app3.maintorna.com	34.86.224.8	true	false		unknown
chat.billionady.com	34.86.224.8	true	false		unknown
app.buboleinov.com	34.86.224.8	true	false		unknown

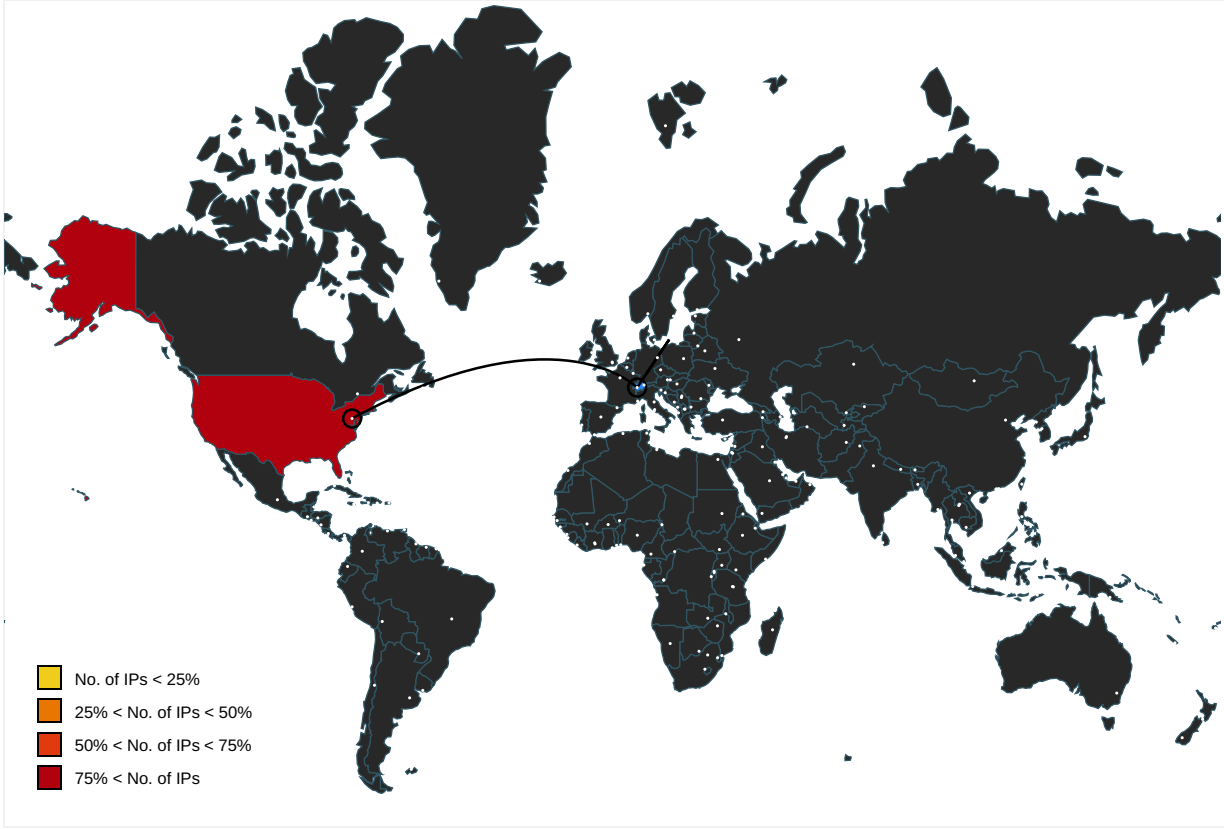
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://app3.maintorna.com/cDNEPwBarUn/ROJH1XYkRfSClQ/qONBPlQo8FxG6mQW9Ogcz/u7mo1Dj2PullrRPq/bR_2BFpPLx7OhU9/HJBhAhHBzmstPPDOE1/w6ebBa_2B/KX_2BOm6FIW3gd6Bvbnj/Sh9h8HN_2BONCwGgPQr/IY0nkmO9u18wIpqrmMTW3z/GWi0vHa3h_2Bj/6IH92Uhj/Iom39I56_2BMfY2_2BRDxU0/VfXOZ9_2BQ/hDbFynpSdJTA10_2B/DTN9zUXGBVIL/6pinDdbjTIZ/J8liN5BZT7oU_2/FDetd44m1Cdm74WjgwpWw/7RPnYCrU0gXGaG9w/dolpQdALprU5fVz/g9lnmYz4c/oMbk6u	false	• Avira URL Cloud: safe	unknown
http://app.buboleinov.com/zWr7XKiLQ_2F3QZ2bR/ZuzwfgbmQ/mjgvv5jUliwpj1wMmSf1/mVwZRrRJ02ozj18W4CC/_2FqTc0J0ACZs0Zo0yB15V/UkO_2BhXUEjqi/ylcme0uu/h88DPxTz52fwzk2KiAITqAX/y1YkE9ueOd/NzFODbcfeCN_2B548/9jGMMg_2FjQB/TCcN38_2FLl/w78Mf5LsU18OtD/O9ldbeaIz2YOBBV9govEw/if1bIKJhlzR9fYIT/Dva1E7_2F2LcgBj/3WJFp2Il273lx9FN_2/B45JK5S6v/rZZWdDOKWu65eMI2rNKK/RAsOHyLCy3eKhZf_2Fm/CD_2FuANPfLuHGjULRoA2Y/Paqy	false	• Avira URL Cloud: safe	unknown
http://chat.billionady.com/1Z7Zv_2Fo_2BBI/5yyu9xO7U6xQJUAU9LBdU/_2BZsJzv4AW1v4_2/FuBHkCgtXKYNI2J/fjLUpx4yvdGQ9xBWU8/nZ2UCR2Fn/6_2BJUjWbSDTFYEq01IK/G2MuJJozgl6fI_2Bxi6/8WHocMwy1m3c6beo7EybdT/0fZNT0A7jOYrz/ZJgKKaGn/V_2Bc6nIeAMBXcBQSTKS3tl/dRpB7HoFuq/5r0h_2Bic5oCoaHxQ/GZIQmnaYFeN7/lgmkXjg8R1P/o6CJiUeiWxo9TA/Om1BRSx_2BLEYhxw_2B1w/ztx7Xd1V_2BwFgLL/5ttSiFJbfjzPnDR/nMd_2BdWk4HTz_2Ftn/Va7N0lfshKE/mKz	false	• Avira URL Cloud: safe	unknown
http://chat.billionady.com/hPJ75Rz1l0Yg172f0/W92Rc6NrZORu/agJ84T4GWPF/71Su9Jrd5ILrko/1XWo5CLa_2Bx1ycL2fXGF/76IsZupbi6IIlogp/P_2BrqGlfT6Z_2F/9HIF9QL_2Ffn95EjHz/EKpbgAout/m_2FkBfNGzNFhXOxCcqe/1zQKvOOwqE_2B22qrZS/vj3rmMMb_2BsLkd2AZhDC4/602lvjtm6dYcP/dyzgfgBT/A_2BC4eofqol5orEsMEQPWe/zZ6Swnuj_2/FM3kwbNjGbF9dztKO/5Sul25wMK_2F/fSrDDmSQa3P/LwvXQje5tWHJ24/YCtfl_2Bd9Wgni_2B/yKHW	false	• Avira URL Cloud: safe	unknown
http://app3.maintorna.com/6r_2FD5QsDWTjJjwzHfBaL/2HYJ2K06UlseV/lZ1msT18/ny_2FHLDol8VG6VjuFqLZ26/y1nZcgTjUQ/HL5YV0taxU5zFMebw/ouCjKnY1SB67/bctA52f0140/sHpnVH95T_2Fuj/QLIAvGeVws2XTmrrXV3BZ/psxvZSZg2i7jPF9N/caz3S5QCjepHp3W/l6q5V6Mw_2BHygdAjz/QFWLuSVDY/2iEYyTYQm6wj63ekurFy/nVWvwQ5A_2FY6vAZ0b2/ysxIi7hdttfqNZtbDq2s51/_2FLPh7LrbbPo/JhDaZ4qW/MGAYB_2BvyA3HE7Ywiz/pWy	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://app.buboleinov.com/zWr7XKiLQ_2F3QZ2bR/ZuzwfgbmQ/mjgvv5jUliwpj1wMmSf1/mVwZRrRJ02ozj18W4CC/_2Fq	{A33D02D4-AC7A-11EB-90E5-ECF4BB570DC9}.dat.19.dr	false	• Avira URL Cloud: safe	unknown
http://app.buboleinov.com/u9JBOXOyCt1J/Cqk3pF0_2B2/evko0P1iOLkfYu/tE8kijPwXl6fpTUvGY0L0/uKSRiZsz1TrV	~DF036A3D1EB4248F1E.TMP.19.dr, {A33D02D2-AC7A-11EB-90E5-ECF4BB570DC9}.dat.19.dr	false	• Avira URL Cloud: safe	unknown
http://app3.maintorna.com/cDNEPwBarUn/ROJH1XYkRfSClQ/qONBPlQo8FxG6mQW9Ogcz/u7mo1Dj2PullrRPq/bR_2BFpP	{CDCCBAD7-AC7A-11EB-90E5-ECF4BB570DC9}.dat.36.dr, ~DF7FEBD80971BE8B6A.TMP.36.dr	false	• Avira URL Cloud: safe	unknown
http://chat.billionady.com/1Z7Zv_2Fo_2BBI/5yyu9xO7U6xQJUAU9LBdU/_2BZsJzv4AW1v4_2/FuBHkCgtXKYNI2J/fjL	{BF692A67-AC7A-11EB-90E5-ECF4BB570DC9}.dat.29.dr, ~DF183688B2D13937F7.TMP.29.dr	false	• Avira URL Cloud: safe	unknown
http://app3.maintorna.com/6r_2FD5QsDWTjJjwzHfBaL/2HYJ2K06UlseV/lZ1msT18/ny_2FHLDol8VG6VjuFqLZ26/y1nZ	~DFE60F766B8C74F7D6.TMP.36.dr, {CDCCBAD9-AC7A-11EB-90E5-ECF4BB570DC9}.dat.36.dr	false	• Avira URL Cloud: safe	unknown
http://chat.billionady.com/hPJ75Rz1l0Yg172f0/W92Rc6NrZORu/agJ84T4GWPF/71Su9Jrd5ILrko/1XWo5CLa_2Bx1yc	{BF692A65-AC7A-11EB-90E5-ECF4BB570DC9}.dat.29.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.86.224.8	app3.maintorna.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403080
Start date:	03.05.2021
Start time:	18:45:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	block.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:	39
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:	mal72.troj.winDLL@24/69@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.8% (good quality ratio 9.3%) • Quality average: 79.1% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 76% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 93.184.220.29, 131.253.33.200, 13.107.22.200, 52.147.198.201, 104.43.139.144, 92.122.145.220, 104.80.23.128, 13.107.5.88, 13.107.42.23, 104.42.151.234, 20.190.160.131, 20.190.160.7, 20.190.160.70, 20.190.160.9, 20.190.160.135, 20.190.160.133, 20.190.160.68, 20.190.160.74, 20.82.210.154, 88.221.62.148, 92.122.213.194, 92.122.213.249, 152.199.19.161, 20.50.102.62, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, arc.msn.com.nsatc.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, ocsp.digicert.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, www.bing.com, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, l-0014.l-msedge.net, skypedataprdcolwus16.cloudapp.net, www.tm.lg.prod.aadmsa.trafficmanager.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/403080/sample/block.dll

