ID: 323940
Sample Name: 2020-11-27-ZLoader-DLL-example-01.bin
Cookbook: default.jbs
Time: 22:42:40
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

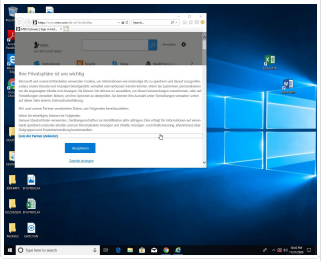
Analysis Report 2020-11-27-ZLoader-DLL-example-01.bin

Overview

General Information

Sample Name:	2020-11-27-ZLoader-DLL-example-01.bin (renamed file extension from bin to dll)
Analysis ID:	323940
MD5:	4a64b13ff53aebb..
SHA1:	7e75f220f6c9e6b..
SHA256:	66ec83aa3631d7..
Tags:	dll SilentNight Silent_Nigh ZLoader

Most interesting Screenshot:



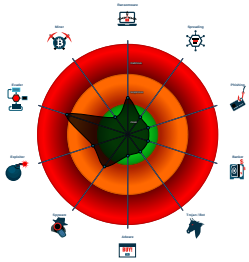
Detection

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Allocates memory in foreign process…
- Contains functionality to inject code …
- Writes to foreign memory regions
- Abnormal high CPU Usage
- Contains functionality to check if a d…
- Contains functionality to check if a w…
- Contains functionality to check the p…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to read the PEB
- Contains functionality which may be…
- Creates a process in suspended mo…
- Detected potential crypto function

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 4748 cmdline: loaddll32.exe 'C:\Users\user\Desktop\2020-11-27-ZLoader-DLL-example-01.dll' MD5: 76E2251D0E9772B9DA90208AD741A205)
  - regsvr32.exe (PID: 4696 cmdline: regsvr32.exe /s C:\Users\user\Desktop\2020-11-27-ZLoader-DLL-example-01.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - msiexec.exe (PID: 2028 cmdline: msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
  - cmd.exe (PID: 3940 cmdline: C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - iexplore.exe (PID: 3868 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
      - iexplore.exe (PID: 5976 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3868 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

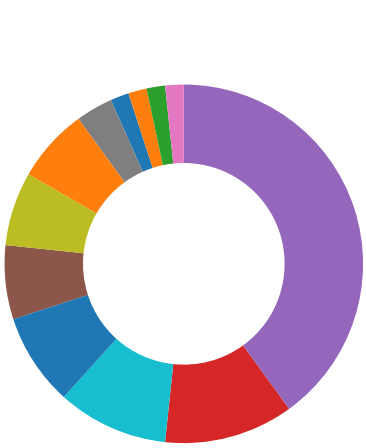
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Contains functionality to inject code into remote processes

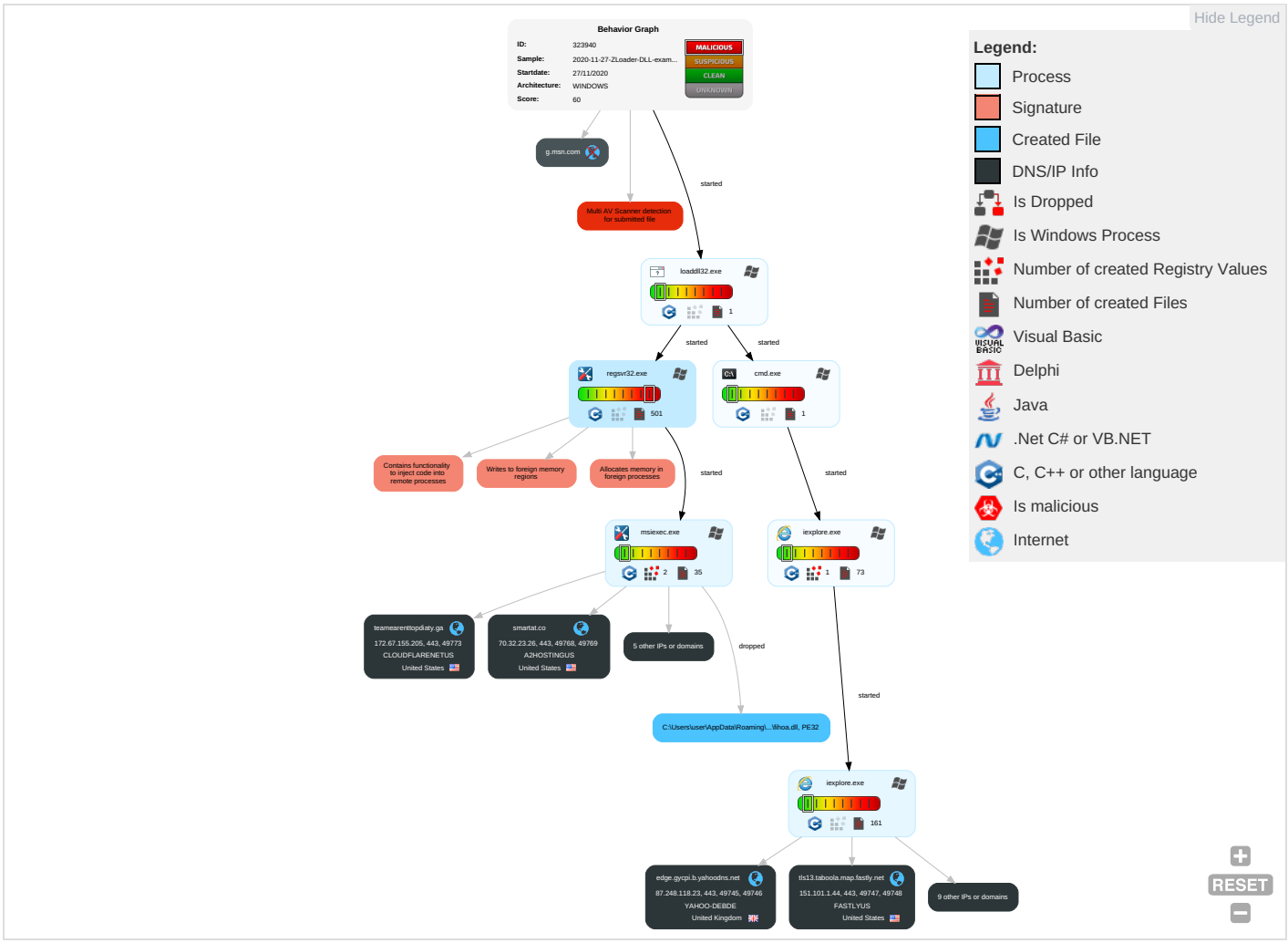
Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	DLL Side-Loading 1	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop c Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	System Information Discovery 2 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

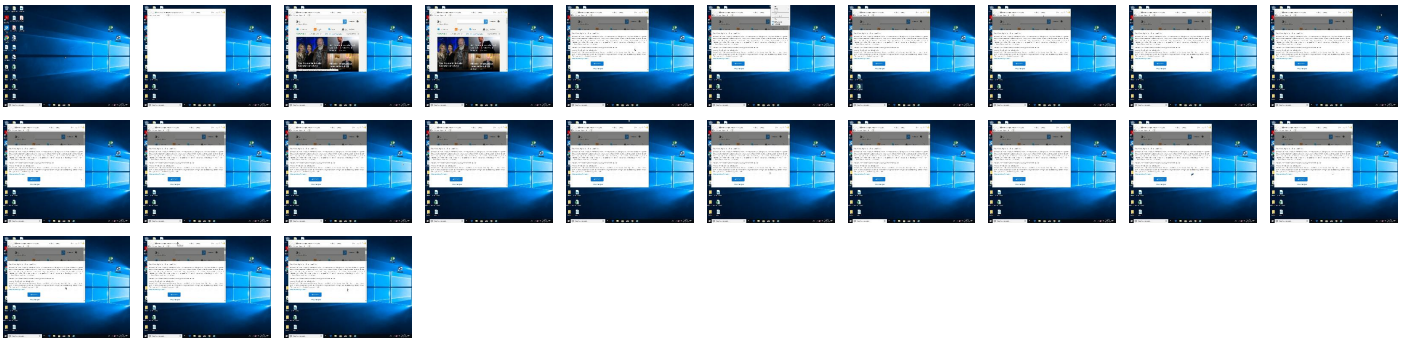
Behavior Graph

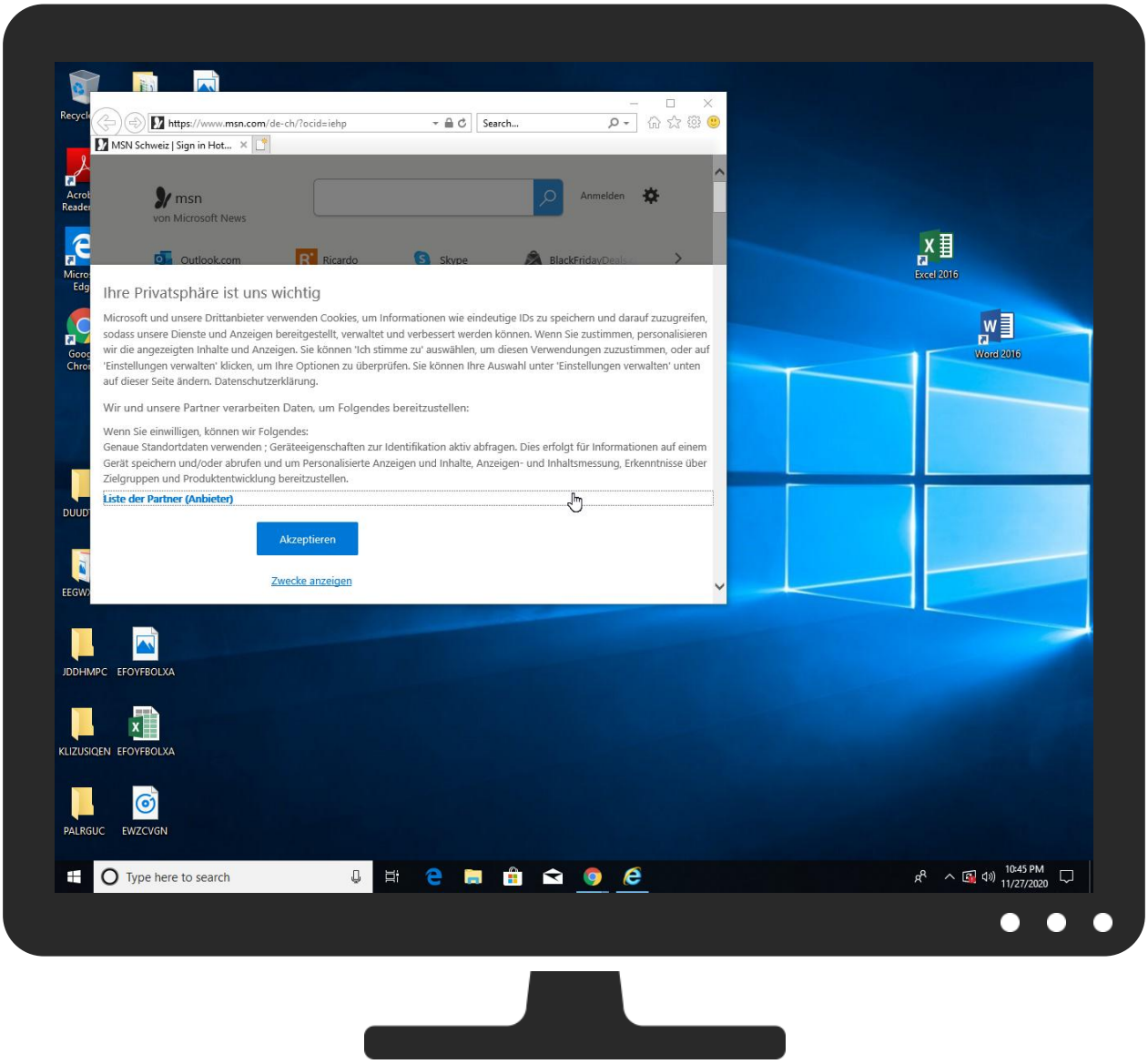


Screenshots

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
2020-11-27-ZLoader-DLL-example-01.dll	12%	Virustotal		Browse
2020-11-27-ZLoader-DLL-example-01.dll	8%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Wigy\fihoa.dll	8%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.msiexec.exe.370000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.regsvr32.exe.6dd90000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
hac3r.com	0%	Virustotal		Browse
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
valitec.co	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.remixd.com/privacy_policy.html	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://www.blackfridaydeals.ch/neuste-angebote?utm_source=ms&utm_campaign=shop-gross	0%	Avira URL Cloud	safe	
http://https://www.blackfridaydeals.ch/elektronik-unterhaltung?utm_source=ms&utm_campaign=infopane-elec	0%	Avira URL Cloud	safe	
http://https://bealion.com/politica-de-cookies	0%	Avira URL Cloud	safe	
http://https://www.gadsme.com/privacy-policy/	0%	Avira URL Cloud	safe	
http://https://portal.eu.numbereight.me/policies-license#software-privacy-notice	0%	Avira URL Cloud	safe	
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	0%	URL Reputation	safe	
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	0%	URL Reputation	safe	
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	0%	URL Reputation	safe	
http://https://www.blackfridaydeals.ch/?utm_source=ms&utm_campaign=topnav	0%	Avira URL Cloud	safe	
http://https://channelpilot.co.uk/privacy-policy	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://www.admo.tv/en/privacy-policy	0%	URL Reputation	safe	
http://https://www.admo.tv/en/privacy-policy	0%	URL Reputation	safe	
http://https://www.admo.tv/en/privacy-policy	0%	URL Reputation	safe	
http://www.fotogestoeber.de	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://www.blackfridaydeals.ch/?utm_source=ms&utm_campaign=mestripe	0%	Avira URL Cloud	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://listonic.com/privacy/	0%	Avira URL Cloud	safe	
http://https://quantyoo.de/datenschutz	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://www.blackfridaydeals.ch/neuste-angebote?utm_source=ms&utm_campaign=shop-trends	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	23.57.80.37	true	false		high
hac3r.com	70.32.23.26	true	false	• 0%, Virustotal, Browse	unknown
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
valitec.co	70.32.23.26	true	false	• 0%, Virustotal, Browse	unknown
teamearenttopdiaty.ga	172.67.155.205	true	false		unknown
empresascreciendobien.com	70.32.23.26	true	false		unknown
hblg.media.net	23.57.80.37	true	false		high
lg3.media.net	23.57.80.37	true	false		high
womtools.com	70.32.23.26	true	false		unknown
smartat.co	70.32.23.26	true	false		unknown
edge.gycpi.b.yahoodns.net	87.248.118.23	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.msn.com	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false		unknown
s.yimg.com	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
g.msn.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high