Simulations

Behavior and APIs

Time	Type	Description
18:46:55	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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.{A33D02D0-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	1.998597132882559
Encrypted:	false
SSDEEP:	96:r0ZTZU2fWjtEgbfEarzXwKMNah4q40l4Q4kBEhu/ap3M4TlapUJaRkmKJaROmoSo:r0ZTZU2fWjtpfxFMCcKNMu/tVcocInYg
MD5:	B24CF1A212CFBBF68F79B5213CEE9F75
SHA1:	7B3560C4290A072EF06C2A36A8A1DCC02D348F6D
SHA-256:	BBAA55CB92A0669BA9668C0C5BD3DB5B4C69E1BA76D5741018DA25E58674DA8A
SHA-512:	ABFEC6ACCE03495AB33B8D55AAF9336BF624AC63897B75B05328BB982BF864C3BCBE2E9A67FD0C12F56AF66531B115019165288794BCA8EEE0229199692300F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{BF692A63-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.0018297658762045
Encrypted:	false
SSDEEP:	96:r3Z8Zh2RWat6bfjzEzKMBbqbLbQ8uzhBMJK3MTSJKmWJiktWJiOlVJcin2JVtcc7:r3Z8Zh2RWat6fvRMgULhM/ilRQEMoU8g
MD5:	C06B04938835F26192BB44AC2AC84E7E
SHA1:	ECBEF63BF5FB3209DE49D711F16217A31073883C
SHA-256:	BF64DB656C32107E023373C2446C4ED16D0E8F1D61868B563E4E85AD0C609256