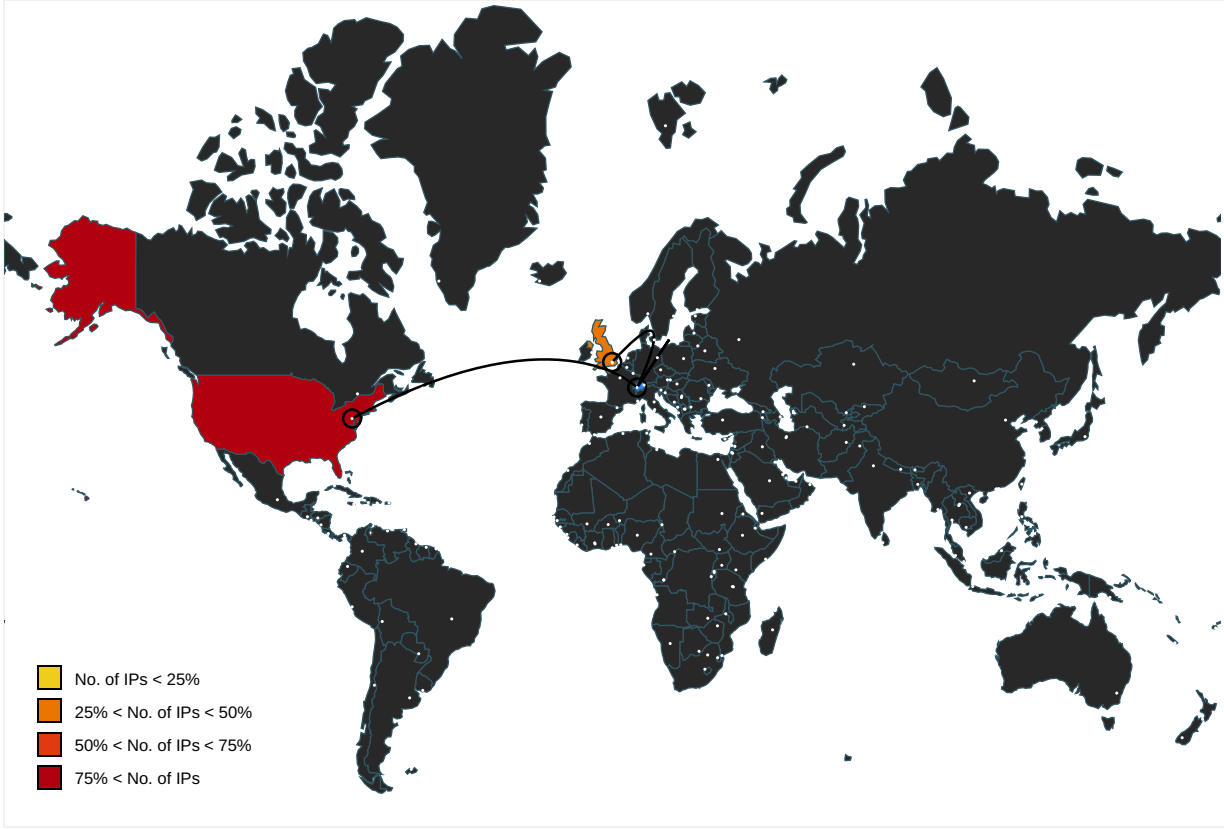
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://searchads.msn.net/.cfm?&&kp=1&	{07A17A1F-3145-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172	de-ch[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/coronareisen	de-ch[1].htm.4.dr	false		high
http://https://www.remixd.com/privacy_policy.html	iab2Data[1].json.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com;Fotos	85-0f8009-68ddb2ab[1].js.4.dr	false	• Avira URL Cloud: safe	low
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_TopMenu&auth=1&wdorigin=msn	de-ch[1].htm.4.dr	false		high
http://https://office.live.com/start/Word.aspx?WT.mc_id=MSN_site;Excel	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://ogp.me/ns/fb#	de-ch[1].htm.4.dr	false		high
http://https://outlook.live.com/mail/deeplink/compose;Kalender	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://res-a.akamaihd.net/__media__/pics/8000/72/941/fallback1.jpg	{07A17A1F-3145-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://https://www.skyscanner.net/g/referrals/v1/cars/home?associateid=API_B2B_19305_00002	de-ch[1].htm.4.dr	false		high
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_Recent&auth=1&wdorigin=msn	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://beap.gemini.yahoo.com/mbclk?bv=1.0.0&es=UMUTI8QGIS_MmDcxCV0LONdevpaNurq1wfWCoP.9WWqQH6Vt	auction[1].htm.4.dr	false		high
http://https://web.vortex.data.msn.com/collect/v1	de-ch[1].htm.4.dr	false		high
http://https://www.office.com/?omkt=de-ch%26WT.mc_id=MSN_site	de-ch[1].htm.4.dr	false		high
http://www.reddit.com/	msapplication.xml4.3.dr	false		high
http://https://www.skype.com/	de-ch[1].htm.4.dr	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	auction[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.blackfridaydeals.ch/neuste-angebote?utm_source=ms&utm_campaign=shop-gross	de-ch[1].htm.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://sp.booking.com/index.html?aid=1589774&label=travelnavlink	de-ch[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/regional	de-ch[1].htm.4.dr	false		high
http://https://onedrive.live.com/?qt=allmyphotos;Aktuelle	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://amzn.to/2TTxhNg	de-ch[1].htm.4.dr	false		high
http://https://www.skype.com/go/onedrivepromo.download?cm_mmc=MSFT_2390_MSN-com	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://client-s.gateway.messenger.live.com	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.brightcom.com/privacy-policy/	iab2Data[1].json.4.dr	false		high
http://https://www.msn.com/de-ch/	de-ch[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/news/other/sch%c3%bcler-15-rast-mit-%c3%bcber-200-km-h-%c3%bcber-autobahn/	de-ch[1].htm.4.dr	false		high
http://https://office.live.com/start/PowerPoint.aspx?WT.mc_id=MSN_site	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	{07A17A1F-3145-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://https://www.awin1.com/cread.php?awinmid=15168&awinaffid=696593&clickref=de-ch-edge-dhp-river	de-ch[1].htm.4.dr	false		high
http://https://www.blackfridaydeals.ch/elektronik-unterhaltung?utm_source=ms&utm_campaign=infopane-elec	de-ch[1].htm.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://bealion.com/politica-de-cookies	iab2Data[1].json.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch	de-ch[1].htm.4.dr	false		high
http://https://sp.booking.com/index.html?aid=1589774&label=dech-prime-verticals-shoppinghub	de-ch[1].htm.4.dr	false		high
http://https://twitter.com/i/notifications;lch	85-0f8009-68ddb2ab[1].js.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.awin1.com/cread.php?awinmid=11518&awinaffid=696593&clickref=dech-edge-dhp-infopa	de-ch[1].htm.4.dr	false		high
http://https://www.gadsme.com/privacy-policy/	iab2Data[1].json.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://portal.eu.numbereight.me/policies-license#software-privacy-notice	iab2Data[1].json.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&http	de-ch[1].htm.4.dr	false		high
http://https://www.sway.com/?WT.mc_id=MSN_site&utm_source=MSN&utm_medium=Topnav&utm_campaign=link;PowerPoin	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.msn.com/de-ch/?ocid=iehp&item=deferred_page%3a1&ignorejs=webcore%2fmodules%2fjsb	de-ch[1].htm.4.dr	false		high
http://www.youtube.com/	msapplication.xml7.3.dr	false		high
http://https://www.msn.com/de-ch/?ocid=iehpQ	{07A17A1F-3145-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://ogp.me/ns#	de-ch[1].htm.4.dr	false		high
http://https://docs.prebid.org/privacy.html	iab2Data[1].json.4.dr	false		high
http://https://ir2.beap.gemini.yahoo.com/mbcsc?bv=1.0.0&es=9MCkPxYGIS9DsbJ8K5XSQqeJgr.yHgIAddEPJ5hfb4YU	auction[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/news/other/gedenktafel-f%c3%bcr-k%c3%b6bi-kuhn-enth%c3%bcllt/ar-BB1bodo5?o	de-ch[1].htm.4.dr	false		high
http://https://onedrive.live.com/?qt=mru;OneDrive-App	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.skype.com/de	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://sp.booking.com/index.html?aid=1589774&label=dech-prime-hp-me	de-ch[1].htm.4.dr	false		high
http://https://srtb.msn.com:443/notify/viewedg?rid=ef8b497139bf46d1a2ac40fcff94f1b9&r=infopane&i=1&	auction[1].htm.4.dr	false		high
http://https://www.skype.com/de/download-skype	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/?wt.mc_id=oo_msn_msnhomepage_header	de-ch[1].htm.4.dr	false		high
http://https://www.blackfridaydeals.ch/?utm_source=ms&utm_campaign=topnav	de-ch[1].htm.4.dr	false	• Avira URL Cloud: safe	unknown
http://www.hotmail.msn.com/pii/ReadOutlookEmail/	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://channelpilot.co.uk/privacy-policy	iab2Data[1].json.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com;OneDrive-App	85-0f8009-68ddb2ab[1].js.4.dr	false	• Avira URL Cloud: safe	low
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.4.dr	false		high
http://www.amazon.com/	msapplication.xml.3.dr	false		high
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_QuickNote&auth=1	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://www.twitter.com/	msapplication.xml5.3.dr	false		high
http://https://office.live.com/start/Excel.aspx?WT.mc_id=MSN_site;Sway	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.admo.tv/en/privacy-policy	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://policies.oath.com/us/en/oath/privacy/index.html	auction[1].htm.4.dr	false		high
http://https://www.bet365affiliates.com/UI/Pages/Affiliates/Affiliates.aspx?ContentPath	iab2Data[1].json.4.dr	false		high
http://https://www.msn.com/de-ch/news/other/das-f%c3%bchrt-zu-unsicherheit-und-willk%c3%bcr-der-plan-von-%c	de-ch[1].htm.4.dr	false		high
http://https://cdn.cookielaw.org/vendorlist/googleData.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.4.dr	false		high
http://https://outlook.com/	de-ch[1].htm.4.dr	false		high
http://https://rover.ebay.com/rover/1/5222-53480-19255-0/1?mpre=https%3A%2F%2Fwww.ebay.ch&campid=533862	de-ch[1].htm.4.dr	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	{07A17A1F-3145-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://https://cdn.cookielaw.org/vendorlist/iabData.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.4.dr	false		high
http://https://www.msn.com/de-ch/homepage/api/pdp/updatepdpdata"	de-ch[1].htm.4.dr	false		high
http://https://cdn.cookielaw.org/vendorlist/iab2Data.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/?qt=mru;Aktuelle	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://cdn.flurry.com/adTemplates/templates/htmls/clips.html"	auction[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/?ocid=iehp	{07A17A1F-3145-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://https://s.yimg.com/lo/api/res/1.2/XxksVvrfxHZk29yD8sVudQ--~A/Zmk9Zml0O3c9NjIyO2g9MzY4O2FwcGlkPWdlbWl	auction[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/news/other/der-vollst%c3%a4ndige-z%c3%bcritipp-adventskalender/ar-BB1bnO4s	de-ch[1].htm.4.dr	false		high
http://www.fotogestoeber.de	de-ch[1].htm.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/homepage/api/modules/fetch"	de-ch[1].htm.4.dr	false		high
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	de-ch[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.blackfridaydeals.ch/?utm_source=ms&utm_campaign=mestripe	de-ch[1].htm.4.dr	false	• Avira URL Cloud: safe	unknown
http://www.nytimes.com/	msapplication.xml3.3.dr	false		high
http://https://web.vortex.data.msn.com/collect/v1/t.gif?name=%27Ms.Webi.PageView%27&ver=%272.1%27&a	de-ch[1].htm.4.dr	false		high
http://https://www.bidstack.com/privacy-policy/	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/en/download/	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://popup.taboola.com/german	auction[1].htm.4.dr	false		high
http://https://listonic.com/privacy/	iab2Data[1].json.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://beap.gemini.yahoo.com/action?bv=1.0.0&es=h1WIJgoGIS.yjATC54OU31VblhZMdH6z8Zk1o.Y3FVvb_do	auction[1].htm.4.dr	false		high
http://https://www.ricardo.ch/?utm_source=msn&utm_medium=affiliate&utm_campaign=msn_mestripe_logo_d	de-ch[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/news/other/je-fr%c3%bcher-desto-besser-die-stadt-z%c3%bcrich-will-die-klei	de-ch[1].htm.4.dr	false		high
http://https://twitter.com/	de-ch[1].htm.4.dr	false		high
http://https://quantyoo.de/datenschutz	iab2Data[1].json.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://outlook.live.com/calendar	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	auction[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.blackfridaydeals.ch/neuste-angebote?utm_source=ms&utm_campaign=shop-trends	de-ch[1].htm.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/#qt=mru	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://api.taboola.com/2.0/json/msn-ch-de-home/recommendations.notify-click?app.type=desktop&ap	auction[1].htm.4.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.155.205	unknown	United States		13335	CLOUDFLARENETUS	false
70.32.23.26	unknown	United States		55293	A2HOSTINGUS	false
87.248.118.23	unknown	United Kingdom		203220	YAHOO-DEBDE	false
151.101.1.44	unknown	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323940
Start date:	27.11.2020
Start time:	22:42:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2020-11-27-ZLoader-DLL-example-01.bin (renamed file extension from bin to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
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:	mal60.evad.winDLL@11/134@16/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 61.2% (good quality ratio 60.9%) • Quality average: 88.1% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 63% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.83.120.32, 204.79.197.203, 204.79.197.200, 13.107.21.200, 92.122.213.231, 92.122.213.187, 65.55.44.109, 23.57.80.37, 23.210.248.85, 51.132.208.181, 152.199.19.161, 51.103.5.159, 2.20.142.209, 2.20.142.210, 20.54.26.129, 52.142.114.176, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, a-0003.a-msedge.net, global.vortex.data.trafficmanager.net, cvision.media.net.edgekey.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, www-msn-com.a-0003.a-msedge.net, a767.dscg3.akamai.net, a1999.dscg2.akamai.net, web.vortex.data.trafficmanager.net, e607.d.akamaiedge.net, web.vortex.data.microsoft.com, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, static-global-s-msn-com.akamaized.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadFile calls found. • Report size getting too big, too many NtSetInformationFile calls found. • Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
70.32.23.26	invoice.xls	Get hash	malicious	Browse	
	invoice.xls	Get hash	malicious	Browse	
	invoice.xls	Get hash	malicious	Browse	
87.248.118.23	http://www.prophecyhour.com	Get hash	malicious	Browse	• us.i1.yimg.com/us.yimg.com/i/yg/img/i/us/ui/join.gif
	http://www.forestforum.co.uk/showthread.php?t=47811&page=19	Get hash	malicious	Browse	• yui.yahooapis.com/2.9.0/build/animation/animation-min.js?v=4110
	http://ducvinhqb.com/service.html	Get hash	malicious	Browse	• us.i1.yimg.com/us.yimg.com/i/us/my/addtomyyahoo4.gif
151.101.1.44	norit.dll	Get hash	malicious	Browse	
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	
	opzi0n1[1].dll	Get hash	malicious	Browse	
	nsetldk.dll	Get hash	malicious	Browse	
	Izezma64.dll	Get hash	malicious	Browse	
	fuxenm32.dll	Get hash	malicious	Browse	
	api-cdef.dll	Get hash	malicious	Browse	
	pupg3.dll	Get hash	malicious	Browse	
	vnaSKDMnLG.dll	Get hash	malicious	Browse	
	tjbdhdvi1.zip.dll	Get hash	malicious	Browse	
	Izipubob.dll	Get hash	malicious	Browse	
	nivude1.dll	Get hash	malicious	Browse	
	Accesshover.dll	Get hash	malicious	Browse	
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	
	con3cti0n.dll	Get hash	malicious	Browse	
	bei.dll	Get hash	malicious	Browse	
	ECvOLhE.dll	Get hash	malicious	Browse	
	opzi0n1[1].dll	Get hash	malicious	Browse	
	c0nnect1on.dll	Get hash	malicious	Browse	
	c0nnect1on.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
contextual.media.net	norit.dll	Get hash	malicious	Browse	• 104.80.21.70
	opzi0n1[1].dll	Get hash	malicious	Browse	• 104.84.56.24
	nsetldk.dll	Get hash	malicious	Browse	• 2.20.86.97
	Izezma64.dll	Get hash	malicious	Browse	• 2.20.86.97
	fuxenm32.dll	Get hash	malicious	Browse	• 2.20.86.97
	api-cdef.dll	Get hash	malicious	Browse	• 92.122.146.68
	pupg3.dll	Get hash	malicious	Browse	• 104.84.56.24
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 104.80.21.70
	tjbdhdvi1.zip.dll	Get hash	malicious	Browse	• 104.84.56.24
	Izipubob.dll	Get hash	malicious	Browse	• 92.122.146.68
	nivude1.dll	Get hash	malicious	Browse	• 92.122.146.68
	Accesshover.dll	Get hash	malicious	Browse	• 104.84.56.24
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 92.122.146.68
	con3cti0n.dll	Get hash	malicious	Browse	• 2.18.68.31
	http://https://westsactrucklube.com/cda-file/Doc.htm	Get hash	malicious	Browse	• 92.122.146.68
	bei.dll	Get hash	malicious	Browse	• 104.80.21.70
	ECvOLhE.dll	Get hash	malicious	Browse	• 2.18.68.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	opzi0n1[1].dll	Get hash	malicious	Browse	• 2.18.68.31
	c0nnect1on.dll	Get hash	malicious	Browse	• 104.84.56.24
	c0nnect1on.dll	Get hash	malicious	Browse	• 2.18.68.31
tls13.taboola.map.fastly.net	norit.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 151.101.1.44
	opzi0n1[1].dll	Get hash	malicious	Browse	• 151.101.1.44
	nsetldk.dll	Get hash	malicious	Browse	• 151.101.1.44
	Izezma64.dll	Get hash	malicious	Browse	• 151.101.1.44
	fuxenm32.dll	Get hash	malicious	Browse	• 151.101.1.44
	api-cdef.dll	Get hash	malicious	Browse	• 151.101.1.44
	pupg3.dll	Get hash	malicious	Browse	• 151.101.1.44
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 151.101.1.44
	tjbdhdvi1.zip.dll	Get hash	malicious	Browse	• 151.101.1.44
	Izipubob.dll	Get hash	malicious	Browse	• 151.101.1.44
	nivude1.dll	Get hash	malicious	Browse	• 151.101.1.44
	Accesshover.dll	Get hash	malicious	Browse	• 151.101.1.44
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 151.101.1.44
	con3cti0n.dll	Get hash	malicious	Browse	• 151.101.1.44
	bei.dll	Get hash	malicious	Browse	• 151.101.1.44
	ECvOLhE.dll	Get hash	malicious	Browse	• 151.101.1.44
	opzi0n1[1].dll	Get hash	malicious	Browse	• 151.101.1.44
	c0nnect1on.dll	Get hash	malicious	Browse	• 151.101.1.44
	c0nnect1on.dll	Get hash	malicious	Browse	• 151.101.1.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YAHOO-DEBDE	norit.dll	Get hash	malicious	Browse	• 87.248.118.23
	opzi0n1[1].dll	Get hash	malicious	Browse	• 87.248.118.23
	http://searchlf.com	Get hash	malicious	Browse	• 87.248.118.23
	api-cdef.dll	Get hash	malicious	Browse	• 87.248.118.23
	pupg3.dll	Get hash	malicious	Browse	• 87.248.118.23
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 87.248.118.23
	tjbdhdvi1.zip.dll	Get hash	malicious	Browse	• 87.248.118.23
	http://https://eti-salat.com/x/	Get hash	malicious	Browse	• 87.248.118.22
	Izipubob.dll	Get hash	malicious	Browse	• 87.248.118.23
	nivude1.dll	Get hash	malicious	Browse	• 87.248.118.23
	Accesshover.dll	Get hash	malicious	Browse	• 87.248.118.22
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 87.248.118.23
	http://https://westsactrucklube.com/cda-file/Doc.htm	Get hash	malicious	Browse	• 87.248.118.23
	bei.dll	Get hash	malicious	Browse	• 87.248.118.23
	opzi0n1[1].dll	Get hash	malicious	Browse	• 87.248.118.23
	c0nnect1on.dll	Get hash	malicious	Browse	• 87.248.118.22
	http://tracking.mynetglobe.com/view?msgid=QLykQQgnO8vsE7HiT7Bwow2	Get hash	malicious	Browse	• 87.248.118.22
	c0nnect1on.dll	Get hash	malicious	Browse	• 87.248.118.23
	http://https://www.sarbacane.com/	Get hash	malicious	Browse	• 87.248.118.23
	c0nnect1on.dll	Get hash	malicious	Browse	• 87.248.118.22
A2HOSTINGUS	invoice.xls	Get hash	malicious	Browse	• 70.32.23.26
	invoice.xls	Get hash	malicious	Browse	• 70.32.23.26
	invoice.xls	Get hash	malicious	Browse	• 70.32.23.26
	http://https://showmewhatyouhave.com/wp-includes/ID3/ASB/?email=kmcpherson@deloitte.co.nz	Get hash	malicious	Browse	• 68.66.226.85
	2hXlfEl7ClfpfY1.exe	Get hash	malicious	Browse	• 85.187.154.178
	invoice_no_H04618.doc	Get hash	malicious	Browse	• 75.98.175.94
	invoice_no_H04618.doc	Get hash	malicious	Browse	• 75.98.175.94
	invoice_no_H04618.doc	Get hash	malicious	Browse	• 75.98.175.94
	invoice.exe	Get hash	malicious	Browse	• 68.66.248.44
	Inquiry-20201118105427.exe	Get hash	malicious	Browse	• 85.187.154.178
	EMMYDON.exe	Get hash	malicious	Browse	• 85.187.154.178
	OUTSTANDING INVOICE_pdf.exe	Get hash	malicious	Browse	• 85.187.154.178
	uM0FDMSqE2.exe	Get hash	malicious	Browse	• 70.32.23.14
	VeiRTphBRH.exe	Get hash	malicious	Browse	• 85.187.154.178
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 68.66.216.20