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{BF692A63-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
SHA-512:	66A05E525798097AC87112E97D9E2B05CB421623D86051BFC7914BDFCC52CD63C329D6B57F16B11D5484652861076B866C8927A3A302AAEED70150E1466C93F1
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CDCCBAD5-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.0039146351507484
Encrypted:	false
SSDEEP:	192:reZlZBl2oWf5ztUfcdMZRx5MJspF3pFVF4QUoLVog:rqLB8fhxaJZR42jCoZ
MD5:	342C91CC0B0353F57DBF32BB29242C8E
SHA1:	037E3195062CA1DCCA584265D2A0525F325A49C3
SHA-256:	750BCE72B7FD2B9DAAF1BBBB883401D45CECB498BF9A2127BCFCE50E009D01C1
SHA-512:	D267971695F28B25473C00FDBEC26F6DB975E91F9C58DFD925B6E21C12E0A2607886EC9234417BAD5AEC5DFCDEEC9CB49A91E4445722389B50E8DE4EF8739C3
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A33D02D2-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27596
Entropy (8bit):	1.9182205322719534
Encrypted:	false
SSDEEP:	96:rZZWQP69BSLjh21W8M1tvnjNvvlvnjNJjgA:rZZWQP69kLjh21W8M1tvnjRlvnjjjgA
MD5:	0D590BFF9E92402520284095D370E3F0
SHA1:	07CD80D0E3EFD4958A7F611B3C7D7A41AE9CF281
SHA-256:	E9E32838A457E664EBB5A46C6898C786A8364C65EAEF5348737B141968497DE0
SHA-512:	87BF1D0307E6A4F44A03317EB3DC89EF276AC16D2A1BB0846F7CB0482D26D3BD8F8F1DB81548C0E1E35000316D28ED51318AF7640B50E4F7C21828330E58E35
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A33D02D4-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28148
Entropy (8bit):	1.9198453830362774
Encrypted:	false
SSDEEP:	192:ryZ5QE6CkGj9cs293W9SM9OF/N+nlKd1/N+0+nlbsA:ruev7AU0twl+lKHl+0+lbH
MD5:	F3CCC6032DDDD268833EE14565131965
SHA1:	33DF253B55348C0C3E53E7ADB3938480DD84ABD3
SHA-256:	42CD4E34995742C5B784EEA3DDD3E9FB80C000DFB284CD6863C78FEF37DAA173
SHA-512:	C178A5A3CCB576B1D3E3129ADDB8194E544B6AB9FF6D78B1EF4F014520738D47DA0D0E2B61F4E89A41A528850793A83C5A6A993595844E1613B49B474D6E3B4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BF692A65-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BF692A65-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Category:	dropped
Size (bytes):	28120
Entropy (8bit):	1.9093964950608238
Encrypted:	false
SSDEEP:	96:rNZGQA6GBSljh2BW4MIlKPmIOH1KPmDlPmIXgpr:rNZGQA6Gkljh2BW4MIlKOIc1KOZOIQr
MD5:	DD41FB0A5E33BB3831AD3FF333D560D3
SHA1:	EF4A5E9DACEDDDEFF2E6D0D8BD0AA575F0F5223E
SHA-256:	CFE343C85BADE722FE4C6CD48C576173AAAA6617CE63EB02B276E2D08F3A2A3B
SHA-512:	3D6022539DAB8848F978C06B9D0D48D9541A5215CD26907C4A6B774C1D443AD70CD5245A860104E9E484072B33374BA9721C1A49151290F73E47524CB79785DE
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BF692A67-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28164
Entropy (8bit):	1.927016630884296
Encrypted:	false
SSDEEP:	96:rPZwQF63BSZje2WWtM6VuX9Z/n3vPwVuXi9Z/n3vA4A:rPZwQF63kZje2WWtM6VmDPvYVmiDPvRA
MD5:	40D370F27939E2349B750DFFD06F88E7
SHA1:	C9D7F691C6686D22246313915656A05AA7C2F77B
SHA-256:	1E43B85064E78FB8BEE17184B34C1B47A2143EBE4905D53C5650B5486D3E89D6
SHA-512:	7C3A2184D98FD608DC336E666516F47BC70B694105FAE92DD9106BEAF5E84A4BFC77A1E66C6902F95DE809E2DAA9780C48F6D303CB384B2977CFB1E33B77B3 3
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CDCCBAD7-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28152
Entropy (8bit):	1.9240152253776737
Encrypted:	false
SSDEEP:	192:rhZiQ26SxkVjXV2VWfMXgxG1fV7BzHlAi1fV7BTA:rnPBSixXMsUwGFxrzFxO
MD5:	B2E71E580093535DB184380A68367272
SHA1:	F980CD6B05440BF4B0671288895689EBFBDEB2CB
SHA-256:	17AC595F46F8556684A1397CBBB4C63224C74083E0B8F0E80428C42006371412
SHA-512:	D681DD25A6685B73C081866AB3450B7EC7695AAD39359D3656466E5A144AB0F491A4AC492846E82819E7AD3475A24FBBF5C681A2C5A135D046518D7D5B9F2D6
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CDCCBAD9-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27580
Entropy (8bit):	1.9114557863672967
Encrypted:	false
SSDEEP:	96:ryZZQu6ABSbj62yW9MZdbPRchG9iflbPRchG9aoCA:ryZZQu6Akbj62yW9MZdbrClbrMoCA
MD5:	4312B662D19AD293677065294986C2E1
SHA1:	1F8517251DBF1A1042A1614CFB5487576FA96CA3
SHA-256:	9AC7298D22034FF871E5FF910BF7A222CCC854480A4FB569E77FA23EEE897770
SHA-512:	7520357BCEE5EBBCD8FE65785884CDB9BC1BAD9C036B411E28D47431A9B97A690407D7132AB42ABE50B1554558C498597D8EA7944897B0EA909779B6EB6AAB3 1

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CDCCBAD9-AC7A-11EB-90E5-ECF4BB570DC9}.dat	
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\ErrorPageTemplate[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):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	.....JFIF.....d.d.....Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\bullet[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):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\down[1]	
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t.,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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:	downloaded
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:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
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\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:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
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\4PB7FJMT\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\http_404[1]	
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ErrorPageTemplate[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):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ErrorPageTemplate[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):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ErrorPageTemplate[2]	
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	dropped
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Preview:	......JFIF.....d.d......Ducky.....P......Adobe.d..... ....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.:j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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..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\B87Z87FM\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\errorPageStrings[1]	
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
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\B87Z87FM\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:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
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\B87Z87FM\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\B87Z87FM\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\httpErrorPagesScripts[2]	
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
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\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
IE Cache URL:	res://ieframe.dll/http_404.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http_404[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\info_48[1]	
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0.."/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v..:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.".. ....}!$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a... .N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,...3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\info_48[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0.."/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v..:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.".. ....}!$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a... .N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,...3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\ErrorPageTemplate[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):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	dropped
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Preview:	......JFIF.....d.d......Ducky.....P......Adobe.d..... .....W..... .....Qa.....?.....%.....x......s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\bullet[1]	
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

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..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:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
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:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\httpErrorPagesScripts[1]	
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
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\NUEPGTR9\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..\|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..l{.n...../....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~."....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\ErrorPageTemplate[1]	
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	dropped
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Preview:	......JFIF.....d.d......Ducky.....P......Adobe.d..... ....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\bullet[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):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

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:	downloaded
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
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\errorPageStrings[1]	
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
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\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:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
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\PEJLKQA8\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\info_48[1]	
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.".. ....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a... .N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

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):	89
Entropy (8bit):	4.440534734931472
Encrypted:	false
SSDEEP:	3:oVXUWWwdfHyT498JOGXnEWWwdfHyu7n:o9URCO49qERCP
MD5:	8FF4370F22C0CE2351DA947BE6F83F5B
SHA1:	FDF569D73F3FFD3F570F647307D6B917C27A9B41
SHA-256:	FDC14D2864207C5D9365DF8E3EB6502A65FFE051DC60D95802E7AF839222316F
SHA-512:	9CA7256AA9B361D687C16E72752A3C05EAC378E512A332A74C00AB9F0CF99A412666BF974F717934AC5D42032F86619FB8268DD7F910A52B926669BE0C99578C
Malicious:	false
Preview:	[2021/05/03 18:48:22.538] Latest deploy version: ..[2021/05/03 18:48:22.538] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF036A3D1EB4248F1E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40089
Entropy (8bit):	0.6599359687427162
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+bVHuVsvnjN3vnjNovnjNl:kBqoxKAuqR+bVHuVsvnjhvnjivnj3
MD5:	FF2D15E011E0496306B6C2414AB0B8CC
SHA1:	2906B71E01D3B84C3A349A5BB141579B9881D7B9
SHA-256:	E8DA3049827E46B694E8BBDDD06CB5DEEC783E01A683355B74D98D4ED7B78ABB
SHA-512:	BC77343357EDFD93D7734638ED8D94AFC5F93FD981CA5C1BF0F1A742200AD4410FBC13E3F3BB55F3F7419C6C1289D9639EF8F6FF7423C993E7CAB4CA2E3A805
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF0A1D9E093A9500C1.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40169
Entropy (8bit):	0.6772971799557037
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+9l9L9p9Y979u/N+nlji/N+nlx/N+nlC:kBqoxKAuqR+npLCJgl+l+l+lxl+lC
MD5:	160079EFD579CA666BE735C08F26C445
SHA1:	1806885C8CA36C4CDF7794EBDC30389DE3237329
SHA-256:	D9A217BC6B4A301CD000FE5100157868A11F35DD60A6066E84CE97C48D909135
SHA-512:	B988E463C1258F77A3B40D7EBFE0D01BB0AB69AA3C5E5FDB1659A38B94F13F112D2C2DCDC9F16BDB78DCB67950DE51484E1ABF908F45F26C239B2A75A14980BC
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF183688B2D13937F7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DF183688B2D13937F7.TMP	
File Type:	data
Category:	dropped
Size (bytes):	40201
Entropy (8bit):	0.6811893827704737
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+5XF03SuX9Z/n3vbuX9Z/n3v8uX9Z/n3vp:kBqoxKAuqR+5XF03SmDPvbmDPv8mDPvp
MD5:	27BB594A0AB53DD29A7E9CDB971620AD
SHA1:	72E143229D158D7C83B8664C454B548FA5AD2B87
SHA-256:	932489B48044D1A6D882E08888F8729273C08E074363682C87CAA9FACA075D9D
SHA-512:	40917888B0935FE1276A55A18E8D69BFB956D78186B109E1F4428F4BA43482F8F2F5E3B182155832C5A50F6272250E835E8E8C68BAB0EECD7271715CD8FD9A70
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF187EAA56E17D73EA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.6016360207526511
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lobr9lobr9lWbev:kBqoIg+0
MD5:	914561B0C688E8E1CA14C67499BE30C2
SHA1:	5C448977B3168081D531995338AAF0D60F9B00C7
SHA-256:	6B26353DE2521CC4461700595A9AB0D43B9EFE720935303C8204F57094646BC9
SHA-512:	DCD826769FF92EF0AEA11C152A471DE2CEC1BCF7F7290BEE23F36C67768485543E9CE6F00D153EE918BF9B0D9D739BCB607267A1FF35AAF770020F6E386EEC D
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF436970D6C9CDDC13.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.601268923597091
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loM9loc9lWodv5qII6/I6t:kBqoI3Rob5Bt
MD5:	77B34D67FC181C06D52989A09253DBCA
SHA1:	0CA09CAEA3B28D8D2118D22BB0F60DACDE737A56
SHA-256:	DC8DC05DD69E6D108C3E1FC75BBCFE68EDAD675619EB9E5D60CB5E25B99FFD8D
SHA-512:	21D7B9A214CA1B89104CBC5589C1D86651AD748634769663AAAB7FA71431BA36C1BC1AB6CE3A0EB245F5545FD00DBDD114858EE098DAE2CFAC2837C54F3784 A0
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF4827C4CB6E557F67.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.6022427977290185
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loS9loC9lWtMc19G:kBqoIdbtD1Q
MD5:	13A5C0F618708CA28DF68FD701769E5C
SHA1:	694068741D15485FCFDBC5A35A22954FC3146161
SHA-256:	D60BADA94C131DEBB03E213A7306E8C2ED86600FE0151B4DB43F9713D2612A14

C:\Users\user\AppData\Local\Temp\~DF4827C4CB6E557F67.TMP

SHA-512:	31ACFD9D0E04D2A5D7E677F2AC2C56D2867DB59ECC9A230A57FDDDE5E88C009701C4ADF221957A9D177BA457BD8B12CEACEFAB25976E98789708E576A3885 6E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF712A270B72970A19.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40105
Entropy (8bit):	0.6634934338478001
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+xvdc/KKPmIMKPmIfKPmIw:kBqoxKAuqR+xvdc/KKOIMKOIfKOIw
MD5:	A222915BA4257C6D1EB386FECB056DC6
SHA1:	C6BBC1049D55CB4C6824EA9BB7687AC2F06B3103
SHA-256:	99AF70584489BEC168813A14F24E4AC44D04FD2338AA21AF033950B59F3E499B
SHA-512:	591C89D6A22B0CBD5878FCED2B91F4B5B2E7134C7C46F769FC6B096CF7AADAF7D332A63CF6BE3A94D7A6754DC2EA3E402E3261FA482D8C9DADD94362F6650 52
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF7FEBD80971BE8B6A.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40177
Entropy (8bit):	0.6755040498857002
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+w2st2PG1fV7BzbG1fV7BzQG1fV7Bz9:kBqoxKAuqR+w2st2PGFxNGFxqGFxH
MD5:	1E1D9A17053F05ED7918C93FACB955B1
SHA1:	D6EB7A136B1CF8A73D0B620DD7DCC754A835EDA6
SHA-256:	343C1B870724E97FA3E8BB51F5C6005F95EB7CF49D0980CD47C8874160DECEA9
SHA-512:	E959A20BCAC14030042AA508C4E5C16E39B4E363A5C71146615D8711F9B6C6056BD01658BCA0357036EB9B73AB45CC19CA75CA044A8CDF8E0DF51650038FC53 E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE60F766B8C74F7D6.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40057
Entropy (8bit):	0.6519938493574535
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+Jn1kH6bPRchG9VKbPRchG9bbPRchG9s:kBqoxKAuqR+Jn1kH6brbKbrpbrK
MD5:	5559F80F8E342C6FECAC7491773371EF
SHA1:	50FE132B31270D9638F5E6B45A03003AD47A3F75
SHA-256:	8BF42482148F7407571C8F04A19285EF5047F7DF09EA55639B0C048E9E8405EC
SHA-512:	A764381138313CFDAB5FC17232316E4D6E03213C2C2258D44D8FC97F73B57A54C4BAA060354F68EA01DA0A93BE48D56BE0A9444610948FF63C766760C9EA8F5E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.133421258123313
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:	block.dll
File size:	312832
MD5:	5a7c87dab250cee78ce63ac34117012b
SHA1:	554c4ccf2341182768d475087d8a8bcfaa525a12
SHA256:	8a26c32848c9ea085505359f67927d1a744ec07303ed0013e592eca6b4df4790
SHA512:	3b4bd7963e3c397618562708064674bd2418f5cab71ce861986efa3bcd14fa6b0155daece10b9a7ad3fe0f7fac6fdfd693b4ac2451f4eaabb30ba8253286b7ed
SSDEEP:	6144:92dsJtFrYUZZqrS6HtYP612U8ZIbBmWMOzWb/0:9SsJtFrYJS6NYy123IMWLz5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Rich.....PE..L....Hn`.....!.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1033bd2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x606E48DF [Thu Apr 8 00:05:51 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	1b129b745ed786ce1fe8186651a3c22d