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://pixelksa.com/po/NewfilServices/index.php	Get hash	malicious	Browse	• 67.209.116.21
	http://https://www.desimealz.com/wp-content/plugins/xnbwwmx/Payment_Report_EFT_FX_FT%202020-13-11.jar	Get hash	malicious	Browse	• 85.187.137.156
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 68.66.216.20
	DHL RECEIPT_pdf.exe	Get hash	malicious	Browse	• 85.187.154.178
	RFQ-1324455663 API 5L X 60.exe	Get hash	malicious	Browse	• 85.187.154.178
CLOUDFLARENETUS	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.86.226
	Final_report_2020.html	Get hash	malicious	Browse	• 104.16.18.94
	norit.dll	Get hash	malicious	Browse	• 104.31.69.174
	380000_USD_INV_011740_NOV_2020.jar	Get hash	malicious	Browse	• 104.20.22.46
	380000_USD_INV_011740_NOV_2020.jar	Get hash	malicious	Browse	• 104.20.23.46
	http://https://tinyurl.com/y9xs2oe6	Get hash	malicious	Browse	• 104.20.138.65
	case.2522.xls	Get hash	malicious	Browse	• 104.31.87.113
	http://https://ch1.amorozon.fr/.zz?&78387439&user=jon.parr@syngenta.com	Get hash	malicious	Browse	• 104.27.129.197
	case.2522.xls	Get hash	malicious	Browse	• 104.31.87.113
	coinomi-1.20.0.apk	Get hash	malicious	Browse	• 162.159.200.1
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.143.180
	http://fonts.mafia-server.net	Get hash	malicious	Browse	• 104.18.40.210
	caw.exe	Get hash	malicious	Browse	• 162.159.138.232
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 104.16.19.94
	Soda_PDF_12_Installer (7).exe	Get hash	malicious	Browse	• 104.16.181.79
	REQUEST FOR BID 26-11-2020.ppt	Get hash	malicious	Browse	• 104.18.49.20
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 104.16.19.94
	DHL_Nov 2020 at 1.85_8BZ290_PDF.jar	Get hash	malicious	Browse	• 104.20.23.46

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	INVOICE.html	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	Final_report_2020.html	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	norit.dll	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://https://tinyurl.com/y9xs2oe6	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://https://ch1.amorozon.fr/.zz?&78387439&user=jon.parr@syngenta.com	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://https://ib.adnxs.com/getuid?https://a.adrsp.net/dsp/ci/2/E8quIp-RUbrsO6XnZMkW-Z82IQ_D_mG3bKHPbyWqDJNAFkp2JZBiBD4qwJcECqeCBYZccMP3y2IGKpMkBSJ3emkLIw/%24UID	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://fonts.mafia-server.net	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://https://broughtguarantees.com/1/oZrheD/cHBlcmluaUBhZmZpbmlvbmdyb3VwLmNvbQ%3D%3D&d=DwMDaQ	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://https://offiubtj7banjz48zrg8d4nz2ns9.web.app/?c=brynjar.t.gudmundsson@landsbanki.is	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://https://erabansoupala.blogspot.com//?m=0	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://mincast.us-south.cf.appdomain.cloud/redirect/?email=prampon@soteb.fr	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://https://dagevleri.com/inv	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://https://dealmaker.pl/au_au.html	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
	http://https://wilkinsonbutler.tallverse.ga/YW1iZXJAd2lsa2luc29uYnV0bGVyLmNvbQ==	Get hash	malicious	Browse	• 87.248.118.23 • 151.101.1.44
37f463bf4616ecd445d4a1937da06e19	document-152186451.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1544626742.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1544163851.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1511922671.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1577042928.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	norit.dll	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1593116601.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1435187538.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	invoice.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	case.2522.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	http://https://ch1.amorozon.fr/.zz?&78387439&user=jon.parr@syngenta.com	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1525171907.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1509971776.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-158579829.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1588534000.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1441856683.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1710999016.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1550335181.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-1206377353.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26
	document-15937128.xls	Get hash	malicious	Browse	• 172.67.155.205 • 70.32.23.26

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.msn[2].xml	
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3692
Entropy (8bit):	4.832871516361626
Encrypted:	false
SSDEEP:	96:h1oY1oYM1oY1oYd1oY331Y33f3tLtL3tLtLKMMRMMTv9F9MTv9F9GMTv9F9MTv9e:YLMLDoQ
MD5:	C31ADDB945F676CC7E501919B63A8C40
SHA1:	D83C18965004DDFC03073676BED3215F10C9CCE7
SHA-256:	0843E26A008AFAA940AA95A114856F4EA75C1906B3688C8CF7927BFAF11AEB85
SHA-512:	BE97EDFDDF8CC4141094A505CCB4E2FD37C7432C07D90E5DBC7BC57E646A0C4549145001F8E0D28FC5ACAB1C701B04118B2292123772FB227AED87DDBDBCF 34
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="3437918832" htime="30852433" /></root><root><item name="HBCM_BIDS" value="{}" ltime="34380 78832" htime="30852433" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3438078832" htime="30852433" /><item name="mntest" value="mntest" ltim e="3438158832" htime="30852433" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3438078832" htime="30852433" /></root><root><item name="HBCM_B IDS" value="{}" ltime="3438078832" htime="30852433" /><item name="mntest" value="mntest" ltime="3438238832" htime="30852433" /></root><root><item name ="HBCM_BIDS" value="{}" ltime="3438078832" htime="30852433" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3438278832" htime="30852433" /></r oot><root><item name="HBCM_BIDS" value="{}" ltime="3438278832" htime="30852433" /><item name="mntest" value="mntest" ltime="3438358832" htime="30852433" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3438278832" htime="30852433" /></root><ro

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{07A17A1D-3145-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24152
Entropy (8bit):	1.7560692670331646
Encrypted:	false
SSDEEP:	48:IwgGcprJGwpLOG/ap86rGIpcVPGvnZpvVbGvHZp9VdGoSiqpvVAGo4+vKpcYGWS6:rEZjZs269W6tGfy7tx+vKWln6
MD5:	F046036DD9047D9A75B19C00923D1E00
SHA1:	67A427062DE85F586352FA0231F4349ACC957B89
SHA-256:	23638981C3E4A7B8B3FF5ABBFB7C5B4F28B91F1B80A1489C1ACB1B5488816ED5
SHA-512:	57CD19AE8B0365D2E025E95A083A25BD0D35E1C2060CE3D21E496DD0392B9DE3CD79C2D6F909F0AADB0A29D2E19F633699781B6257CF897F2F12E7FC4A11EE 6
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{07A17A1F-3145-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	192394
Entropy (8bit):	3.6061773721928656
Encrypted:	false
SSDEEP:	3072:HoiqZ/2Bfc6ru5rXfVStsiqZ/2BfcJru5rXfVStx:ZPs
MD5:	45355EE8C7C21E42A0D4928DDD23D2B0
SHA1:	0166B202C72664A5667FDDA65DACA9708595D9EA
SHA-256:	D1A9A5CA5E2108F1342C7E43F75C33CC4F697E1C9F5AE1669C725CA31C111110
SHA-512:	1FF0EB14A229656B7AE8CA782199671F432F58E6C6CDE4076964D1D475FDEC3ABA25DFE3EFDD94196A1977883705A6F68A1EBC4354B93430436801569D4A29BE
Malicious:	false
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):	657
Entropy (8bit):	5.034940520263983
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE/Q1Q1nWimI002EtM3MHdNMNxOE/Q1Q1nWimI00ONVbkEtMb:2d6NxO4oGSZHKd6NxO4oGSZ7Qb
MD5:	04ACC8C1D65796C96276B43AD77DBA5B
SHA1:	472552B8D1D6A2E9D56DAE14B886607D5F0D5C94
SHA-256:	BFDADD3318B81421281AB24827F30AFE281CE10A205F31BD25212B3CDABAB1FA
SHA-512:	84CFC561CA727B6946F926543F5801FFB903098984E1B586CF82DA3C9FAD5BF796497F5A631B4AE948CE66A52843BDBC39A288803E602F1516D4BD93F072FEFF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xde202cec,0x01d6c551</date><accdate>0xde202cec,0x01d6c551</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>0xde202cec,0x01d6c551</date><accdate>0xde202cec,0x01d6c551</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):	654
Entropy (8bit):	5.0822360553003
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k351nWimI002EtM3MHdNMNxe2k351nWimI00ONkak6EtMb:2d6NxrGSZHKd6NxrGSZ72a7b
MD5:	5F06B2732C9B946BB50E1CA9CC1F39BD
SHA1:	85EFEBD9F8E02E7431A9D4537D0A25393A89F888
SHA-256:	56DBCD54A59D3BB07743FB339CA570EAE3BA6F27D6D154FBB41F05DD8CE723FE
SHA-512:	AD98129565B528BD3DEF6C7639627F9ED916418DBCE4C08B6499DB6A9C06AE65FF46DFF0B8C5A9F1AA55384ECC5CBE430908F54E58FA008E29FD4A95E5B682C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xde1905d9,0x01d6c551</date><accdate>0xde1905d9,0x01d6c551</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>0xde1905d9,0x01d6c551</date><accdate>0xde1905d9,0x01d6c551</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):	663
Entropy (8bit):	5.054205130835748
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL/Q1Q1nWimI002EtM3MHdNMNxvL/Q1Q1nWimI00ONmZEtMb:2d6NxvLoGSZHKd6NxvLoGSZ7Ub
MD5:	7567715AE2D9303EEA66EF0A278A2BCC
SHA1:	55BE061D8377277A0001D453E7FB6895BAAE7079
SHA-256:	3C6253A8ABD425282055CEE7406625D948345CA922566487FFA2B63317E31FB1
SHA-512:	6CD89C40FC69DAB5C639C8E58F89B4DE8DAE6FC651AF45383FE0313760FCC030170746A86C10251D5C50062553D0BD6C17A26840BEB95DD87A7FFC1609ABE90
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xde202cec,0x01d6c551</date><accdate>0xde202cec,0x01d6c551</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>0xde202cec,0x01d6c551</date><accdate>0xde202cec,0x01d6c551</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.0512936478911294
Encrypted:	false
SSDEEP:	12:TMHdNMNxiCSoS1nWimI002EtM3MHdNMNxiCSoS1nWimI00ONd5EtMb:2d6NxgSZHKd6NxgSZ7njb

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
MD5:	155B7F641A3B73BA25227BFB668A701C
SHA1:	61E452A8BFAC8E1EA99A74955408F6B2AE2E22EC
SHA-256:	C1D1D399435AACE09AFCAE40F5AF117FC7AC1DBA4608A127D9E4CCFF0B85F499
SHA-512:	C4E096A6BF4FB4DBB6F60652416E7D07978378D152AB47D520068D2F7801974A4E6872991CB09B5EBECEB7E8878F5CF1701589DD1911292585831E94EB081EDA
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xde1dca87,0x01d6c551</date><acc date>0xde1dca87,0x01d6c551</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>0xde1dca87,0x01d6c551</date><accdate>0xde1dca87,0x01d6c551</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.110254016599087
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwfzNVzN1nWimI002EtM3MHdNMNxhGwfzNVzN1nWimI00ON8K075Ety:2d6NxQKSZHKd6NxQKSZ7uKajb
MD5:	82EBA9B143D14CB1E54C73834C0530B8
SHA1:	CBDE8C3A7D4AF7F937236B0B1AB2ACBCB7E2A787
SHA-256:	78ABA2C16B628972E470755FBCF40F262AAAA74184E28D86E2B4D91FD77359E1
SHA-512:	0D1A96FD19D5BF574B64529AFA66B70E8CCB0CDD6DF29A59F690DF5436D6289E027467149AE7662E0DE507B7636BEDC1CE8D913817B2C1F96586FA38E61C8F 4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xde228f51,0x01d6c551</date>< accdate>0xde228f51,0x01d6c551</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>0xde228f51,0x01d6c551</date><accdate>0 xde228f51,0x01d6c551</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):	654
Entropy (8bit):	5.035869855475188
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n/Q1Q1nWimI002EtM3MHdNMNx0n/Q1Q1nWimI00ONxEtMb:2d6Nx0/oGSZHKd6Nx0/oGSZ7Vb
MD5:	E7270CD45AA98654A99F8C40D2398342
SHA1:	A7574A7BD96A03AAF3980D436E33CC2494B8A674
SHA-256:	5E712C3D693276978EE9A13A3B25B582332ABA58559827DE116F7D1BF81B81AB
SHA-512:	1F0F9F7CA8DACBF0191FDD11106B7258C11B1CA8045874D1C2722F8A8034D178856EF3EF5287B5FD1FE1772451A12CFA7ECDCD8DDDAAACCCEEBFB295DB22 5C0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xde202cec,0x01d6c551</date><a ccdate>0xde202cec,0x01d6c551</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xde202cec,0x01d6c551</date><accdate>0xd e202cec,0x01d6c551</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin202591677780\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):	657
Entropy (8bit):	5.076493966005991
Encrypted:	false
SSDEEP:	12:TMHdNMNxxCSoS1nWimI002EtM3MHdNMNxxCSoS1nWimI00ON6Kq5EtMb:2d6NxNSZHKd6NxNSZ7ub
MD5:	ACB57A218EFBB2CAA03B9E67B0F9B9D2
SHA1:	34720EBD8A4B694A279403882BC5ADF91E92B6DB
SHA-256:	1D44FB64953D093C5451A034AF3DCEAA31CFE6D25149B43898BFB4C29E6BCCFF
SHA-512:	1B57812FE04B1ADCA0248F049B6A5CB5DD33B2FC461CDDEE0ACD531041F0976F9147B7412807D98D58C3CCEA718A228A6DAACE4BBEA79A61092B5E68DF015 2A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xde1dca87,0x01d6c551</date><accdate>0xde1dca87,0x01d6c551</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>0xde1dca87,0x01d6c551</date><accdate>0xde1dca87,0x01d6c551</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):	660
Entropy (8bit):	5.077615829325296
Encrypted:	false
SSDEEP:	12:TMHdNMNxcWhw0hw1nWimI002EtM3MHdNMNxcWhw0hw1nWimI00ONVEtMb:2d6NxDLmSZHKd6NxDLmSZ71b
MD5:	CA0D4B030C1DE01DA8DA2AE1BF0ED74C
SHA1:	F36E9B3D57FDE87FFD8A3D431008C557B99F60A4
SHA-256:	40023D1A7FCC94F8F9D0792E5DE265F1D299668205A12159EBAD95F8BFAE1FEE
SHA-512:	5F15D7AAC5A5CA446FF98E0DEE7393A31958809DFA507499044C2547ABB4D5B6B1A5623CED102300E5104807A3763EA4B521039F9005F1877EDE227646286378
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xde1b6830,0x01d6c551</date><accdate>0xde1b6830,0x01d6c551</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>0xde1b6830,0x01d6c551</date><accdate>0xde1b6830,0x01d6c551</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):	654
Entropy (8bit):	5.037102291409875
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnCSoS1nWimI002EtM3MHdNMNxfnCSoS1nWimI00ONe5EtMb:2d6NxjSZHKd6NxjSZ7Ejb
MD5:	65A4ACA6F8A928D83ED0A7C189330B74
SHA1:	EA5E344314636E36ABE45E64D78D2D83F4CB65F6
SHA-256:	2B6E1BAC6EE2C6C3C4DC1E2F3BD01BD5E084B14DBC5884DB942B412EB98CFC90
SHA-512:	0E3B249D80827942E0BEE1114387876C8A7560B76F443629E243AD7E8B9E59BBC55E3CA8BBC083D98BD0D0D28320944A76444834149FD6E37458D46389B8EC44
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xde1dca87,0x01d6c551</date><accdate>0xde1dca87,0x01d6c551</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>0xde1dca87,0x01d6c551</date><accdate>0xde1dca87,0x01d6c551</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\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.035388589152814
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGe:u6tWu/6symC+PTCq5TcBUX4bE
MD5:	EC3D7BE799FBB3F34B2A261805D57E0B
SHA1:	797908D6AD8BE32348356D837E616C49DE6812B3
SHA-256:	F125362D8D6DAC807C430FB038FDE74ADCBCC011CA7E6545488BA17CEF17217D
SHA-512:	5A716330A274B88306522700AF1527495DD1FD2DB105C790E8C66DF918CAD412C0C5A6F6E5997591A9BFD409DBAE69256AA37C7BD8F40AB45FC606B2CB3525C
Malicious:	false
Preview:	E.h.t.t.p.s.:././.s.t.a.t.i.c.-.g.l.o.b.a.l.-.s.-.m.s.n.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.h.p.-.n.e.u./.s.c./.2.b./.a.5.e.a.2.1...i.c.o.....PNG.....IHDR... ... .pHYs..... .vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....)....;..Bx..2.}.. ._>w!..%B..{.d... LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@IA.,>\.Q|.N.P.....<.!....ip...y..U....J...9 ...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R..... .72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. ... .,_.....,_....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\17d7518f-d5e8-44e7-9ac7-05e1d2be2ab2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\17d7518f-d5e8-44e7-9ac7-05e1d2be2ab2[1].jpg	
Category:	downloaded
Size (bytes):	67574
Entropy (8bit):	7.976737629047781
Encrypted:	false
SSDEEP:	1536:I+hkPgJTviCUhvtBvGazEw5+mYzSM6I5SEF2alD8J24f:ISPDCUhvvhl+mYz4I5SEjlDr4f
MD5:	20167C9B301C089D80A7D4E2F5BCDD1F
SHA1:	FD9D70793E0BB69B5AE6A913699E41CAE70D4153
SHA-256:	27D2374BFC5E9C6C8616FCC0A91DC9B0CCA5E28118300B4C4259E223E4CDEB44
SHA-512:	4A20F728FF73536755544BAA151BF1A2B885738B88A9F6FF6509F629FDD4708028DFD9BDB6B7A5A93436F559FC0159CEEB432C509F4F3FA8A05A41D1D30D65A1
Malicious:	false
IE Cache URL:	http://https://cvision.media.net/new/300x300/2/94/148/210/17d7518f-d5e8-44e7-9ac7-05e1d2be2ab2.jpg?v=9
Preview:	......JFIF.....C.....C.....,,..".....F.....!.1."AQ. .2a#q..B...$3R.....Sbr%4.'5C.....@.....!.1.."A.Qa.#2q..B....3R...$%b.CS...4r.....?...|.>.._h:.....R.Q.Z.d....m..x%....H..sF.2...g....Z..ToC Z.X$.2C#.RH.Hh.F.$.AR.....e..f..Ys.....*.x`FA.....]...Fy4..T..1...j.....36.....+..}....2..7 .....}....Z..E.v.....>O...+...V..Ice*..H.u.K#.,....`X..m).c.u~>2.*....P.28.....j...0#..@..Ug. ..z.i$y..f..r..8...EUH.1....e...<....#q.@.0j..!..<...<D.q_.x`:t.v.m..i...(a.S.....t..._s..8,.l;G..w\|..?.....\6.p.....hF.n.J7#.....<..o...@..?...6.....a.?.<p..F.....&V.._..S.....$m....8..R..... v.9..q..K.rG.....n~.....O.<q.o....Y....8..>...p.....g...3....._.<.H.....=....>..`.....^...q.?...s...}...o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\39ab3103-8560-4a55-bfc4-401f897cf6f2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	downloaded
Size (bytes):	64434
Entropy (8bit):	7.97602698071344
Encrypted:	false
SSDEEP:	1536:uvrPk/qeS+g/vzqMMWi/shpcnsdHRpkZRF+wL7NK2cc8d55:uvrsSb7XzB0shpOWpkThLRyc8J
MD5:	F7E694704782A95060AC87471F0AC7EA
SHA1:	F3925E2B2246A931CB81A96EE94331126DEDB909
SHA-256:	DEEBF748D8EBEB50F9DFF0503606483CBD028D255A888E0006F219450AABCAAE
SHA-512:	02FEFF294B6AECDDA9CC9E2289710898675ED8D53B15E6FF0BB090F78BD784381E4F626A6605A8590665E71BFEED7AC703800BA018E6FE0D49946A7A3F431D7
Malicious:	false
IE Cache URL:	http://https://cvision.media.net/new/300x300/3/167/174/27/39ab3103-8560-4a55-bfc4-401f897cf6f2.jpg?v=9
Preview:	......JFIF.....C.....C.....,,..".....Q.....!.1A."Qa q.....#2...$B...3Rb.%CS...&4Tr..(56cs.....F.....!...1..AQ"aq.2....BR....#3..Cb....$Sr..&FTc.....?...N..m.1$!..l({&.l...Uw.Wm...i..VK.KWQH.9. .n...S~.....@xT.%.D.?....}Nm.;&.....y.qt8...x.2..u.TT.=.TT...k.....2..j.J...BS...@'.a....6..S/0.l,.J.r...,<3~...,A....V.G..'*....5].....p...#Yb.K.n!'n..w..{o...._.....1..l...).(.l.4.....z[}.Z... .D2.y...o..}.=..+i.=U.....J$.(.IH0.-...uKSUm*P..T.5..H.6.....6k,8.E....".n.....pMk+...q...n)GEUM..UUwO%O...)CJ&.P.2!!.....D.z...W...Q..r.t..6]... U.;m...^..:*.k.ZO9...#...q2 ....mTu..Ej....6.)Se.<.*.....U.@...K.g\D.../..S....~.3 ....hN..".n...v.?E^,.R<-.Y^)...M.^a.O.R.D...;yo.~..x;u..H.....-.%.....].*.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2830
Entropy (8bit):	4.775944066465458
Encrypted:	false
SSDEEP:	48:Y91lg9DHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAcHHPk5JKIDrZjSf4ZjfumjVLbf+:yy9Dwb40zrvdip5GHZa6AymsJjxjVj9i
MD5:	46748D733060312232F0DBD4CAD337B3
SHA1:	5AA8AC0F79D77E90A72651E0FED81D0EEC5E3055
SHA-256:	C84D5F2B8855D789A5863AABBC688E081B9CA6DA3B92A8E8EDE0DC947BA4ABC1
SHA-512:	BBB71BE8F42682B939F7AC44E1CA466F8997933B150E63D409B4D72DFD6BFC983ED779FABAC16C0540193AFB66CE4B8D26E447ECF4EF72700C2C07AA700465E
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/55a804ab-e5c6-4b97-9319-86263d365d28.json
Preview:	{"CookieSPAEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":true,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","ws","gd","ge","gg","gh","gi","gl","gm","gn","gq","gs","gt"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAuTnto[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	801
Entropy (8bit):	7.591962750491311

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAuTnto[1].png	
Encrypted:	false
SSDEEP:	24:U/6yrupdmd6hHb/XvxQfxnSc9gjo2EX9TM0H:U/6yruzFDX6oDBY+m
MD5:	BB8DFFDE8ED5C13A132E4BD04827F90B
SHA1:	F86D85A9866664FC1B355F2EC5D6FCB54404663A
SHA-256:	D2AAD0826D78F031D528725FDFC71C1DBAA21B7E3CCEEAA4E7EEFA7AA0A04B26
SHA-512:	7F2836EA8699B4AFC267E85A5889FB449B4C629979807F8CBAD0DDED7413D4CD1DBD3F31D972609C6CF7F74AF86A8F8DDFE10A6C4C1B105422225059793055
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAuTnto.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O].[H.a...s..k.x..$....L...A.(T.Y....S$T....E.J.EO.(=..RB^..{..4..M...^f/3.o..?,..|...9.s>...E.]rh j2.4....G.T"..!r.Th.....B..s.o.!...S...bT.81.y.Y....o...O.?.Z..v.....#h*;.E.....)p.<.....'.7.*{.;.....p8...:..).O..c!.....5...KS..1....08..T..K..WB.Ww.V....=.)A.....sZ..m..e..NYW...E... Z].8Vt...ed.m..u.....|@...W...X.d...DR.....007J.q..T.V./..2&Wgq..pB..D....+...N.@e.....i..:.L...%....K..d..R.....N.V.....$.....7..3.....a..3.1...T.`.]...T{.....).....Q7JUUlD....Y... .$czVZ.H..SW$.C.....a...^T.....C..(.;]\|,.2..;.....p..#.e..7....<..Q...}..G.WL,v.eR...Y..y.`>.R.L..6hm.&,...5....u..[$_.t1.f...p..(.."Fw.I...'.....%4M..._....[.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB10MkbM[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	965
Entropy (8bit):	7.720280784612809
Encrypted:	false
SSDEEP:	24:T2PqcKHsgioKpXR3TnVUvPkKWsvIos6z8XYy8xcvn1a:5PZK335UXkJsgIyScf1a
MD5:	569B24D6D28091EA1F76257B76653A4E
SHA1:	21B929E4CD215212572753F22E2A534A699F34BE
SHA-256:	85A236938E00293C63276F2E4949CD51DFF8F37DE95466AD1A571AC8954DB571
SHA-512:	AE49823EDC6AE98EE814B099A3508BA1EF26A44D0D08E1CCF30CAB009655A7D7A64955A194E5E6240F6806BC0D17E74BD3C4C9998248234CA53104776CC00A0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB10MkbM.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs...#...#.x.?v...ZIDAT8OmS[h.g.=s..$n...]7.5..(.&5...D..Z..X..6....O.-.HJm.B.....j..Z,.D.5n.1....^g7;;.;3.w../..... ..}....5....C==}..hd4.OO..^1.I..*.U8.w.B..M0..7}.....J....L.i...T...(J.d*.L..sr.....g?.aL.WC.S..C...(.pl..}[Wc..e.....[...K.....<...=S.....]..N/.N....(^N'.Lf....X4.....A<#c.....4fL.G.. 8..m..RYDu.7.>...S....-k.....GO.....R.....5.@.h...Y$..uvpm>(<..q.,.PY....+...BHE..;.M.yJ...U<..S4.j..g....x.....t".....h.....K...~._...:...qg.).~..oy..h..u6....i._n...4T..Z.#.. ...0....L.....l..g!..z...8.I&....,iC.U.V,j_._...9.....8<...A.b.|.^..;..2...../v .....>....O^..;.o...n .'!k\l..C.a.I$8.~.0...4j..~5.\6...z?..s.qx.u....%...@.N.....@..HJh].....l.....#'.r.!../..N .d!m...@.....qV...c..X....t.1CQ..TL....r3.n..".t.....`...$...ctA....H.p0.0.A..IA.o.5n.m...\.l.B>....x..L.+.H.c6..u...7....`....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB15AQNm[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	23518
Entropy (8bit):	7.93794948271159
Encrypted:	false
SSDEEP:	384:7XNEQW4OGoP8X397crjXt1/v2032/EcJ+eGovCO2+m5fC/lWL2ZSwdeL5HER4ycP:7uf4ik390Xt1vP2/RVCqm5foMyDdeiRU
MD5:	C701BB9A16E05B549DA89DF384ED874D
SHA1:	61F7574575B318BDBE0BADB5942387A65CAB213C
SHA-256:	445339480FB2AE6C73FF3A11F9F9F3902588BFB8093D5CC8EF60AF8EF9C43B35
SHA-512:	AD226B2FE4FF44BBBA00DFA6A7C572BD2433C3821161F03A811847B822BA4FC9F311AD1A16C5304ABE868B0FA1F548B8AEF988D87345AEB579B9F31A74D5BF3 C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB15AQNm.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=868&y=379
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOO.....p.n.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...(...CKHh.....i.@.....i..IR2...MpR..^E....&EYv..N.j...e..j..U,..*..BZ...qQM.dT....@..8..s..i..}....n..D...i..... VC.HK"..T.iX.f.v&.}.v..7..jV.....jF.c..NhS.L.b>x".D.....G.Z..!.i..VO..._4.@X.].p..].5b+...Uk...((@.s'..?Hv.....\z.z.JGih..}*S.....T..WBZ...'.T?6..j.H".....*..%p3.YnEc.W.f.^. .....Q.....#..k..Z.....I:..MC..H.S..#..Y ..A.Zr...T..H..P..[..b.C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1b6vzA[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1181
Entropy (8bit):	7.7288928012776195
Encrypted:	false
SSDEEP:	24:qhEQPY2/Tygr5eXq+/RfX3ZUgsTDCALZVDwY1o8UkI:aEX8egz+3ZwMY1o8O
MD5:	F04F6408BCA330EB02293C06239D9DD5
SHA1:	3447ED257FD3AEE3E3113A80979F989EEF343032
SHA-256:	85337EE31515CEC275335BA15A1966B8AC45C5F97212FF97C367BEE8D06BF1C1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1b6vzA[1].png	
SHA-512:	5A53C0BA9012B639E7CC2A033352EC093C92C7E8430B1C3DED5FC61E040682A5661F59E21650829D0C077B3FCBF816ADD35E489E382140192E959136BC7082D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1b6vzA.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....U....sRGB.....gAMA.....a.....pHYs.....o.d...2IDATHK.TKH.W.>....V.X.&*.(..fdh7-m.T.. t.].....dZ7..Bp!..../...."jUD..(.~.g|f...o.&.8Bw....{....9.;.....(--....;nnn....L....444.....h...j.....W:...m $.]aaa.uuu.%..@..?.....~...^.....Q.>..Eaaa.....>..z5>....xx.....w...=...u...f.....M.....a.....w.....GFuD....w.Q.....,_...9.....uaa....Dj70....j...l.....Y..0".....M.....,..z8.)))....S....J.w.(g.;;;L*...(.....b....~+.;.K..=;88.~f...!Dm).-233)))I.....N..L..MNN>.IFDD.....x.D....)_.....X..iuu.c..b..=2\.....f3...P\\.v!.....`.=.....bu...N...=2....788HH....0.....<***"....n...&t.....Q.?.g+++....2.....K&....b.#....K/".....X.333411!.p.P....C...B...!b`..s_.....9A..!,....A...B...$a.,...!y...3....]...'d..mJYIDRRR".....L&...;.TH....O.....<..3.O766n.@|<.....jjjhllL...Bf.8_....G.',...p<.....Y....?.G..TWWG...bg"nM..fo.[.....n.p..jz....Hx.....Cn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bnj39[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	22806
Entropy (8bit):	7.932321649486506
Encrypted:	false
SSDEEP:	384:7T2P4auuEFTqekqxTCKCuPW37eZSLJmPJFbgz+R+kMOGHee/7X5jG3XscSowxHJj:7T2VpxqxTOuPW3DLJmPQG+e87XIHscS/
MD5:	47575A12CA7EF3F7449A69EC636249C8
SHA1:	B2F3DAF576054703A88BB3CB83CD4572898F5402
SHA-256:	45A23C228E2547E47950F714B322EEA5AF7B8298E63C996A529166C805C43C4C
SHA-512:	784EC5A0C4D4FC65B64149B20A3C1F08A59E396003ECE18550C3B5615F5665C7697BE1CFC4A58E9B790421814A0F568DE9B8BBD950226D716E7621B01637510C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bnj39.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...`.f..w1.)...D..Z.S..3d.R-D....Fl.R.E(.$Z(....(...(...'Ju6N..p.6_...5.@:.Y.Q..>.\.8.$.:i.N..I....#.1.D<.dh.3-.v..y.2.5(....d.+r.{hF....5..X.pj.....+..`XWQc.W-m.c...`.M,..dv.D.W....B8.z..Sf.....n...4.ibyf;x5G.c&sR.$R*.r..b..e7.Z.&k"...zV..aR...).....E.9Z...i0)..VRM'+.....4.#..i..Q..V.....Wi%.....z...#$..&..d...=(.qi.....v5.D...Xs.d...+.{.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bq2gt[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	10651
Entropy (8bit):	7.894477350730833
Encrypted:	false
SSDEEP:	192:xYmvlcn57l9vy6oyAtGbyc9R0U9qDuuxBVR7chnaA5hVKZ0KLl2kzKmwDKwvSuRZ:OmvlcnRl9vGyEG2U04YBVRwRfa0KLlJY
MD5:	B689F5E5989B6811D3AC3A24CB576797
SHA1:	C7764863F817AB5A7A1F66D71208055477BC01B7
SHA-256:	6EF77C05673497E05619EE779E8B12943AEF73A954CD0ED1DC0CF37D68311084
SHA-512:	E010D7E7486C18E711EBA1D7C9BDA5DEBE425369BE35648609DAAC396CFB9F4F8C3B19096886C46B64C4256AB185D77715D6181D1F4FB082D45613672FC56B0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bq2gt.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...(...(...(...(...(...(...(...(...(.....&.k...ZT.ew2. .c...X.L.u..%....c.+9.Q..u.OE..Qk.O.F&..]....z.U..R..i<..M...y.....9<t.+.r..R.....Y*..Ug..\....}KXY....-wb2.....#.....QE...QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE.y....B....@.....v..$..}+.....I&..Y.f;..$.=...Y....g..n.....nRW.L.%.9....9.c....].@.3H.o,.o^.Z./.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bqfE9[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	9538
Entropy (8bit):	7.916719778857752
Encrypted:	false
SSDEEP:	192:xYPkRlOViI4TEdTmxswRz5g7wsF6ihGuqYp9B3Y8xR3mlwtF8S8u:OMl2n44d6iw7g8sF6op9hY8HHtFX8u
MD5:	E2DE1BEA5F43F7646A53FCF93BBB984F
SHA1:	E22AEFBF24112B2FCA59A7FCA623A6964FC280F2
SHA-256:	5ABAE6AAD4345821B0FD2AD49D0D9473AEEF4FC69D0422E37185446356AED9E4
SHA-512:	B7EF610E3D3BBB404EF19AF64EBE0455332920CF5874D32A841672049471BD415AD3EBC176C1AD4B3445456960C08DBEFAF0E1B69C2D664290E0B3D28955BF5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqfE9.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=524&y=430

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bqfE9[1].jpg	
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.M..*..6.X.e(J.e...r4J~.z.<-RBd;).*..iZv$.....iXeo...Y.K..B+.|.Jz.5(Jb..S(.V..1..4.I.i@...L.D..Q @..!Z...S..|.a...9..q@.b.'CR..Z3..1..K/.5.Vf.w..I...s.R%.'..Z...+Df.A...e9d.V/+S..D|....=..05(ni.f!E..*X..6..F(..m..R(@)qJ.;...R.O.....&(.@.....@.....sR.L..v(....7..\sE.J.:...S)...i3HM.'.T....Nk..\...SL.9.....<Aa..e,..'.-2F..+7$k.....5.<VI.....{qN]j..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bqhpW[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	9465
Entropy (8bit):	7.9472224967729215
Encrypted:	false
SSDEEP:	192:BClQqaosuAITW7TJ7bL6tmMfkys5K43ftoi5SH1Ip3K5hwa05D/qowvD5dA:k0+FYTtrytwtor5hwa0E7o
MD5:	8B4A4BDBC183A252E32D3137CB4C1B72
SHA1:	BDD912B37FB149AE15B0236F2930DDDFF1947025
SHA-256:	F7982CCE63A0EACDD5F25257EC6C5DB0173F598B6C9F8CE6F29A99EC29546A82
SHA-512:	37675B61E6F0EE1CA4BAB22A4E563A22668EE3A7308F789CED7217BAEF78AA7956696D5E320E74282327719AC966977A09A1637AE2470D568A06936339D34186
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqhpW.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=748&y=318
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?....irZGov5.y.d.8..m..0.*..7..._..L{.....5...;..-.`...c.....*.z.i....h.....H`..Z.....o.q...E.}E+..|M".Q...|RL.'..>z0....c..... =.K.....RXf;.*.....?.....8...qL..+.:.....(....S2..P.v.....T.an.@VB:....F.|....H.....t.....(.rs...S.....<m#.H....b;...7oZ.4.....1.....s...&t..J3.B...=~....3.N.Z.L.....$....sR.E..ZZ..4. ...I.....o.V.P.....-wod_..I...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bqixM[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	10436
Entropy (8bit):	7.94320141953579
Encrypted:	false
SSDEEP:	192:BFPNB3e3h6ZObaowd/EJbu+GEX73ZnBbHi9yjLvtnder1QamPdBYvDlR:vLux2kmIbVGK3rjAyjLFl+Uv
MD5:	B7814CD62B64E5F172BDE2EE5F3BDFF8
SHA1:	FFDDF833EBC2CED8F63708E55BFE34AB67F548F6
SHA-256:	C531AF43D8C42F6E62658B8C0281785F99E965F393BB804A7CE451E3854409B9
SHA-512:	C368D80014C7BB7A9F7889EB48BC2679AC18131D47C0A0ADE2AC4221E378E3AD75DB46BB8F68B80E75B9F3CDCF0D71E783428C3B1591991A189E0A7BA3EE08 3
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqixM.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...`l.....8p.....j..{.>...r?.>.4\..Vy...=.*...#g.;.f....5u..j..._.8..65.n9.*.....+..t..X...Z...:{...h.K..=.>...P.8<W:....U.$.na.@ ..N.{.p..qy..n.d.....*....]H..pG&..Ay.F ..;[.?Z.'..T.?..*...l...f.U.N..2...sU."h..-..SF.....1H.c..OOz..Z..d....=jC..H.v.E<O.....=ib`.T1..h.}..f,.F..\.u.5....eo....R.....QW9.2.b.k..=.$..V.. /.V..yV.8..oB...$q...h>g...(.4..g,ZU.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bqpJ5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	8732
Entropy (8bit):	7.946727564789854
Encrypted:	false
SSDEEP:	192:xCSuAJg3jJMwLk5ncsIUbUU8k+GsTyzi10hxDkycHVxFnp1rJ:USuAJgzJj+IUAU85HOKGxDs1JZJ
MD5:	4DEFFC91FA2836BABD1A0C385C9F775F
SHA1:	5D161C54128E92C8294921A99495D8D6914FB82B
SHA-256:	764D5C2CE1F68D50D856987E0D207432C3DBB9C2DC078E5BE05F344DA550F1BB
SHA-512:	5DD37BF565E8EEE02F6E78687401DAFD02F7169FE44DCC4BA371EA04DD18747D4D97F42AA040402FAC3DE9CD36C627A19D6385E4D10EE1E33DFF60A18F7497 D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqpJ5.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=492&y=331