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F36F0D6BA57h
call 00007F36F0D71962h
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+0Ch]
call 00007F36F0D6B941h

Instruction
pop ecx
pop ebp
retn 000Ch
mov eax, 0104A110h
ret
mov eax, dword ptr [01151140h]
push esi
push 00000014h
pop esi
test eax, eax
jne 00007F36F0D6BA59h
mov eax, 00000200h
jmp 00007F36F0D6BA58h
cmp eax, esi
jnl 00007F36F0D6BA59h
mov eax, esi
mov dword ptr [01151140h], eax
push 00000004h
push eax
call 00007F36F0D711BBh
pop ecx
pop ecx
mov dword ptr [01150120h], eax
test eax, eax
jne 00007F36F0D6BA70h
push 00000004h
push esi
mov dword ptr [01151140h], esi
call 00007F36F0D711A2h
pop ecx
pop ecx
mov dword ptr [01150120h], eax
test eax, eax
jne 00007F36F0D6BA57h
push 0000001Ah
pop eax
pop esi
ret
xor edx, edx
mov ecx, 0104A110h
jmp 00007F36F0D6BA57h
mov eax, dword ptr [01150120h]
mov dword ptr [edx+eax], ecx
add ecx, 20h
add edx, 04h
cmp ecx, 0104A390h
jl 00007F36F0D6BA3Ch
push FFFFFFFEh
pop esi
xor edx, edx
mov ecx, 0104A120h
push edi
mov eax, edx
sar eax, 05h
mov eax, dword ptr [01150020h+eax*4]
mov edi, edx
and edi, 1Fh
shl edi, 06h
mov eax, dword ptr [edi+eax]
cmp eax, FFFFFFFFh
je 00007F36F0D6BA5Ah
cmp eax, esi
je 00007F36F0D6BA56h
test eax, eax

Instruction
jne 00007F36F0D6BA54h

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [ASM] VS2008 build 21022 • [LNK] VS2008 build 21022 • [RES] VS2008 build 21022 • [EXP] VS2008 build 21022 • [IMP] VS2008 SP1 build 30729 • [C++] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x49f60	0x54	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4959c	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x152000	0x388	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x153000	0x10d0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11f0	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x9e10	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1a8	.text
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	0x48fb4	0x49000	False	0.632240608947	data	6.19236668836	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x4a000	0x107148	0x1000	False	0.2314453125	data	2.33342954195	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x152000	0x388	0x400	False	0.3984375	data	3.01615246914	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x153000	0x1d08	0x1e00	False	0.478645833333	data	4.6094977131	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x152058	0x330	data	English	United States

Imports

DLL	Import
KERNEL32.dll	TlsAlloc, TlsSetValue, VirtualProtectEx, FindFirstChangeNotificationW, CompareStringW, CompareStringA, CreateFileA, GetTimeZoneInformation, SetStdHandle, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, CloseHandle, GetLocaleInfoW, HeapSize, SetFilePointer, IsValidLocale, EnumSystemLocalesA, GetLocaleInfoA, GetUserDefaultLCID, GetDateFormatA, GetTimeFormatA, GetStringTypeW, GetStringTypeA, HeapAlloc, GetCurrentThreadId, GetCommandLineA, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, FatalAppExitA, HeapFree, VirtualFree, VirtualAlloc, HeapReAlloc, HeapCreate, HeapDestroy, GetModuleHandleW, Sleep, GetProcAddress, ExitProcess, WriteFile, GetModuleFileNameA, TlsGetValue, TlsFree, InterlockedIncrement, SetLastError, GetLastError, InterlockedDecrement, GetCurrentThread, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, InitializeCriticalSectionAndSpinCount, RtlUnwind, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, SetConsoleCtrlHandler, FreeLibrary, InterlockedExchange, LoadLibraryA, GetConsoleCP, GetConsoleMode, FlushFileBuffers, LCMapStringA, MultiByteToWideChar, LCMapStringW, SetEnvironmentVariableA
snmpapi.dll	SnmpSvcGetUptime, SnmpSvcSetLogLevel, SnmpSvcSetLogType, SnmpUtilAsnAnyCpy, SnmpUtilIdsToA, SnmpUtilMemAlloc, SnmpUtilMemFree, SnmpUtilMemReAlloc, SnmpUtilAsnAnyFree, SnmpUtilDbgPrint, SnmpUtilOctetsCmp, SnmpUtilOctetsNCmp, SnmpUtilOidAppend, SnmpUtilOidCmp, SnmpUtilOidCpy, SnmpUtilOidFree, SnmpUtilVarBindFree, SnmpUtilVarBindListCpy, SnmpUtilVarBindListFree

Exports

Name	Ordinal	Address
Pape1	1	0x103343e
Riverslow	2	0x103328b

Version Infos

Description	Data
LegalCopyright	Equalher Corporation. All rights reserved
InternalName	Period
FileVersion	3.4.8.182
CompanyName	Equalher Corporation Doublemolecule
ProductName	Equalher Size self
ProductVersion	3.4.8.182
FileDescription	Equalher Size self
OriginalFilename	How.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 87