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bqpJ5[1].jpg	
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....4..Y.>i.C)U.z.....V:.}zx.-..k.o.zV.HGZ|..r.M..gm.[.;.MhGy..D.....qVV.D^$a..\\..o:/.r..F...o.*...Z..."l..(.Y..)*..{..C..^..%.....E...R..d..b9.....8D.I....tc&|..9.O...<P.-....G.RV.....nv.....H..).../l.z....W%.....s..4.....E...../2.@...W..Fp3.Wt.B}:Q,,..%....aX.\.1Ut.B-F.I..>..U.R..sN.....`...Tb...._..W0Y...62.O..R..H..sN..u..6.kg5#"..)..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bqsti[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 142x142, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	12350
Entropy (8bit):	7.940432881493806
Encrypted:	false
SSDEEP:	384:eOdCWVq4RrbfzOBfBxm0BVhLiuiTMvVrJ2Hy:e2Cgrb78BxmKzWuioAHy
MD5:	4986846000791E2EE3EAD8699A548501
SHA1:	08E3FE91DF5024D8E5AAF39FF71C009D54494646
SHA-256:	0901E2AF355114C1148DE394BA83EF427F209061D09A9345C883C7C9087D9CDD
SHA-512:	1C966DEAD1E2C1654C8F023117F77DEEDD15BFACDE22E10C3416CE7345E89050DD7FBDE652D4F21AC4596814BD96A017F68B25D9639EF60779A69E1C46BFC09
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqsti.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1438&y=749
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..1F)h..b.R.@..1KE.&(.-..LQ.Z).....P.b.Z(.(.....Z).....-.....S.(....E-..LQ.Z(.1F)h.....1KE.&(.-..LQ.Z(.1E-..QE..QE..QE..(...(..`.QE..QE..QE .(...(...(...(...(...(....QH..(...(...(..E.b.8&..;.....y1...4<=...~..#A.....Z+..I..[O.L..)%.b...Orh...Q^.....O2<.....4.V..] ...k..{...$xE..M....t....c.*....1..dz.q.....`.g..]..l.[F....'.....Y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bqwGV[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	21560
Entropy (8bit):	7.966481062413512
Encrypted:	false
SSDEEP:	384:OVvRRhlpBL5WnxUhB1kYMsu9uF/8p8XMtf8LCZO8GouPCSluxOtzzDMMnSeAGOeL:OVvRRhlpyxUhfGdut8p8cx8LCZO8ADBx
MD5:	D3889DF262B3770881A123D9978AEA8E
SHA1:	551060BBD45F31EB6FC584E3D516F445291B3660
SHA-256:	2EB493FC0FFDDAF3580277985484ADCD3E2183846B6029A5B591BC601312C7D2
SHA-512:	EA96ECAFCFAC8CDF75E4A78804E0E0151F131EEB790B09953EF731022B725DAF5AC88F88DA6F5E71BA7D29F11EC1D6776F461ABD06A43BB4E71F5D1DC9CE9FFE6
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqwGV.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..=>....z..dH.:.....Z8W...A.'.Y3.....3.h.Rj.yq....N8.+uf.a...,I'....IMA#.h.....+`...2....v...q...:..b...*.-..4....Rj...32]?<.....n....bl.....g..yx.5-.....5h./`Qb-...bG ..}.I,..s..e....Y.....Pp.cg.....i[..A"M..|.kA..W.1....L..L.O....W.....`.\t5f.._7.I$q..-.=p..m.P.fc.}3.V..ll.c..... ...W..?ByGiB..M.I%....V\.....t-..v...{..=.?O.....Dr. .";...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bqyxR[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	5048
Entropy (8bit):	7.8579962925927385
Encrypted:	false
SSDEEP:	96:BGEETvFtlWGWPLU/8ph9Rqkq42q7o3YzxFTdnwCY+4RMztcut3KAJXUxm:BFablbWPLUk/dJ0ovJnVYZRMpaAhv
MD5:	C863CAAC6E0AC5E8BAA7B8F1CBD293CD
SHA1:	787BC15E09597ACC6AD209B6C8B1F15833F4E6CC
SHA-256:	873E4C0195B71DCAC8529DB10453E557212C736C5D5D9FBEAA4C298290DA71CC
SHA-512:	1951812B179B5BF30006E5C186E2B799A1802E691F78237C23A8CC5E7E81196B556B7423D3EC15B0025B88030C68E89B80FFAEC62B7ED48E1B169B5EFE63C78A
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqyxR.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg&x=542&y=435

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1bqyxR[1].jpg	
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.D.t.j.z....sP.k.t..9I....[.^..7z....=kN.Q<.5..[Tk..V...n3.`...kJ..ls\.F.W,.../T.....RZ....sQ.*y...z.c..W7.....C..k...P<..Fk..S$..NsJEDlP..w.Z..4.f.d..AT.`....+q....."..UzU...L.x....,.....S.#....#.K..UccV..@..8.j-..@..N.....4"..Pj:e..j.....H..V.1.cse>...d.E.....xf.\.....i#Q..~.?....KCw[./v...>.P.-.H.T.g.N..Y..w..X-.....C,...g.F...r..\99.gJ..M_nj6Pj

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB4j8lS[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	502
Entropy (8bit):	7.275090598817661
Encrypted:	false
SSDEEP:	12:6v/78/kFqpMa5RkFIIAugOKv/pWdYG0VvgUnWevayqc:ofwzbx+D0VXWevayqc
MD5:	B5EE375D16BF365C12D70B587E622965
SHA1:	456F47ACEA559A58301BB22B1A97BA46EA4527FB
SHA-256:	757CC784CB24EB8903E4BF6751C6E221304D43E0018B720067E92C5CC69D07EE
SHA-512:	04E0FE5CC08811F02883B8C682F428A1490A8C87B1742F3E26AD08A806F13EAAC494E964792CE0F1604D4F95E75F364CA1CBC927E41EF4B867D421B31E13FE83
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB4j8lS.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O.._J.@..gv.*".=...P..Ui..E.....>.f.7.J.../...T..... ..b..nC.*..{.o...,....Qx\.C..J%.M..M.r.....6|.K..+...6....F...g...Z..N....G_.....@....R9.>.A9..mf.2w..N..4B....)..gm.....2e..b.&~.z....q..~s1P.... ...C.k"c....9.....q5..#EM...^..T....`.J..0..l<.8.%.G..9.....c....l....D..8...<.F2.a...7..p..1..5.]n .^...-+cDML....D.[N."..6.@E..=&^.J....<"..L .....@....27...B..]......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB7gRE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	482
Entropy (8bit):	7.256101581196474
Encrypted:	false
SSDEEP:	12:6v/78/kFLsiHAnE3oWxYZOjNO/wpc433jHgbc:zLeO/wc433Cc
MD5:	307888C0F03ED874ED5C1D0988888311
SHA1:	D6FB271D70665455A0928A93D2ABD9D9C0F4E309
SHA-256:	D59C8ADBE1776B26EB3A85630198D841F1A1B813D02A6D458AF19E9AAD07B29F
SHA-512:	6856C3AA0849E585954C3C30B4C9C992493F4E28E41D247C061264F1D1363C9D48DB2B9FA1319EA77204F55ADBD383EFEE7CF1DA97D5CBEAC27EC3EF36DEFE8E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7gRE.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....wIDAT8O.RKN.0.}v\....U....-.. .....8..{$...z..@.....+.....K...%)...I.....C4.../XD].Y..:.w.....B9..7..Y..(.m.*3. .!..p..,.c.>.\<H.0.*...,w:..F..m...8c,.^.....E.....S...G.%.y.b....Ab.V.-.}.=..."m.O..!...q.....]N.)..w..\..v^.^...u...k..0.....R.....c!.N...DN`)x..:.."*Brg.0avY.>.h...C.S...Fqv._.]....E.h.\|Wg..l.....@.$.Z.]....i8.$).t..y.W..H..H.W.8..B...'.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBK9Hzy[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	541
Entropy (8bit):	7.367354185122177
Encrypted:	false
SSDEEP:	12:6v/78/W/6T4onImZBfSKTIxS9oXhTDxfIR3N400tf3QHPK5jifFpEPy:U/6rIcBfYxGoxfxfrLqHPKhif7T
MD5:	4F50C6271B3DF24A75AD8E9822453DA3
SHA1:	F8987C61D1C2D2EC12D23439802D47D43FED3BDF
SHA-256:	9AE6A4C5EF55043F07D888AB192D82BB95D38FA54BB3D41F701863239E16E21C
SHA-512:	AFA483EAFEAF31530487039FB1727B819D4E61E54C395BA9553C721FB83C3B16EDF88E60853387A4920AB8F7DFAD704D1B6D4C12CDC302BE05427FC90E7FAC8
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBK9Hzy.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O.Q.K[A...M^L../+....`4..x.GAiQb..E<..A.x..'!.P(-..x....`.,...D.).....ov..Yx.`_.4...@._ .r...w.$.H....W.....mj."...IR~f....J..D.|q.....~.<....<.I(t.q.....t...0.....h,.1.....\.1.....m.....+.zB..C.....^.u:.....j.o*..j....\../eH.,.....}...d-<!t.\.>..X.y.W....evg.Jho..=w*.*Y...n.@.....e.X.z.G.....(4.H...P.L:".%tls....jq..5....<.)~....x...]u(..o./H.....Hvf....*E.D.).....j/j.=].....Z.<Z....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBO5Geh[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBO5Geh[1].png	
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	463
Entropy (8bit):	7.261982315142806
Encrypted:	false
SSDEEP:	12:6v/78/W/6T+syMxsngO/gISwEIxclfcwbKMG4Ssc:U/6engigHDm7kNGhsc
MD5:	527B3C815E8761F51A39A3EA44063E12
SHA1:	531701A0181E9687103C6290FBE9CCE4AA4388E3
SHA-256:	B2596783193588A39F9C74A23EE6CA2A1B81F54B735354483216B2EDF1E72584
SHA-512:	0A3E25D472A00FF882F780E7DF1083E4348BCE4B6058DA1B72A0B2903DBC2C53CED08D8247CDA53CE508807FD034ABD8BC5BBF2331D7CE899D4F0F11FD199E 0E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBO5Geh.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....dIDAT8O.J.A.....,.....v"".....;X.6..J.A,D.h:El...F,lT..DSe.#..$i..3..o.6..3gf..+..\....7..X..1...=.....3.....Y.k-n....<..8...}...8.Rt...D..C).)..$...P....j.^.Qy...FL3...@...yAD...C.\;o6.?.D|..n.~..h....G2i....J.Zd.c.SA....*...l.^P.{....$\..BO.b.km.A.... ...]|.o_x^. .b.Ci.I.e2.....[*..]7.%P61.Q.d...p ...@.00..\`...,..v..=.O.0.u.....@.F.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBSdFEK[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	229
Entropy (8bit):	6.32582687955373
Encrypted:	false
SSDEEP:	6:6v/lhPkR/EhlNkXiuYkCo/Vzj94mmJSUVp:6v/78/lkXiuYNMVjCdSu
MD5:	9464877AC3BEFD45D26A2C6B47FE193C
SHA1:	A04A44EA1FE78980E1423755071FF18AD6CE1208
SHA-256:	9089566EE7142F457AB4D29ED695CDC887A063D1ACECB6C69627F199AFBA5C1C
SHA-512:	4E58A99FAF309FD60F75AE348D1CEAFDA5E8668AECB3CDBC55E241C98405DC421374B365E4A620632950F9142F8D7A559C15100BD4DE95F4C5A88A11B0C244E 7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBSdFEK.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....\.r...zIDAT8Ocd8s.?....J..P\`... ....a....e.....f..55.{^^(.;8..3..[P.... ,....g.....bX..-....O8..p...w...(...T0`.3... 00....-....u....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBX2afX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	688
Entropy (8bit):	7.578207563914851
Encrypted:	false
SSDEEP:	12:6v/74//aaICzkSOms9aEx1Jt+9YKLg+b3OI21P7qO1uCqbyldNEiA67:BPObXRc6AjOI21Pf1dNCg
MD5:	09A4FCF1442AD182D5E707FEBC1A665F
SHA1:	34491D02888B36F88365639EE0458EDB0A4EC3AC
SHA-256:	BE265513903C278F9C6E1EB9E4158FA7837A2ABAC6A75ECBE9D16F918C12B536
SHA-512:	2A8FA8652CB92BBA624478662BC7462D4EA8500FA36FE5E77CBD50AC6BD0F635AA68988C0E646FEDC39428C19715DCD254E241EB18A184679C3A152030FD9FE 8
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBX2afX.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....U....sRGB.....gAMA.....a.....pHYs.....o.d...EIDATHK.Mh.A.....4.....b.Zoz....z."....A../.X.../....."(*.A.(.qPAK/.....I.Yw3...M...z./...7..}o... ~u'...K_...YM...5w1b....y.V.|.-e.i..D...[V.J...C.....R.QH.....:....U.....].$]LE3.}.....r..#.]...MS.....S..#..t1...Y...g..... 8."m.....Q..>,..?S..{.(7.....;..I.w...?MZ..>.....7z.=.@.q@.;.U..~. ...:.[.Z+3UL#.....G+3.=.V."D7...r/K.._..LxY.....E..$..{. sj.D...&.....{.rYU..~G....F3..E...{. .....S....A.Z.f<=.....'.1ve.2}[.....C....h&....r.O..c....u... .N_.S.Y.Q~.?..0.M.L..P.#... b..&..5.Z....r.Q.zM'<...+.X3..Tgf._...+SS...u.....*./.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBnYSFZ[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	560
Entropy (8bit):	7.425950711006173
Encrypted:	false
SSDEEP:	12:6v/78/+m8H/Ji+Vncvt7xBkVqZ5F8FFl4hzuegQZ+26gkalFUx:6H/xVA7BkQZL8OhzueD+ikalY
MD5:	CA188779452FF7790C6D312829EEE284
SHA1:	076DF7DE6D49A434BBCB5D88B88468255A739F53

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBnYSFZ[1].png	
SHA-256:	D30AB7B54AA074DE5E221FE11531FD7528D9EEEAA870A3551F36CB652821292F
SHA-512:	2CA81A25769BFB642A0BFAB8F473C034BFD122C4A44E5452D79EC9DC9E483869256500E266CE26302810690374BF36E838511C38F5A36A2BF71ACF5445AA2436
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBnYSFZ.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a....pHYs.....o.d....IDAT8O.S.KbQ..zf.j...?@.....J.....z..EA3P....AH...Y..3.....|6.6}.....{..n. ...b.....".h4b.z.&.p8`. ..:..Lc....*u:.....D...i$.)..pL.^..dB.T....#.f3...8.N.b1.B!.\...n..a...a.Z.....J%.x<....|..b.h4.`0.EQP.. v.q....f.9.H`8..\...j.N&...X,2...<.B.v[.(.NS6..|>..n4...2.57.*.....f.Q&.a-..v..z..{P.V... ...>k.J...ri...,.W.+.....5:.W.t...i.....g....\.t..8.w...:.....0....%~...F.F.o".'rx...b..vp....b.l.Pa.W.r..aK..9&...>.5...`..'W.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28
Category:	downloaded
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A57 40EF7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/64/a8a064.gif
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e. ....Q... ..-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,.A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.t]S.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.l:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....\|~\|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\fcmain[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	38647
Entropy (8bit):	5.089664389189447
Encrypted:	false
SSDEEP:	768:n1av1Ub8Dn/enW94h04o/ui5xYXf9wOBEZn3SQN3GFl295oYlI8BNlGsjm:1Q1UbOSWmh04o//5xYXf9wOBEZn3SQNK
MD5:	02D057D3980B3792BC6328BABFBFE0B0
SHA1:	7D6FA2FECB0E1D2FF4200B7B4EC987B8C6CAF98B
SHA-256:	0EA663B43B6A761DD236C27F461F808DBE686B47D398A00210262A284BC5263C
SHA-512:	672DB9199432AFDEB530A0F789B21485B6322304DB30E0A785DF288D8A2F239BCB8A2EA2ADD193B953DCB064FB7CA783FAEA31B309642EBDBF16AD454BFCA4 9C
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/803288796/fcmain.js?&gdpr=0&cid=8CU157172&cpcd=pC3JHgSCqY8UHihgrvGr0A%3D%3D&crid=722878611&size=306x271&cc=CH&https=1&vif=2&requrl=https%3A%2F%2Fwww.msn.com%2Fde-ch%2F%3Focid%3Diehp&nse=5&vi=1606513416433457087&ugd=4&rtbs=1&nb=1&cb=window._mNDetails.initAd
Preview:	;window._mNDetails.initAd({"vi":"1606513416433457087","s":{"_mNL2":{"size":"306x271","viComp":"1606512390995377805","hideAdUnitABP":true,"abpl":"3","custHt":"","setL3100":"1"},"lhp":{"l2wsip":"2887305233","l2ac":""},"_mNe":{"pid":"8PO641UYD","requrl":"https://www.msn.com/de-ch/?ocid=iehp#mnetcrid=722878611#"},"_md":[],"ac":{"content":"<!DOCTYPE HTML PUBLIC \"-\/\/W3C\/\/DTD HTML 4.01 Transitional\/\/EN\" \"http:\/\/www.w3.org\/TR\/html4\/loose.dtd\">\r\n<html xmlns=\"http:\/\/www.w3.org\/1999\/xhtml\">\r\n<head><meta http-equiv=\"x-dns-prefetch-control\" content=\"on\"><style type=\"text\/css\">body{background-color: transparent;}<\/style><meta name=\"tids\" content=\"a='800072941' b='803767816' c='msn.com' d='entity type'\" \/><script type=\"text\/javascript\">try{window.locHash = (parent._mNDetails && parent._mNDetails.getLocHash && parent._mNDetails.getLocHash(\"722878611\",\"1606513416433457087\")) || (parent._mNDetails[\"locHash\"] && parent._mNDetails[\"locHash\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\log[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	35
Entropy (8bit):	3.081640248790488
Encrypted:	false
SSDEEP:	3:CUnl/RCXknEn:/wknEn
MD5:	349909CE1E0BC971D452284590236B09
SHA1:	ADFC01F8A9DE68B9B27E6F98A68737C162167066
SHA-256:	796C46EC10BC9105545F6F90D51593921B69956BD9087EB72BEE83F40AD86F90
SHA-512:	18115C1109E5F6B67954A5FF697E33C57F749EF877D51AA01A669A218B73B479CFE4A4942E65E3A9C3E28AE6D8A467D07D137D47ECE072881001CA5F5736B9C0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\log[1].gif	
Preview:	GIF89a.....,.....@..L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\medianet[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	384364
Entropy (8bit):	5.484075060970784
Encrypted:	false
SSDEEP:	6144:leN9T2oOFvb2H0m943GNVLgz5QCuJbkqU21fij:lhFvye3GNVLgWxpkqU21fij
MD5:	9308F2EE3FC1EBD72AD815771D8D527A
SHA1:	04AA7F693CDC8CAFD205175C3AAC178158A61028
SHA-256:	69F24BDFCE7BE58D866F73C23317C599DEF2B2527625B08C89056C6EB4FD4C3F
SHA-512:	65CFCAB9A9B8D33A7516478FFD44B13678CA5BFE5B55B3B152B85D1EFD601F3F72D625ACEBB3EC5DA8CFF3EB42F03261B21550D846B74D305993741F4F2467A5
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";function e(e){"object"==typeof e&&(p=e)}function n(e){g=e}function t(e){m=e}function o(e){d=e}function r(e){"undefined"==typeof e.logLevel&&(e={logLevel:3,errorVal:e}),e.logLevel>=3&&w[e.logLevel-1].push(e)}function i(){var e,n=0;for(e=0;e<v;e++)n+=w[e].length;if(0!==n){var t,o,r,i,s=new Image,a=p.lurl?p.lurl:"https://lg3-a.akamaihd.net/nerrping.php",f="",c=0;for(e=v-1;e>=0;e--){for(n=w[e].length,t=0;t<n;){if(i=1===e?w[e][t]:{logLevel:w[e][t].logLevel,errorVal:{name:w[e][t].errorVal.name,type:g,svr:m,servname:d,message:w[e][t].errorVal.message,line:w[e][t].errorVal.lineNumber,description:w[e][t].errorVal.description,stack:w[e][t].errorVal.stack}},r=l(i),!(r.length+f.length<=1200)&&f.length){c=1;break}0!==f.length&&(f+=","),f+=r,w[e].shift(),n--

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\medianet[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	384365
Entropy (8bit):	5.4840815405857235
Encrypted:	false
SSDEEP:	6144:leN9T2oOFvb2H0m943GNVLgz5QCuJboqU21fij:lhFvye3GNVLgWxpoqU21fij
MD5:	1F22DDD0891E08C676F1146D67346EF7
SHA1:	C0F569FD5D656F7E604D2CEA44177AEE508CB239
SHA-256:	24DE932941F2BC4B5F962CCA29BD4735F805676C1A37FB7AEB5CE820BDE76B36
SHA-512:	DEE6D952CE909C9F7DFAEFEEB682A164DE547550F61FA0C1678CCABCC5F7977A56A5B62536AE7A466FE722A12FECC60F2A580CCFC41442C5424E5C399530EE2
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";function e(e){"object"==typeof e&&(p=e)}function n(e){g=e}function t(e){m=e}function o(e){d=e}function r(e){"undefined"==typeof e.logLevel&&(e={logLevel:3,errorVal:e}),e.logLevel>=3&&w[e.logLevel-1].push(e)}function i(){var e,n=0;for(e=0;e<v;e++)n+=w[e].length;if(0!==n){var t,o,r,i,s=new Image,a=p.lurl?p.lurl:"https://lg3-a.akamaihd.net/nerrping.php",f="",c=0;for(e=v-1;e>=0;e--){for(n=w[e].length,t=0;t<n;){if(i=1===e?w[e][t]:{logLevel:w[e][t].logLevel,errorVal:{name:w[e][t].errorVal.name,type:g,svr:m,servname:d,message:w[e][t].errorVal.message,line:w[e][t].errorVal.lineNumber,description:w[e][t].errorVal.description,stack:w[e][t].errorVal.stack}},r=l(i),!(r.length+f.length<=1200)&&f.length){c=1;break}0!==f.length&&(f+=","),f+=r,w[e].shift(),n--

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\nrrV97497[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	91720
Entropy (8bit):	5.417918168381897
Encrypted:	false
SSDEEP:	1536:Ght5EFuQkZu/ePhXO8InqFS0FkxcK+uLJXsD0voBZeTFuQNgaCpLf4LfcVFS:GhoghXZFpyEuLSkoLeTRCw
MD5:	87940B215EBED321358F0B3A40E7E821
SHA1:	B412235B3BF3229069D487ABFEEF28AA06811193
SHA-256:	4412C168BF8CFC076BD23DC69129CDD7EAA61AD5CCFF8828FB3BF84FD67FA8D0
SHA-512:	2ED8189A2B97DEE4042E8CB2BC063F4F7594C2EE6975F2EED7DEB7BCE3C5F9F8ED4B1BC2D6F984E0841CC940963CFFB5D595000E1514A42CE496034CF80366E
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/48/nrrV97497.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\nrrV97497[1].js	
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";function n(n){return"[object Array]"===Object.prototype.toString.call(n)}function e(n){return void 0!==n&&""!==n&&null!==n}function t(n){return"function"==typeof n}function r(r,i,o){return t(i)&&(o=i,i=[]),!!(e(r)&&n(i)&&t(o))&&void(u[r]={deps:i,callback:o})}function i(n,e){var r,c=[];for(var f in n)if(n.hasOwnProperty(f)){if(r=n[f],"object"==typeof r||"undefined"==typeof r){c.push(r);continue}void 0!==o[r]?c.push(o[r]):(o[r]=i(u[r].deps,u[r].callback),c.push(o[r]))}return t(e)?e.apply(this,c):c}var o={},u={};_mNRequire=i,_mNDefine=r}();_mNDefine("modulefactory",[],function(){"use strict";function r(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(i){e=!1}return o.isResolved=function(){return e},o}function e(){o=r("conversionpixelcontroller"),i=r("browserhinter"),n=r("kwdClickTargetModifier"),t=r("hover"),a=r("mraidDelayedLogging"),c=r("macrokeywords"),d=r("tcfdatamanager")}var o={},i={},n={},t={},a={},c={},d={};return e(),{conversionPix

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otSDKStub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	12814
Entropy (8bit):	5.302802185296012
Encrypted:	false
SSDEEP:	192:pQp/Oc/tyWocJgjgh7kjj3Uz5BpHfkmZqWov:+RbJgjjjaXHfkmvov
MD5:	EACEA3C30F1EDAD40E3653FD20EC3053
SHA1:	3B4B08F838365110B74350EBC1BEE69712209A3B
SHA-256:	58B01E9997EA3202D807141C4C682BCCC2063379D42414A9EBCCA0545DC97918
SHA-512:	6E30018933A65EE19E0C5479A76053DE91E5C905DA800DFA7D0DB2475C9766B632F91DE8CC9BD6B90C2FBC4861B50879811EE43D465E5C5434943586B1CC47F
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/scripttemplates/otSDKStub.js
Preview:	var OneTrustStub=function(t){"use strict";var l=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}},e=(i.prototype.initConsentSDK=function(){this.initCustomEventPolyfill(),this.ensureHtmlGroupDataInitialised(),this.updateGtmMacros(),this.fetchBannerSDKDependency()},i.prototype.fetchBannerSDKDependency=function(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\41-0bee62-68ddb2ab[1].js	
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):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F
Malicious:	false
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.localStorage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c.data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("office")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-dependent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAzjSw3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	6.995750220984069
Encrypted:	false
SSDEEP:	6:6v/lhPkR/C+kHocTbhb6Ve3eG4ZMPgeir16YDFkAgDiArTXqQkDSBulUMjfMD+8i:6v/78/YoY6VagM49EyOiAr7qRFjMMgyN
MD5:	FE6E36688E331DF4D28EADB7DC59BA21
SHA1:	EDBAB1D7C78149DFB01B8ED083DB5AB8FF186E0D
SHA-256:	8AE4F73BC751478FF2995E610EA180720E91FA3C9E69E47901AA56925DA0C242
SHA-512:	F5D627D4369FECE4BF72D321E6F9FE3B18408345E3EA489A74280E01417CA2B458AE9F31F0CBABF521116F80B9599FE989D5ACA7B26962DDBA9600E2FDBAC660
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAzjSw3.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAzjSw3[1].png	
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....o.d...TIDAT8Ocd....@.`..d.Af@..).....f.:.3pq.....b`.....(..Ez1.m-``fbb`ffbX.V...9...D."....).....v... ...`...`... ....w3....@...}....{0..P...4..@...t.~...p..u0[FT.A]N....P.8.....w....A..1..p.a..c.....`5 W".....%..}u.3-e.-..0l.b.0Cq.7.....^..U..(.....Nv6..` n=z....w..n?d...`.{....?..*!.#).rq2xX..n8t.,f... (%.p....k....``4/00..Q.f.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB14hq0P[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	14112
Entropy (8bit):	7.839364256084609
Encrypted:	false
SSDEEP:	384:7EIqipbU3NAAJ8QVoqHDzjEfE7Td4Tb67Bx/J5e8H0V1HB:7EIqZT5DMQT+TEf590VT
MD5:	A654465EC3B994F316791CAFDE3F7E9C
SHA1:	694A7D7E3200C3B1521F5469A3D20049EE5B6765
SHA-256:	2A10D6E97830278A13CD51CA51EC01880CE8C44C4A69A027768218934690B102
SHA-512:	9D12A0F8D9844F7933AA2099E8C3D470AD5609E6542EC1825C7EEB64442E0CD47CDEE15810B23A9016C4CEB51B40594C5D54E47A092052CC5E3B3D7C52E9D67
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB14hq0P.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..ii(....(.h.....Z(....JZ.)i(....(.....(.....(....J...+h...@....+...e.9...V..'."!.@....|.....n...@My..w9;.5I...@....L..k...w2.'... M8)4..>.u9..5U.w9,M(....!E..!.[.5<v.?AV..s...VS....E5v.....Q.^jwp*3&MJrf..J..|p...n .j..qW#.5w.)&.&..E^..*..."..T.....y.U.4.lK.sK.ooj.....Z..3j...".)..c..~... .RqL...lcym..R.. gTa..a9.+....5-.W'.T@.N.8"...f.:....J.6.r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1aUsw7[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	16057
Entropy (8bit):	7.897945706053911
Encrypted:	false
SSDEEP:	384:7NdQcqxUrji7gQl69r411+lopeoAc+2Xh9N1I3:7UcWSjicQl69g1MloAb2X7o3
MD5:	5F73A34E9EB19376A5EA98AC404AF48F
SHA1:	3A2E27925352DE9A67A94E3014A1FE46C2C11DA8
SHA-256:	A011E9F2D4CB505AD9CF8846C1F38A1867E6B20E285C2F1D44CB9531BBED37B4
SHA-512:	2269CC1CF2DB8555DBBFDCAE6EBFCDDB3220CD0D2D5E79041487FA334B26CA2C1131AD7374A1792BDF8379B5A82B8953935BEC5C8B7E36117A6091EE9DC26B2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1aUsw7.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...R.Z.#..R.S.!.)@...0.....C.....ZZJZ@-2I..z..sT...8...$d.]..~..\..P~.j..>~QN.Q+...V.P:.M.)....j....cO..I..?Z%@c$ U-4b..|.Zk.][9&..NH.jvS.'.[V.t9...p..H.#".hc...Hb..(...E..-.Q@.....(.h.R..QE..(..@.QE..QK@..Q@..Q@.....(...).QKE.%..P.QE..QE..(...(...))h.....(.....S.w..8RR...i.....R..S. ..1iE%8R.....lp....e.....4.s....{.i%[...S$..M.A..&.E-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bdz6e[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	38850
Entropy (8bit):	7.9724164314581625
Encrypted:	false
SSDEEP:	768:7DvZhicRE8eMc1hJaBMk6Cm1J/vQb3Ov4LZnnGQVluNY/f98rFA:7Dj7uMy0qk6bBvfgL1T/f9Om
MD5:	6CEF5DEDEA9217D8DB1B5370E2E77B49
SHA1:	4B0B183BF461F4D3BE7A83D24C28B9B2CD309CAE
SHA-256:	0315836561F3E11E08FB4D2E2C981268C9D797996D7F1F93DA8D5C6E8E90DF3E
SHA-512:	08A5451D4EE71263659470F33CB0CD97C5AC2AF938BC181E9EF8008CBF82B8D950E5B9CDA9E1E8B1F41AF7D5988962945A45AC5205B515918C943D776979FA9
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bdz6e.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bdz6e[1].jpg	
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...b....Y..bk...[f (#...c.8C.s..A/Z.$...FEbO..xL...U-...:...N..N.2...apr+... ..+^&.VS+.m[.L....f.O.k.a...mw....\K....I R...x..*Ta....Q.z...hv..6...-Df..+sL9._.cj....k...$d.!.~....aW.1.+....6l.H....H.....S[B#...9..Y.S...lZg.V..=*(.)..4.{.j.....b.....jY.8..Td.p..yu}..UWT..9..s..j.....i=l.w..N9..>..ml.!e...o}.$~.:.."... ...M..p1)...a.3SN.z..S...!.x>....5..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bo8x3[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	12143
Entropy (8bit):	7.951495982029468
Encrypted:	false
SSDEEP:	192:BYHJxd8DctOqCjZRpbDgt7QeUWfWY9NSyu1cSTOvznDb/mHSar51GKbvVn4K2Ylj:epxYpjZRpbUhkWfW5JDorDbmHSu5RrVn
MD5:	F1E20950A10B4EAE350F10C40B00F874
SHA1:	C1E419F1DC262EE06DAF2EDF88AD4896B43DC08F
SHA-256:	48156A2D2468E711A36E6B04A45DFEF876F9A4A45209CE5E07160FA09A54E341
SHA-512:	7F9154D995BEC6B3914B70559EA02969138DE732D4F2C2D4961B66DD2974B71B8D57739B3ADB597F8B9217E77B4A4101AD912868B2B4FDA2B52EDB89B25E986
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bo8x3.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=390&y=349
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.....7ZI7*C....GqQ:.RA.h..f[8.F.....Z.W .5..1..@%..\..r.I.\.4.W].u.D:..4.9K.\....S.....o..*...f.m!X..X#.d. .n..gz&A...=.@.o.`.....m.d.{V.[..s`0....2.....S.....Dz..l.r.i&f#..h..&..X]<...E\.H....Z.|?^*..~.g.3.m..C.e..;43.$...k.X.m...}+..[.U./.H.w..}.cZ.....H.....{..}.n.8.Y.].i..#.j8e.I.a....:..4Y...-$.g.. ..XIpaL.SQ..u+l.....L.I..Y.....%a6...=...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1borR4[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	7438
Entropy (8bit):	7.929805759931841
Encrypted:	false
SSDEEP:	192:BFgKi3/6UEWgrix+3SF2qDcqjQvflV51KySLsOhjoefa02G63DY0j1ws:vgKsCUEJHiFrDnU3lV51Ky+4eIT91ws
MD5:	D55F0E083F7DA24D174205D81BD89113
SHA1:	B54A9317423019397FA8C0613CB59C921FC01A01
SHA-256:	8585E941FF1C1582AEC9599DCE3DE4394D44FF260EE3B6F7D70EFBC088DD3635
SHA-512:	CD8C5071C6EF7BF8B27ED40720E423C5FA0B378EF58B86C6DB4AA690C2DBDC8583344F26DA62D90FBD100F6C3057537D0AFCC027318471BAB8E03BE55AE340 2B
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1borR4.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg&x=2137&y=1023
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?....ll*...'\TS..x...).....{t.. !'..}<.7.\nL.G....V.k.b.;Oz..<.....Y.EjPe..._..V#.cU....e"Z.....Q.....k._.._k.o.Q_.c....N.T..n... G.(O.....J.z.J|.4J..^...:m.r.....<H...jy..C.D.....*Q...nf...} ...q...l.P..c..`..k....*...>d?.K..S...p....:&.....!...G!.....5Z..}Z..p.....*.uv....S.M[t.J.r..... .`.[.4.-..].`!=j..$.....Z..5....`....%....[. [ic.U.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bq2xq[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 200x200, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	16833
Entropy (8bit):	7.9542459011491236
Encrypted:	false
SSDEEP:	384:ON9+hS3Ygt4b9IhKzIfUxwjuNoLHQg3g0UVEPrChjC+2WshQ:Oj+hS3DGIszIcxQLwgPEqr6B2WshQ
MD5:	F201FF4208916B61D8994339524BB862
SHA1:	F9D22E88B7262E947B4A6804D7E89F3D008E06A1
SHA-256:	B4D2437D8FA54099A5E24750E0A77F803351ED0AF92AF5E76D99737DD21F04EF
SHA-512:	8F1052C9E8622A41B317C54E112F4C97C1B7EC7E0F7C86A4E553058FE04359F0E8AF5B71C8A781F252E02D26591DAA885AC97B7CA7E0759F2452CED7AAC8246
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bq2xq.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bq2xq[1].jpg	
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..:Z(..E.P.E.....Q@...R.(....(...(...)h.....(.....S....p..j..#.....J,..2+..h....I.S.$..*)p}(.H.R.@.KE....QL.....J)h..tU.g8M..*.....L.ciiqF.{P.QN...[zQp..Zx..)..y..a.R...J).....\,EEX[Y.j.l.....Tb.F.{..(..C.fPRz.z.....2V..L.,kP(..(..u..Q.,..O[5...q....v..D+m..)v..).I8..1E.P..(.'...-..DNqR.)&....5...."...qRco..^.+.D'.D..y.{p.....4.'.gIb...v.q..n.T.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bq5eA[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	5698
Entropy (8bit):	7.865472010835922
Encrypted:	false
SSDEEP:	96:BGEEf1L7T2jOMcXeAn+gogtMjZ5LxjyBTmrFw624GLHdO65vK+r0vvBc9CTSqXgx:BFe2vQr2BE2FcE6FK+i5jGgo
MD5:	5A061B69FAC737B39C70E6719C9CDEDF
SHA1:	0499C3A51309EC23E7D77678DC24A0214E79A3A1
SHA-256:	847E6EF74FB1279CFD5DE8FD26CE660527455365F7D60EFC487B582CB15C72EE
SHA-512:	5A7B2ADF0B4A953294F120A77E713AC5F1AEF4E8017A43A8D790D8180C10B863837FA14B1AB26E7AAF5CA8C6D595C20351AFE84C9CBCCE7750AB2B3D52132D4D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bq5eA.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..O..O.....4S..(..@..(....).h..S.J.>(..F..z..4...NAV.....@...[..[....I..M....D+...0).R-<..LR.Rb.P.c....m.....4....N...@..&).(..0.f*R)1@.b.).T..^H.....?..Sa...E...M...!.1.....<.jP8..0..q.B*F...@..HE>.h..SM<.M.0.KE.F).)...8R.p...<S..R(..QZ.N.{.3..Ub.fl.m..SF...i\;.'.en7.....cW..Kca..b.....?.....-(.#.\.Ws..>.r...U...e..-..?...e...->...n}J.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqdFM[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	downloaded
Size (bytes):	1908
Entropy (8bit):	7.726894571855442
Encrypted:	false
SSDEEP:	48:BGpuERAH7+jzl14XrYz+cI/sK4+la01vMLo:BGAErQUCcksKPla01ULo
MD5:	36FCF0BE1586215BE3DE097A68DA7CB3
SHA1:	A6BEFEB9729D8B271CDA0AA156EAC00E69BA13E3
SHA-256:	7105C8356BFC919278B00BF7A83A8E9073A8CA9AF1213548F872EF9455135F08
SHA-512:	2739B4028261ABB3D590D07977958003AABE7B28FEE624AA28A5DB4DB6E0F70F1D2CC69BE674C5EE41E69AE1F2A1BE8D020F2AE71255A6404418 64CC78FD1BF5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqdFM.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg&x=596&y=258
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....Z..;d,..p..e.g...V%....6.g..e.$P).5.}O.e)hZEK.....N.6/.FO....'s..c..tKI..OA.....I..`U..;Vo.L..%...V.a.....).B.Tu..".!.pjWd..*.%.^g...}z..".A.F__.T.....}+P.....~...;.<~b...*..Y...51.!!..1Vc.2F.[.R .G..s.2.xQL.....E.i.8.#..%`.....V.`[K8.^..>.g..&.#...1%.....L.....V$..O.1.SY.K... ..\..;i..!g.#.rwq.j...@..pF.. .r.....'...R...LZ...<V..7S.uY