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 18:47:14.766761065 CEST	49721	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:14.766959906 CEST	49722	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:14.891196012 CEST	80	49722	34.86.224.8	192.168.2.5
May 3, 2021 18:47:14.891220093 CEST	80	49721	34.86.224.8	192.168.2.5
May 3, 2021 18:47:14.891552925 CEST	49722	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:14.892385006 CEST	49722	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:14.892384052 CEST	49721	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:15.058485031 CEST	80	49722	34.86.224.8	192.168.2.5
May 3, 2021 18:47:15.634268045 CEST	80	49722	34.86.224.8	192.168.2.5
May 3, 2021 18:47:15.634433985 CEST	49722	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:15.638557911 CEST	49722	80	192.168.2.5	34.86.224.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 18:47:15.679776907 CEST	49724	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:15.680658102 CEST	49723	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:15.762906075 CEST	80	49722	34.86.224.8	192.168.2.5
May 3, 2021 18:47:15.803977966 CEST	80	49724	34.86.224.8	192.168.2.5
May 3, 2021 18:47:15.804167032 CEST	49724	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:15.804209948 CEST	80	49723	34.86.224.8	192.168.2.5
May 3, 2021 18:47:15.804286957 CEST	49723	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:15.804673910 CEST	49724	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:15.970056057 CEST	80	49724	34.86.224.8	192.168.2.5
May 3, 2021 18:47:16.549617052 CEST	80	49724	34.86.224.8	192.168.2.5
May 3, 2021 18:47:16.549760103 CEST	49724	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:16.550539017 CEST	49724	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:16.674575090 CEST	80	49724	34.86.224.8	192.168.2.5
May 3, 2021 18:47:17.380839109 CEST	49721	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:17.615365982 CEST	49723	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:59.645054102 CEST	49728	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:59.645824909 CEST	49729	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:59.769587994 CEST	80	49729	34.86.224.8	192.168.2.5
May 3, 2021 18:47:59.770083904 CEST	80	49728	34.86.224.8	192.168.2.5
May 3, 2021 18:47:59.770087004 CEST	49729	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:59.770190001 CEST	49728	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:59.770210028 CEST	49729	80	192.168.2.5	34.86.224.8
May 3, 2021 18:47:59.937794924 CEST	80	49729	34.86.224.8	192.168.2.5
May 3, 2021 18:48:00.452465057 CEST	49730	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:00.452893019 CEST	49731	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:00.513370991 CEST	80	49729	34.86.224.8	192.168.2.5
May 3, 2021 18:48:00.513503075 CEST	49729	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:00.518239021 CEST	49729	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:00.576894999 CEST	80	49731	34.86.224.8	192.168.2.5
May 3, 2021 18:48:00.576932907 CEST	80	49730	34.86.224.8	192.168.2.5
May 3, 2021 18:48:00.577028990 CEST	49731	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:00.577064037 CEST	49730	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:00.591386080 CEST	49731	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:00.643784046 CEST	80	49729	34.86.224.8	192.168.2.5
May 3, 2021 18:48:00.757878065 CEST	80	49731	34.86.224.8	192.168.2.5
May 3, 2021 18:48:01.351161003 CEST	80	49731	34.86.224.8	192.168.2.5
May 3, 2021 18:48:01.351258039 CEST	49731	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:01.357287884 CEST	49731	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:01.481477022 CEST	80	49731	34.86.224.8	192.168.2.5
May 3, 2021 18:48:01.666564941 CEST	49728	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:02.654160976 CEST	49730	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:23.810090065 CEST	49739	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:23.810103893 CEST	49738	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:23.933738947 CEST	80	49739	34.86.224.8	192.168.2.5
May 3, 2021 18:48:23.933774948 CEST	80	49738	34.86.224.8	192.168.2.5
May 3, 2021 18:48:23.933928967 CEST	49739	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:23.933994055 CEST	49738	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:23.936448097 CEST	49739	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:24.102051020 CEST	80	49739	34.86.224.8	192.168.2.5
May 3, 2021 18:48:24.354640961 CEST	49741	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:24.354646921 CEST	49740	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:24.479403019 CEST	80	49741	34.86.224.8	192.168.2.5
May 3, 2021 18:48:24.479603052 CEST	49741	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:24.480334044 CEST	49741	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:24.480357885 CEST	80	49740	34.86.224.8	192.168.2.5
May 3, 2021 18:48:24.480648994 CEST	49740	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:24.645802975 CEST	80	49741	34.86.224.8	192.168.2.5
May 3, 2021 18:48:24.702848911 CEST	80	49739	34.86.224.8	192.168.2.5
May 3, 2021 18:48:24.703027964 CEST	49739	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:24.710391045 CEST	49739	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:24.834032059 CEST	80	49739	34.86.224.8	192.168.2.5
May 3, 2021 18:48:25.221971035 CEST	80	49741	34.86.224.8	192.168.2.5
May 3, 2021 18:48:25.222157001 CEST	49741	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:25.223335028 CEST	49741	80	192.168.2.5	34.86.224.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 18:48:25.348866940 CEST	80	49741	34.86.224.8	192.168.2.5
May 3, 2021 18:48:25.779598951 CEST	49738	80	192.168.2.5	34.86.224.8
May 3, 2021 18:48:26.596709013 CEST	49740	80	192.168.2.5	34.86.224.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 18:46:12.911582947 CEST	61805	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:12.963943958 CEST	53	61805	8.8.8.8	192.168.2.5
May 3, 2021 18:46:13.134573936 CEST	54795	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:13.191581011 CEST	53	54795	8.8.8.8	192.168.2.5
May 3, 2021 18:46:15.593848944 CEST	49557	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:15.642363071 CEST	53	49557	8.8.8.8	192.168.2.5
May 3, 2021 18:46:16.634701014 CEST	61733	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:16.688988924 CEST	53	61733	8.8.8.8	192.168.2.5
May 3, 2021 18:46:17.805114985 CEST	65447	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:17.856762886 CEST	53	65447	8.8.8.8	192.168.2.5
May 3, 2021 18:46:18.751509905 CEST	52441	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:18.804245949 CEST	53	52441	8.8.8.8	192.168.2.5
May 3, 2021 18:46:19.863552094 CEST	62176	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:19.915088892 CEST	53	62176	8.8.8.8	192.168.2.5
May 3, 2021 18:46:20.678106070 CEST	59596	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:20.726871014 CEST	53	59596	8.8.8.8	192.168.2.5
May 3, 2021 18:46:22.204437971 CEST	65296	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:22.258414030 CEST	53	65296	8.8.8.8	192.168.2.5
May 3, 2021 18:46:23.192095041 CEST	63183	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:23.249205112 CEST	53	63183	8.8.8.8	192.168.2.5
May 3, 2021 18:46:23.490803957 CEST	60151	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:23.548022985 CEST	53	60151	8.8.8.8	192.168.2.5
May 3, 2021 18:46:24.179348946 CEST	56969	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:24.232636929 CEST	53	56969	8.8.8.8	192.168.2.5
May 3, 2021 18:46:44.178430080 CEST	55161	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:44.244565010 CEST	53	55161	8.8.8.8	192.168.2.5
May 3, 2021 18:46:52.540476084 CEST	59736	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:52.541141033 CEST	51058	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:52.541220903 CEST	52636	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:52.590992928 CEST	53	59736	8.8.8.8	192.168.2.5
May 3, 2021 18:46:52.592092037 CEST	53	52636	8.8.8.8	192.168.2.5
May 3, 2021 18:46:52.594736099 CEST	53	51058	8.8.8.8	192.168.2.5
May 3, 2021 18:46:55.826813936 CEST	54757	53	192.168.2.5	8.8.8.8
May 3, 2021 18:46:55.880345106 CEST	53	54757	8.8.8.8	192.168.2.5
May 3, 2021 18:46:59.982454062 CEST	49992	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:00.041860104 CEST	53	49992	8.8.8.8	192.168.2.5
May 3, 2021 18:47:01.451494932 CEST	60075	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:01.511352062 CEST	53	60075	8.8.8.8	192.168.2.5
May 3, 2021 18:47:11.411353111 CEST	55016	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:11.470191002 CEST	53	55016	8.8.8.8	192.168.2.5