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqdHn[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	7514
Entropy (8bit):	7.942409253232958
Encrypted:	false
SSDEEP:	192:xCs2EennqfUiD9+isb+3xrdrJKg7AmL+sQutlae3:Us2EonqskEV+3xrdrJd7AmtQA8G
MD5:	548A952B02EBA43291A22DD4C6B1B875
SHA1:	789241A886119A85D1ECABD1E0803F433C04E66D
SHA-256:	7332784F84EE451C0C2E04523C4DCF542DA1CBD8F3C41EF3A3F185331A4164FE
SHA-512:	37990B0B92CB8AD5325BF3D89400A6F8ECF808F5E37B7E2CAC199AA383DA75E4EAA3F61EC96A1378A92649FD83711964A8D6F72E62F1D4658822CA307377DF2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqdHn.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqdHn[1].jpg	
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?....m..\...0..j..U.....6.H?.55K.k'....G..Z.C....V.....l.....Y0..k...J.oC:h....=..[*8.....'...h.1{..J....A.b$.4.....i\....t...OI..g]... <O.,...or...O..?..>..Q..m.5q..U..U....:#....O...P.N!O.y... ..h.:..9...=..cT...k.E#m!"...4.....@s....}+.e.o%..W.j#.m^yw..J?..U...%P..7..|.R...c..-..kJ."..P..n*.DOK....=._...^kg.I..^.?.#...Z.- ..7s.{.;.F...qm..../.Q..M...G2..gv.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqeN4[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	8587
Entropy (8bit):	7.93777261537888
Encrypted:	false
SSDEEP:	192:BF+ZmhHBmctwuUeqbNlN3sgQtL27lE/W0TorqN6XDahGFu:v+ZkHQctgFNvh3E/1sqN6zPFu
MD5:	031088AFB7C013746FF0762137026011
SHA1:	2822EFFFD110B598D9F89F71547C8DC091F081C8
SHA-256:	8FD32152CE7FDCC36FB35E875C5D83FE172DBB7A37D4B32F8C44C86517A46C13
SHA-512:	1776349C0189D6E52D7C02E6FFE928884EA2DD73FEC0D6A6505E8208198DD615306AD6B7CDF0EA472C77EB8448F3921E943D72D87D68007ED6A6AEF2F8D5A5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqeN4.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..E.HG.).cVE.+.5.6A.[<S.1V....`./^.I.....&..1PL.<U...H..Wo..LP{.P..8..Y.c.P.).F....n..U1.k.YL..,.=ME...!.<..b...J.- .,M.@kn.U+..:....9.g%q..A.J\...H..rjXe..}j#.R%..cUf. .U.@{RK...j..2c.Dl..q..n.A".cDl.qX....l...V.e..e....W.....cIW....<U.9.....v..+.z(.5v.v0.El**...Uu.=.....{.....>..]....n\..sW..V H.V.NI"...p.qP*...#..e.,...U..m....m..-.&I>..E...{.Lh.9.;z{...%..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqevD[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	9754
Entropy (8bit):	7.94583332976925
Encrypted:	false
SSDEEP:	192:BCH5DxBsXTdDVJxlwr/4W+Kq8SPbuG41o68S+PzduX3b8:kZDsDdB74AwqpCb1VJ2w78
MD5:	10CEEF4D6BB855459B6FD0A81D6F5095
SHA1:	29316EA7D0A2EDDE513F69B02D936DDBE0D33E7A
SHA-256:	E54946F79581F2D2B30AC6A47CF1BB161629642AD0B83360914D890E1BD36473
SHA-512:	F13ED518A7F3FFF4875B3F159407371C30B5A0D78D404A46548F7AB3E5D38C301296F6D9260F83EA78AE26A3774B88B0A8571C9A0165B603EC631F5D5142B534
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqevD.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..^....E8..).b..[.-.sc>...:.....G.o...(.....7.....q.>.9.H\.....>.(..V..[/.4.jF7.4gg...h.....w?.5G.>...Z...0[*3.....O. ..O.A.3P.<...?g....k{....`...z..i...%.#.P...P.....;...*...:.)x.6.$pA..?5b..Z}...<....3.....H.^..76.}On...:m.....#..K..SR$..W^..<...c..rM.....0.g.(..8..?.....[[M...H.`..p..Bb\=.&.+%....[...0.?. .....uT.]..P..Oa....S1.=..m4.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqew7[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	8005
Entropy (8bit):	7.927136392406839
Encrypted:	false
SSDEEP:	192:BF17+yAmXxwEExbHHqweYsVrjG+ZfZqvJKWxMKn4qa8Zu:vE9mhwEwh4m+xZoXxB4L8E
MD5:	52072C30742AD3265D8CE47B7BB4A1B2
SHA1:	F8EABB30995F5073CFC452241165AB3D7F337726
SHA-256:	5E60644C9BA8333D78E387AC321F0FE76D83F7EEB29F1F5B6199799E9023D2D4
SHA-512:	32D0A66E830133F984BA55C8B775FE50EFD3EDC57247681D8A15336B2D724E079EF3061476D48B8C03CF59DF0A8A1B622A002C014F2901184E38446EDEB4445E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqew7.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqew7[1].jpg	
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?.....@.,Q.`.{....$e.....j..t_=C0.H4hc..+9.!.c+.[.2.0...Qlb.pA..Ka..m.....(....J.q.W..Ci..WK.."B...ci....+...a..)bk.. ...wvF...v..+...V+..Wn..t.+....Xa.....A.[n.y.+..*}+3F.....j.....]5h.../.....q.*9..)<..lc...5...N.1\...j.U[.....P...r.q..K.Y.....oqtl"b"..3...A....H.c$..:..3.K;....>.5.ZV.....h.2G'.=....\..hC*.!.. .6[.d..v,..sU.`...U..3T.v.q0`x.?.P(.'m=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqfpP[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	7696
Entropy (8bit):	7.934844814228387
Encrypted:	false
SSDEEP:	192:BCtE7DeTZ4Ax29YN7QIZIudRuth2jKBt71SRWe7cDy/BET3H:kePuaFPth2mL79du63H
MD5:	B36F90282E5F293B982C826D558A1DB9
SHA1:	A8608881AC83827C1B740AB91614FA6E8A7A8B1B
SHA-256:	4D2FD19B15D711A1EDC97733935731B32E84448FC10B60EA58D14E2D6806D811
SHA-512:	B769CC1E131FF60440881B9CAD66A3EDAE25C76C9A092416E23F5488B1CDC9489FB33CD414B9DEF1668A3F34E94754F1088190E5D6321004066EC6F757FC8E5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqfpP.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=609&y=191
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..a\..zb.....B.b.l....74.5.w&.....6*lRd..j..f...4..e..|...L.....Mm.iv."...82M...*gV1...c..c%.....'...\..$q.S...../.. .^...U....V8..#.U....wH.....O.....1=K.!A..u9v.x.O..Vl.....B....9..)r+.h.f...$)5jv.<.U.!.V..)...+...Y.c.\..J...9...-..m..Vmb..5..4O.W.UV.....>..N.Tu>.".k.7..Fq.t.E&..I.....8.k.S... .Y.%m.....@ .f..?LH0..:.n%L.r1..#.W.^{.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqfyq[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	17116
Entropy (8bit):	7.961724706136161
Encrypted:	false
SSDEEP:	384:OV/Rnvk9u2s8HFjJe8GgFfVQMobLXDappk+nRwrmLFH:OVpvT2s8phr9ojapPfpH
MD5:	50C59EEC1EB5AE22D37B176AEFDACF83
SHA1:	FE5C7EEC37D3F46ABD6E2A6CF4F1C5EC3345D089
SHA-256:	30050069D4251865ABC16E4109D3987CB9AEFD08F9D3AF37625CBD2ABEA0F4C3
SHA-512:	E0EA9E179EB9B582E0D773CA5B66C0A1E27A96408760D59DFE4B738E96E6780111194C8B9A30B4AF4CB97185A84F93D7E9280B84F0B72922C9E1FE7E572E31C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqfyq.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?...5:..YjE.M.JA.F*+x..8...c..E.,....Ke$.* S.b..mi..l....\..'.5..1.?L....._).W^..X.....,..P.H.=.Zv..-.~..T.? ..U.....m..[.f.W..=.....~T.....W_X..F....Z.'._..i...o.....Y...kL.s..$C....>...`h....J:...{.....f../.)...D..y5.]Y...~.....].Z..Cv..k.)^...<..Kv).....bNy..2*.<Sw.X...j?2....I.Aa...I..... z.C..9.0.p0...QZ...d.\R).}....ZcI...&.c..i3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqhu1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	5179
Entropy (8bit):	7.883797909280466
Encrypted:	false
SSDEEP:	96:BGEEQslaQFWiOJOIcWl8LcDcoQsT+iXUXPh8oF8LXMrDg7m6pMI:BFDaxFW2WlOcDcoWtD82c7mI
MD5:	2CFE0BA8DD7C4CE1E05188A8FB6C2124
SHA1:	EBFCA3C77C6E10A1421EE1487AB14C0680E252D1
SHA-256:	D9DA28DA26FD94ECF6E68A94F08810E09DE90AB1CA33A8642F07AF5CAFC6BFFC
SHA-512:	AE1295779E89DEFC343B593CA25548964A5B240EAE6E8F97505A847E1CC955AD9662F983A0EB2125F9EAA23B3CF5F8C1726AE756494A0C22C54E4CCAD9652F6
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqhu1.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqhu1[1].jpg	
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..qp.}..P..^....d..x.....L..L..z..<S.AN..*A@.%:..v....SR../6..u .C....wC...o.....k.]...*,.....01X._i.q...G....9-lz..sn$..... Y..l.`.T.m.*.s&$.*. ~um..v.9..gBW*.....a....qSh..A0..X.Q..f.G.U...9..vS$.2p2q..3.@...[.3.E."..T<9.L.z.jc.C&.z.Z. V..7)...r.8kA.....Z....L..Q@...).T.P0.....H. ..p..S..1.S.4.x..(.... R0....-.QH..(....K..n:...$....4lJ..Zb,..O\f.....^O#...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqpMv[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	13465
Entropy (8bit):	7.940126346926118
Encrypted:	false
SSDEEP:	384:epRqDZOMEuH/l7wvBtyxVGXtTTou6L570:e7CH/gwvBAG9Ts3Z0
MD5:	948079EB95BE08770F67F1892F4CCDCA
SHA1:	232BDFF8AF4C0988B7AA3F6F197836B39175DEBD
SHA-256:	96719F48A869D39EEA551F5CB23219866CA3372B52FED9348183B446A77A286C
SHA-512:	23A9868AF7C628C8608275373DE21ECB3B62A2474DA57BB1634E9F5A4738C785FD7BB97F0D47623D2A173E28CEA2E3D27D0A147B19B2B94B85A0280634197449
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqpMv.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?...(...(...(...(...(...(...0.A.\...G&.,...:t.T`..l$\u1.o.....W.P6.b#>....g.....aU>.....-..m.O..n|.=.R..J..... .....*....O.J.....).pGF_..b.....=2..5.Z..M..... .y.H<Q...}.....P..Z9X.....vo.....?...}:...,..w`.G.Vc..FE..(...(...(...(...(...(...(...(...(...(...(...(...(..#..gn..4..x..Hb.H[k.4...6...r.j.;..5r... \...k.}.{d.?.#q.u..<.I.;..`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1bqrbd[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	12434
Entropy (8bit):	7.953523603736893
Encrypted:	false
SSDEEP:	192:BYa0R7tPI1FHrbG0Hcqwx0HWZqIYkFoJfSOkl5iYFXNhnZPW9u4:e8fHXY0gt8tkl5hFXNhnZuE4
MD5:	92983B8F3377D0F0EB2F49D27AB09B01
SHA1:	26FF90DAC113D22D90DA04ED0D12B1DC2A752214
SHA-256:	E03B9F424A030CB6BC3FE4344DBAD292FF65277A17A1C70C5C7E1C5A052A08C1
SHA-512:	877B969102DC9A09DC9CFCB1F52D44D92C70E1A14F5911252E57DF8E926B0F5F3283726D27322D023DA9A24EC639F04C12F81894FEC06F7EFA57948EB5257AA
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqrbd.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?...>.>....+.j..^7.#8....E...&...SHy..S,i.b.....R.K.@4..M.}....4..1.1N"....R.N.b...R..:.."....j..X..sF.?..k2. X.....:..=..J+.<.h.....J.))sI..ZJZJ.3E...ZJ(.a^]....=....k..l6..\wU5.u.P..Ni2i.....q..&N(.3q.q..)4Rf.v.B.Oh.....4_$gr.y...r.{U..G..dt.z.T...m.YX.x..z..;|.A.3.Yy5..[..'..Q.n.,}.X.....G. .ojvb..i3Qo=..h.\.4..n4d..Xw$...}i..:.h.J)j M;q.a..A....X..W9...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1kc8s[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	799
Entropy (8bit):	7.616735751178749
Encrypted:	false
SSDEEP:	12:6v/7ee//6FAU+ZPhOPnAgOydY9vYyfS1Y+OyGo0VtgzKkcbqeGOrlkTR+a1eXGyI:QGp+Zpajd4/ObGPngzKkcOSnGLT
MD5:	2C55F358C8213245D8DE540D89B76ED0
SHA1:	413A0EA00DBB2A54C6A3933B8864E1847D795124
SHA-256:	D11901D46370D97173C94754B69E90D7540FAF1F5C571C5E521E3A062FBF0A77
SHA-512:	0385C2FE61CFFF69EE6A85D13003B4729B93132007294DF3407DAAB97318157C421940D689E01B6CE5360A57029393FEAB949A83647DF22D43DF5064E7B82DD0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1kc8s.img?m=6&o=true&u=true&n=true&w=30&h=30
Preview:	.PNG.....IHDR.....;0.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATHK.kZQ....W.Vc.-m,...&`....`."....b...%...E2...&.R*...*...A0.....d."......>o-i....~...9...=?.!C.\{ .j.bmmMR.V_.D.....P(..j.*.Z-]..?...uV_...>.o.e.o..a.d21....|>..mh4..J.....g..H.....;..C.R..".....J....Q.9..^.....8>??O.zo.Z.h4.N...r9...).....>R.9...Kz..W.T....J.w.3fee..*a; .....+.X._]]....?q.\w.Ri.n.....p...CJ.N.Y....l:..).....d2.5..1.3d....\.s....6....nQ..Q...E..d.....l..B!2...G".H&.....ag5..ZR^..0.p.....4...\.2...6.....).....Xj.Ex.n.....&.Z.d.X..#V.b..l ll..[...&'i.....x....*8...w3..=.A...E..M.T..!8...Q(....L6)..r.....h4..>.....yj...j.9.:....f..+'._#.....j..I...&.0.H4....<R...:....7.Y...n.....Z.s..2.....#A.j:s.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBY7ARN[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	778
Entropy (8bit):	7.591554400063189
Encrypted:	false
SSDEEP:	12:6v/78/W/6TiO53VscuiflpvROsc13pPaOSuTJ8nKB8P9FekVA7WMZQ4CbAyvK0A:U/6WO5Fs2dBRGQOdl8Y8PHVA7DQ4CbX0
MD5:	7AEA772CD72970BB1C6EBCED8F2B3431
SHA1:	CB677B46C48684596953100348C24FFEF8DC4416
SHA-256:	FA59A5A8327DB116241771AFCD106B8B301B10DBBCB8F636003B121D7500DF32
SHA-512:	E245EF217FA451774B6071562C202CA2D4ACF7FC176C83A76CCA0A5860416C5AA31B1093528BF55E87DE6B5C03C5C2C9518AB6BF5AA171EC658EC74818E8AB E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBY7ARN.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8OMS[k.Q..v.....)&V*.*"./(H. U..|P,.....DP.}...bA.A|.....J..k.5Mj..ic...^.3.Mq..33;.\....*..EK8.".2 x.2.m;.}."..V...o..W7.\.5P...p.....2..+p..@4.-...R..{....3..#.-.. .E.Y....Z..L ..>z...[.F...h.....df_...-....8..s*~.N...|...,..Ux.5.FO#...E4.#.#.B.@..G.A.R._. .."g.s1.._@.u.zaC.F.n?. w.,6.R%N=a....B:.Z.UB...>r..}.....a.....\4.3.../a.Q.....k<..o.HN.At.(../).....D*...u...7o.8|....b.g..~3...Y8sy.1IlJ..d.o.0R]..8...y,\...+.V...:?B}.#g&.`G.....2.....#X.y).$..'.Z.t.7O .....g.J.2..`..soF...+....C.....z.....$.O:./...../].]..f.h*W....P....H.7..Qv...rat....+.(..s.n..w...S...S...G.%v.Q.aX.h.4....o.~.nL.lZ..6.=...@..?.f.H...[..I)..["w..r.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBaK3KR[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	551
Entropy (8bit):	7.412246442354541
Encrypted:	false
SSDEEP:	12:6v/78/kF5ij6uepiHibgdj9hUxSzDLpJL8cs3NKH3bnc7z:WO65iHibeBQSvL7S3N03g
MD5:	5928F2F40E8032C27F5D77E3152A8362
SHA1:	22744343D40A5AF7EA9A341E2E98D417B32ABBE9
SHA-256:	5AF55E02633880E0C2F49AFAD213D0004D335FF6CB78CAD33FCE4643AF79AD24
SHA-512:	364F9726189A88010317F82A7266A7BB70AA97C85E46D15D245D99C7C97DB69399DC0137F524AE5B754142CCCBD3ACB6070CAFD4EC778DC6E6743332BDA7C7 1
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBaK3KR.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O..9,.q..:&.E..#.,B".D.Zll..q,H.....DH..X5.@....P!.#.....m?...~C....}.....M\.....hb.G=..}.N..b .LYz.b.%.>..}...]..o$..2(.OF_..O./...pxt%.....S.mf..4..p~y...#:2.C.....b.....a.M\S.!O.Xi.2.....DC... e7v.$.P[....l..Gc..OD...z..+u...2a%.e.....J.>..s.....]..O..RC. ...>....&.@.9N.r...p.$..=.d|fG%&..f...kuy]7....~@eI.R....>.....DX.5.&..,V;.[..W.rQA.z.r.].....%N>\..X.e.n.^&.ij...{.W....T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\auction[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20953
Entropy (8bit):	5.766258047616982
Encrypted:	false
SSDEEP:	384:JK6TgzJFJdTglVOGze1I9zqF7VubNsQVRCQQsddRYOUTDqvmtW028VCVwrTX:JLTgN+OxLuBsap1U/y4RX
MD5:	5D90DE5247D4AF272FC67A85EC3F989A
SHA1:	E9F58A5FBCE75A9A1325F5B4C24053511174C0BF
SHA-256:	B7DD07D4DCCF8CF48CF38781B05A43C4380A393166C233A7E0B63B543AD61E6C
SHA-512:	4ADA7D07448B1390A2D2EB8573FC599329EA919785556873AC8828E0DF73E2008DC99BED8FEA1F03F9AFD796005A5A93AFF0E271477705B19318D0DB5EE204AE
Malicious:	false
IE Cache URL:	http://https://srtb.msn.com/auction?a=de-ch&b=ef8b497139bf46d1a2ac40fcff94f1b9&c=MSN&d=https%3A%2F%2Fwww.msn.com%2Fde-ch%2F%3Focid%3Diehp&e=HP&f=0&g=homepage&h=&j=0&k=0&l=&m=0&n=infopane%7C3%2C11%2C15&o=&p=init&q=&r=&s=1&t=&u=0&v=0&_=1606545815944
Preview:	.<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_7f7ff3a71a000ab0e393f37a80eb126a_15d04d58-66f6-4d1c-bdab-0c9161e4a33e-tuct6baf88b_1606513419_1606513419_CIi3jgY Qr4c_GPC18c3NxpW3HCABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAQ"},"tbsessionid":"v2_7f7ff3a71a 000ab0e393f37a80eb126a_15d04d58-66f6-4d1c-bdab-0c9161e4a33e-tuct6baf88b_1606513419_1606513419_CIi3jgYQr4c_GPC18c3NxpW3HCABKAEwKziy 0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAQ","pageViewId":"ef8b497139bf46d1a2ac40fcff94f1b9","RequestLe velBeaconUrls":[]}">.</script>..<li class="single serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"gemini","e":true}" data-provider="gemini" data-ad-region="infopane" data-ad-index="3" data-viewability="{"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cfdbd9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	740