May 3, 2021 18:47:14.400002956 CEST	64345	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:14.752608061 CEST	53	64345	8.8.8.8	192.168.2.5
May 3, 2021 18:47:15.309784889 CEST	57128	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:15.662859917 CEST	53	57128	8.8.8.8	192.168.2.5
May 3, 2021 18:47:22.395927906 CEST	54791	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:22.457612991 CEST	53	54791	8.8.8.8	192.168.2.5
May 3, 2021 18:47:41.384895086 CEST	50463	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:41.450936079 CEST	53	50463	8.8.8.8	192.168.2.5
May 3, 2021 18:47:42.381957054 CEST	50463	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:42.443730116 CEST	53	50463	8.8.8.8	192.168.2.5
May 3, 2021 18:47:43.381807089 CEST	50463	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:43.451868057 CEST	53	50463	8.8.8.8	192.168.2.5
May 3, 2021 18:47:45.400933981 CEST	50463	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:45.461411953 CEST	53	50463	8.8.8.8	192.168.2.5
May 3, 2021 18:47:49.398412943 CEST	50463	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:49.458760023 CEST	53	50463	8.8.8.8	192.168.2.5
May 3, 2021 18:47:54.439112902 CEST	50394	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 18:47:54.489809036 CEST	53	50394	8.8.8.8	192.168.2.5
May 3, 2021 18:47:58.025618076 CEST	58530	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:58.084348917 CEST	53	58530	8.8.8.8	192.168.2.5
May 3, 2021 18:47:59.312661886 CEST	53813	53	192.168.2.5	8.8.8.8
May 3, 2021 18:47:59.627646923 CEST	53	53813	8.8.8.8	192.168.2.5
May 3, 2021 18:48:00.365937948 CEST	63732	53	192.168.2.5	8.8.8.8
May 3, 2021 18:48:00.423192978 CEST	53	63732	8.8.8.8	192.168.2.5
May 3, 2021 18:48:03.370284081 CEST	57344	53	192.168.2.5	8.8.8.8
May 3, 2021 18:48:03.432059050 CEST	53	57344	8.8.8.8	192.168.2.5
May 3, 2021 18:48:08.743448973 CEST	54450	53	192.168.2.5	8.8.8.8
May 3, 2021 18:48:08.814914942 CEST	53	54450	8.8.8.8	192.168.2.5
May 3, 2021 18:48:22.168788910 CEST	59261	53	192.168.2.5	8.8.8.8
May 3, 2021 18:48:22.230268955 CEST	53	59261	8.8.8.8	192.168.2.5
May 3, 2021 18:48:23.448160887 CEST	57151	53	192.168.2.5	8.8.8.8
May 3, 2021 18:48:23.779263020 CEST	53	57151	8.8.8.8	192.168.2.5
May 3, 2021 18:48:24.284624100 CEST	59413	53	192.168.2.5	8.8.8.8
May 3, 2021 18:48:24.341797113 CEST	53	59413	8.8.8.8	192.168.2.5
May 3, 2021 18:48:30.199759960 CEST	60516	53	192.168.2.5	8.8.8.8
May 3, 2021 18:48:30.248704910 CEST	53	60516	8.8.8.8	192.168.2.5
May 3, 2021 18:48:31.403764009 CEST	51649	53	192.168.2.5	8.8.8.8
May 3, 2021 18:48:31.460863113 CEST	53	51649	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 18:47:14.400002956 CEST	192.168.2.5	8.8.8.8	0x65c5	Standard query (0)	app.bubole inov.com	A (IP address)	IN (0x0001)
May 3, 2021 18:47:15.309784889 CEST	192.168.2.5	8.8.8.8	0x3c44	Standard query (0)	app.bubole inov.com	A (IP address)	IN (0x0001)
May 3, 2021 18:47:59.312661886 CEST	192.168.2.5	8.8.8.8	0xcc5f	Standard query (0)	chat.billi onady.com	A (IP address)	IN (0x0001)
May 3, 2021 18:48:00.365937948 CEST	192.168.2.5	8.8.8.8	0x410e	Standard query (0)	chat.billi onady.com	A (IP address)	IN (0x0001)
May 3, 2021 18:48:23.448160887 CEST	192.168.2.5	8.8.8.8	0x57b8	Standard query (0)	app3.maint orna.com	A (IP address)	IN (0x0001)
May 3, 2021 18:48:24.284624100 CEST	192.168.2.5	8.8.8.8	0xe07f	Standard query (0)	app3.maint orna.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 18:47:00.041860104 CEST	8.8.8.8	192.168.2.5	0x44da	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 18:47:14.752608061 CEST	8.8.8.8	192.168.2.5	0x65c5	No error (0)	app.bubole inov.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 18:47:15.662859917 CEST	8.8.8.8	192.168.2.5	0x3c44	No error (0)	app.bubole inov.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 18:47:59.627646923 CEST	8.8.8.8	192.168.2.5	0xcc5f	No error (0)	chat.billi onady.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 18:48:00.423192978 CEST	8.8.8.8	192.168.2.5	0x410e	No error (0)	chat.billi onady.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 18:48:23.779263020 CEST	8.8.8.8	192.168.2.5	0x57b8	No error (0)	app3.maint orna.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 18:48:24.341797113 CEST	8.8.8.8	192.168.2.5	0xe07f	No error (0)	app3.maint orna.com		34.86.224.8	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- app.buboleinov.com
- chat.billionady.com
- app3.maintorna.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49722	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:47:14.892385006 CEST	1455	OUT	GET /u9JBOXOyCt1J/Cqk3pF0_2B2/evko0P1iOLkfYu/tE8kijPwXl6fpTUvGY0L0/uKSRiZsz1TrVOn7H/lYNbZbDXpFfEDld/SZEdzjQiJ4mBJjhxQf/IliemLK4E/fjiV_2FMKJMbBd5i_2F6/V_2Fz7Tym384w5xw_2F/kNwSikyIWBdKPim7R9vG Wb/gFLpN9hJBqDsa/ZkxxO_2B/g7xuaBcPsCTSbIA7GEQ7zhu/w_2FuzPVom/0RGTspDSMbay7GsRJ/O_2BvpZGrQE s/hpy5azZaVzk/tO8Yj0mAC2rNEA/7Y_2FaW8HQeMqJNFtj5QK/iv0XWUt_2F3/3R 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: app.buboleinov.com Connection: Keep-Alive
May 3, 2021 18:47:15.634268045 CEST	1456	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 16:47:15 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49724	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:47:15.804673910 CEST	1457	OUT	GET /zWr7XKiLQ_2F3QZ2bR/ZuzwfgbmQ/mjgvv5jUliwpj1wMmSf1/mVwZRrRJ02ozj18W4CC/_2FqTc0J0ACZs0Z o0yB15V/UkO_2BhXUEjqi/ylcme0uu/h88DPxTz52fwzk2KiAITqAX/y1YkE9ueOd/NzFODbcfeCN_2B548/9jGMMg _2FjQB/TCcN38_2FLl/w78Mf5LsU18OtD/O9ldbeaIz2YOBBV9govEw/if1bIKJhIzR9fYIT/Dva1E7_2F2LcgBj/3WJFp2Il273 lx9FN_2/B45JK5S6v/rZZWdDOKWu65eMI2rNKK/RAsOHyLCy3eKhZf_2Fm/CD_2FuANPfLuHGjULRoA2Y/Paqy 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: app.buboleinov.com Connection: Keep-Alive
May 3, 2021 18:47:16.549617052 CEST	1458	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 16:47:16 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49729	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:47:59.770210028 CEST	1514	OUT	GET /hPJ75Rz1l0Yg172f0/W92Rc6NrZORu/agJ84T4GWPF/71Su9Jrd5lLrko/1XWo5CLa_2Bx1ycL2fXGF/76IsZupbi6IIIogp/P_2BrqGlfT6Z_2F/9HIF9QL_2Ffn95EjHz/EKpbgAout/m_2FkBfNGzNFhXOxCcqe/1zQKvOOwqE_2B22qrZS/vj3rmMMb_2BsLkd2AZhDC4/602lvjtm6dYcP/dyzgfgBT/A_2BC4eofqol5orEsMEQPWe/zZ6Swnuj_2/FM3kwbNjGbF9dztKO/5Sul25wMK_2F/fSrDDmSQa3P/LwvXQje5tWHJ24/YCtfl_2Bd9Wgni_2B/yKHW 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: chat.billionady.com Connection: Keep-Alive
May 3, 2021 18:48:00.513370991 CEST	1514	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 16:48:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49731	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:48:00.591386080 CEST	1515	OUT	GET /1Z7Zv_2Fo_2BBI/5yyu9xO7U6xQJUAU9LBdU/_2BZsJzv4AW1v4_2/FuBHkCgtXKYNI2J/fjLUpx4yvdGQ9xBWU8/nZ2UCR2Fn/6_2BJUjWbSDTFYEq01IK/G2MuJJozgl6fl_2Bxi6/8WHocMwy1m3c6beo7EybdT/0fZNT0A7jOYrz/ZJgKKaGn/V_2Bc6nIeAMBXcBQSTKS3tl/dRpB7HoFuq/5r0h_2Bic5oCoaHxQ/GZIQmnaYFeN7/lgmkXjg8R1P/o6CJiUeiWxo9TA/Om1BRSx_2BLEYhxw_2B1w/ztx7Xd1V_2BwFgLL/5ttSiFJbfjzPnDR/nMd_2BdWk4HTz_2Ftn/Va7N0lfshKE/mKz 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: chat.billionady.com Connection: Keep-Alive
May 3, 2021 18:48:01.351161003 CEST	1516	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 16:48:01 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49739	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:48:23.936448097 CEST	6350	OUT	GET /cDNEPwBarUn/ROJH1XYkRfSClQ/qONBPlQo8FxG6mQW9Ogcz/u7mo1Dj2PullrRPq/bR_2BFpPLx7OhU9/HJBhAhHBzmstPPDOE1/w6ebBa_2B/KX_2BOm6FIW3gd6Bvbnj/Sh9h8HN_2BONCwGgPQr/IY0nkmO9u18wIpqrmMTW3z/GWi0vHa3h_2Bj/6IH92Uhj/Iom39I56_2BMfY2_2BRDxU0/VfXOZ9_2BQ/hDbFynpSdJTA10_2B/DTN9zUXGBVIL/6pinDdbjTIZ/J8liN5BZT7oU_2/FDetd44m1Cdm74WjgwpWw/7RPnYCrU0gXGaG9w/dolpQdALprU5fVz/g9lnmYz4c/oMbk6u 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: app3.maintorna.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:48:24.702848911 CEST	6352	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 16:48:24 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49741	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:48:24.480334044 CEST	6351	OUT	GET /6r_2FD5QsDWTjJjwzHfBaL/2HYJ2K06UlseV/lZ1msT18/ny_2FHLDol8VG6VjuFqLZ26/y1nZcgTjUQ/HL5Y V0taxU5zFMebw/ouCjKnY1SB67/bctA52f0140/sHpnVH95T_2Fuj/QLIAvGeVws2XTmrrXV3BZ/psxvZSZg2i7jPF 9N/caz3S5QCjepHp3W/l6q5V6Mw_2BHygdAjz/QFWLuSVDY/2iEYyTYQm6wj63ekurFy/nVWvwQ5A_2FY6vAZ0b2/y sxIi7hdttfqNZtbDq2s51/_2FLPh7LrbbPo/JhDaZ4qW/MGAYB_2BvyA3HE7Ywiz/pWy 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: app3.maintorna.com Connection: Keep-Alive
May 3, 2021 18:48:25.221971035 CEST	6352	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 16:48:25 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5720 Parent PID: 5648