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cfdbd9[1].png	
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/c6/cfdbd9.png
Preview:	.PNG.....IHDR.....U....sBIT....|.d.....pHYs.....~.....tEXtSoftware.Adobe Fireworks CS6.....tEXtCreation Time.07/21/16.~y....<IDATH..;k.Q....;.;..&..#...4..2... ..V,...X..~.{..|.Cj.....B$.%.nb....c1...w.YV....=g.....!..&.$.mI...I.$M.F3.}W,e.%..x.,..c..0.*V....W.=0.uv.X...C....3`....s.....c.....2]E0.....M...^i...[..]5.&...g.z5]H....gf....I... .u.....:uy.8"....5...0.....z.....o.t...G..".....3.H....Y....3..G....v..T....a.&K.....,T.\.[..E.....?.....D.....M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P.....9.....yI.<...9... ..R.e.!`..-@.....+.a..*x..0.....Y.m.1..N.I...V.'..;.V..a.3.U....,.1c.-.J<..q.m-1...d.A..d.`.4.k..i.....SL.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20537
Entropy (8bit):	5.298606813221356
Encrypted:	false
SSDEEP:	384:kOAG36OllD7XFe0uvg2f5vzBgF3OZOjQWwY4RXrqt:f93D5GY2RmF3OsjQWwY4RXrqt
MD5:	2E8E023F862C5E446EA77929603D4CCC
SHA1:	E493799CE0E9F9CAAAA10757B67F56D714F6B640
SHA-256:	D15675A57DF77672F1F889C6C15C33F8C43AA01B0CB9AE46ED527EB5DA32512F
SHA-512:	F8BA12BC15C4643B9815EFD422E2371689723BC471F4F9E9C6E5DC45E66F83356FF00AE4F122757BAD027F57E2B26CDAA32B24F608204465A089D7AE4A103472
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":72,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime" :"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":" 0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","y ld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20537
Entropy (8bit):	5.298606813221356
Encrypted:	false
SSDEEP:	384:kOAG36OllD7XFe0uvg2f5vzBgF3OZOjQWwY4RXrqt:f93D5GY2RmF3OsjQWwY4RXrqt
MD5:	2E8E023F862C5E446EA77929603D4CCC
SHA1:	E493799CE0E9F9CAAAA10757B67F56D714F6B640
SHA-256:	D15675A57DF77672F1F889C6C15C33F8C43AA01B0CB9AE46ED527EB5DA32512F
SHA-512:	F8BA12BC15C4643B9815EFD422E2371689723BC471F4F9E9C6E5DC45E66F83356FF00AE4F122757BAD027F57E2B26CDAA32B24F608204465A089D7AE4A103472
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":72,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime" :"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":" 0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","y ld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20537
Entropy (8bit):	5.298606813221356
Encrypted:	false
SSDEEP:	384:kOAG36OllD7XFe0uvg2f5vzBgF3OZOjQWwY4RXrqt:f93D5GY2RmF3OsjQWwY4RXrqt
MD5:	2E8E023F862C5E446EA77929603D4CCC
SHA1:	E493799CE0E9F9CAAAA10757B67F56D714F6B640
SHA-256:	D15675A57DF77672F1F889C6C15C33F8C43AA01B0CB9AE46ED527EB5DA32512F
SHA-512:	F8BA12BC15C4643B9815EFD422E2371689723BC471F4F9E9C6E5DC45E66F83356FF00AE4F122757BAD027F57E2B26CDAA32B24F608204465A089D7AE4A103472

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[3].htm	
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":72,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20537
Entropy (8bit):	5.298606813221356
Encrypted:	false
SSDEEP:	384:kOAG36OllD7XFe0uvg2f5vzBgF3OZOjQWwY4RXrqt:f93D5GY2RmF3OsjQWwY4RXrqt
MD5:	2E8E023F862C5E446EA77929603D4CCC
SHA1:	E493799CE0E9F9CAAAA10757B67F56D714F6B640
SHA-256:	D15675A57DF77672F1F889C6C15C33F8C43AA01B0CB9AE46ED527EB5DA32512F
SHA-512:	F8BA12BC15C4643B9815EFD422E2371689723BC471F4F9E9C6E5DC45E66F83356FF00AE4F122757BAD027F57E2B26CDAA32B24F608204465A089D7AE4A103472
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":72,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\755f86[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	390
Entropy (8bit):	7.173321974089694
Encrypted:	false
SSDEEP:	6:6v/lhPZ/SlkR7+RGjVjKM4H56b6z69eG3AXGxQm+cISwADBOwIaqOTp:6v/71lkR7ZjKHHIr8GxQJcISwy0W9
MD5:	D43625E0C97B3D1E78B90C664EF38AC7
SHA1:	27807FBFB316CF79C4293DF6BC3B3DE7F3CFC896
SHA-256:	EF651D3C65005CEE34513EBD2CD420B16D45F2611E9818738FDEBF33D1DA7246
SHA-512:	F2D153F11DC523E5F031B9AA16AA0AB1CCA8BB7267E8BF4FFECFBA333E1F42A044654762404AA135BD50BC7C01826AFA9B7B6F28C24FD797C4F609823FA457E1
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/11/755f86.png
Preview:	.PNG.....IHDR.....w=....MIDATH.c...?.6`hhx.....??.....g.&hbb..... .R.R.K...x<..w..#!.....O ....C..F___x2.....?...y..srr2...1011102.F.(.....Wp1qqq...6mbD..H....=.bt.....,.>}b.....r9.....0.../_.DQ....Fj..m....e.2{..+..t~*...z.Els..NK.Z.....e....OJ.... |..UF.>8[....=...;/.....0.....v...n.bd....9.<.Z.t0.....T..A...&....[.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AA6wTdK[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	543
Entropy (8bit):	7.422513046358932
Encrypted:	false
SSDEEP:	12:6v/78/kFBVoROFJeVmDZFr3iR4f85jaSirm4VFF9LW+etOdx1Y0:+Vom4cfU4mGmab9L7dg0
MD5:	91EE9ECB5C9196CBD18EE4E9C41F94B5
SHA1:	F829201477F63B908789BB895823E5A4D16ABBD7
SHA-256:	2BA5AC02E5C6AE8D5BBD3D8C0CD5603A02A67E192394813514D151AE1D6988B6
SHA-512:	A30B7F28E690DE2B8AB0E413861E4B6ED0BD7CEB0695A93526620E44F20011905FD72A6F489C62EE1753235F063188156D50BBE44F5588250EA9395942505134
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AA6wTdK.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O.S=,CQ.....E..... ..F..`0.....?.``..&D"."......Q.!.OK...S.D.../.....|.....Y.T!.aA.R..P.HJ ....O..sM....rE%.|><o...C.{L0.....i(.m..>....`\.qt.....>..J.G. *.W..l..~=.cN.{.K[.@..W...zeM...@y`..T....O7.....u...F0U. v{..2.....!..T.B.=.<v@....W..ax.+P.81...<....]{....f...E..5... ...6v.;8...2.h..%7...)...|;2....t..,....!.fY.:>.....:.R..(B.s...M&.F.R..Z$.....B.e.w.....N.....AM....O.d.?....>.g...Z&.@....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AA7XCQ3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AA7XCQ3[1].png	
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	635
Entropy (8bit):	7.5281021853172385
Encrypted:	false
SSDEEP:	12:6v/78/kFN1fjRk9S+T8yippKCX5odDjyKGIJ3VzvTw6tWT8eXVDUlrE:uPkQpBJo1jyKGIlVzvTw6tylKE
MD5:	82E16951C5D3565E8CA2288F10B00309
SHA1:	0B3FBF20644A622A8FA93ADDFD1A099374F385B9
SHA-256:	6FACB5CD23CDB4FA13FDA23FE2F2A057FF7501E50B4CBE4342F5D0302366D314
SHA-512:	5C6424DC541A201A3360C0B0006992FBC9EEC2A88192748BE3DB93B2D0F2CF83145DBF656CC79524929A6D473E9A087F340C5A94CDC8E4F00D08BDEC2546BD4
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AA7XCQ3.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O..Kh.Q...3.d.I.$m..&1...[....g.AQwb."t.JE.].V.7.n\Y....n...Z.6-bK7..J. ..6M....3....{.....s...3.P..E....W_.....vz...J..<.....L.<+..}.....s..}>..K4....k....Y."/.HW*PW...lv.I....\..{.y....W.e.....q".K.c.....y..K.'.H....h.....[EC..!.}+.....U...Q..8.....(./....s..yrG.m..N.=.....1>;N...~4.v..h:...'....^..EN...X..{..C2...q...o.#R .....+.}9:~k(.."........h...CPU..`..H$.Q.K.)"..iwI.O[..\.q.O.<Dn%..Z.j)O.7. a.!>.L.....$..$..Z\..u71.....a...D$..`<X.=b.Y'...../m.r.....?...9C.I.L.gd.l..?.....-.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAkqhIf[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	860
Entropy (8bit):	7.60890282381101
Encrypted:	false
SSDEEP:	24:K0TOJV9BOYAz7M84tQle4scs41PjgcpT2MIcTuNN:KYGVrnS7MXtV91PTgxcTuNN
MD5:	BB846CCC67B5DE204B33CF7B805F59A3
SHA1:	A3301490722FA557F169FAA8283DA926F4393783
SHA-256:	9913B44FB1AAF52B9CB0BD7BB4563CAA098BC29D35E2609D4E2A74C4D4026131
SHA-512:	6686582817EB71206178595C9051087412499F7110B1FFE13D8C2E517EC16C7B6B6A1728B546F2EBEE80D0D1388E64FFBE97A628DD7C4B24DD30274AAB7E3D41
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAkqhIf.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....o.d....IDAT8OeS]L.a.>|c../..E.sx...3.....6.K.y..x.3....J...`....,..K...G1u....a...QZ...^>.....y.{.y.....v...o$..)..X..)++...h.....W.N.E..w:1a...<:.!I..P..=3c{.....K.+.d@+`.cc/<....GF.....$.0..r..n....h4...O..P.000."|.....>$yRPTW...8:..li..}}}..BO..]..+*... .....h.&.....n$.q'...lk.\.....J~N N.M.....28....&.....}VV.TUU.<.....uJ....!..`eu.d2....G.....Oy....O...$?..u.<...B!.D"(**.. .....h4....H.R899.c.....$LMM...2<...w-j5.F....H..|>."...v.hP.ggg.L.[[[.nn...B.b.<M..vv" ... 3...@ .W.b.....J.X\\.....D..R:D.....~..d../.v.....8.l6lhh...!...j5.7...6"Y.....qr.....6.j.bGG.NNN....."Y,.....b..Nh2.....:..i..f..i.....h0...LV.....r~mm-.\n. SW..h..`.....?....,F#J..m. ...b...~nn.....V.D".q.....?....?.C....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB14EN7h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	10663
Entropy (8bit):	7.715872615198635
Encrypted:	false
SSDEEP:	192:BpV23EiAqPWo2rhmHI2NF5IZr9Q8yES4+e5B0k9F8OdqmQzMs:7PiAqnHICF5IVVyxk5BB9tdq3Z
MD5:	A1ED4EB0C8FE2739CE3CB55E84DBD10F
SHA1:	7A185F8FF5FF1EC11744B44C8D7F8152F03540D5
SHA-256:	17917B48CF2575A9EA5F845D8221BFBC2BA2C039B2F3916A3842ECF101758CCB
SHA-512:	232AE7AB9D6684CDF47E73FB15B0B87A32628BAEEA97709EA88A24B6594382D1DF957E739E7619EC8E8308D5912C4B896B329940D6947E74DCE7FC75D71C684
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB14EN7h.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...E.(.Y....E.D....=h...<t.S.....5i..9.. .:..".R..i...dt&..J..!...P..m&..5`VE..\|..j.d...i..qL=x...4.S@..u.4.J.u.....J u%.FEU..I.*.]#4.3@.6...yH...=..}.#....bx...1s...O.....7R....."U.....jY.'.L.0..ST.M.:t3...9...2.:.0$...V..A..w..o..T.Y#...=).K..+.....XV...n;.....}.37.....:.!E.P.E%...RQ@ .E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%-...uE,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bowT1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	19148
Entropy (8bit):	7.961138757908785
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bowT1[1].jpg	
SSDEEP:	384:ed+SNxq0bBuCrRl8dvc3roqj+yy4E2FWQ7XOuBZsLUoPtmMR92QP51ZvKIlbBNuP:e8CRhRmdE384+4X7ei85PtBR92QPrplY
MD5:	727FA47EF7643A21BD8F6B4AC58CA518
SHA1:	33D91C5E8F6638A7771C879E5055A65839B5E3C4
SHA-256:	95592E9F54690BD26AAB4BE2FAFBF17CDAC8FA7A79060ED3D03D813225B86282
SHA-512:	B4E997F50B1A2FF19F26D9C8747F6461AD8DD19BA83755368B7A2DA2AD5A12AC7F5B27433DFAD85E74ABCD81ABCF68BC54A52C4900EA42E9C7508E31D2992F7B
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bowT1.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1578&y=832
Preview:	......JFIF.....,.,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...1..&?..}.c....Nh..:.....#x.6+"2..Sj.\J.;...17.y...5..;.t.}m..Nf.6...eJ.ia.=0.?.....EO5....t..*....QE.-.QL....Q.V.B.....7..r..U..oc$....i|.t.~.....R.M5..84..i1[F...PXvsE.R.V.....8<..1..G.4...".Q...n4.....Q.Mlu..#.MsK.v...Fh.....R.G8....X.].0rc.@8..SZO,SoH.....6.y#q.=qZ.....=+.X..M....0.:...M.3.....".#;rj....,=.sJ8.-....m...&....:.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1boxCG[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	14380
Entropy (8bit):	7.953901456845605
Encrypted:	false
SSDEEP:	384:O/8XvtTCsQ7kFsFpNF0kRBi4dRJbmf7ovh6qN6S2HuV:O/6RbvFoVKwJK1+
MD5:	6F7170576724A627D483D1B5C93ABA64
SHA1:	3D1EF1D71213BCCEF109CFEFA165AC17CDDF8E6C
SHA-256:	8357E341985FCD80BA758F8D3954B1A07FE72E2A094AD3CAB93920DF776B1028
SHA-512:	87344941C814E2194CD59830DBCEF3D6630C01F13B2CDEA8F0BF3D716C9BC7C7E4995CB8C25B9E0B2233FC3825240A1B1CD05038A957942C9B409AEBA5DDF39
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1boxCG.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=728&y=485
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....C..|w..|E.....+.....S(e9...n....muh%.YW.z.W1...^}g...H.jA=...f.z.EZ...jz22.CO.q...C.3 u#.qZV^#.^.....Z)E..s..K....m.[O.%V?Z...t5Vc."....6..8...w..>|..B...]...m.'..)6.8.....I..e...L.76.D.:}Ez..