General

Start time:	18:46:22
Start date:	03/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\block.dll'
Imagebase:	0xd20000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.352720988.0000000003D28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.352839215.0000000003D28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.352637772.0000000003D28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.299036321.0000000001670000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.352699094.0000000003D28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.352816951.0000000003D28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.352743659.0000000003D28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.352664971.0000000003D28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.352761373.0000000003D28000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4516 Parent PID: 5720

General

Start time:	18:46:22
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\block.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5592 Parent PID: 5720

General

Start time:	18:46:23
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\block.dll,Pape1
Imagebase:	0x1f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.285453583.0000000003F50000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5752 Parent PID: 4516

General

Start time:	18:46:23
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\block.dll',#1
Imagebase:	0x1f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.353402660.0000000005A48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.353461083.0000000005A48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.353493626.0000000005A48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.353527674.0000000005A48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.353601646.0000000005A48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.353567176.0000000005A48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.286919905.0000000003050000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.353611757.0000000005A48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.353343104.0000000005A48000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 4648 Parent PID: 5720

General

Start time:	18:46:26
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\block.dll,Riverslow
Imagebase:	0x1f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000003.294762520.0000000004D50000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5856 Parent PID: 792

General

Start time:	18:47:09
Start date:	03/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff795120000

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

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

Registry Activities

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: 6328 Parent PID: 5856

General

Start time:	18:47:11
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5856 CREDAT:17410 /prefetch:2
Imagebase:	0xa40000
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

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: 6452 Parent PID: 5856

General

Start time:	18:47:13
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5856 CREDAT:17414 /prefetch:2
Imagebase:	0xa40000
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

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: 5708 Parent PID: 792

General

Start time:	18:47:56
Start date:	03/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff795120000
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

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

Registry Activities

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: 5816 Parent PID: 5708

General

Start time:	18:47:57
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5708 CREDAT:17410 /prefetch:2
Imagebase:	0xa40000
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

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: 6100 Parent PID: 5708

General

Start time:	18:47:58
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5708 CREDAT:17414 /prefetch:2
Imagebase:	0xa40000
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

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: 6616 Parent PID: 792

General

Start time:	18:48:21
Start date:	03/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff795120000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596

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

File Activities

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

Registry Activities

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: 6480 Parent PID: 6616

General

Start time:	18:48:21
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:17410 /prefetch:2
Imagebase:	0xa40000
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: 1972 Parent PID: 6616

General

Start time:	18:48:22
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:17414 /prefetch:2
Imagebase:	0xa40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis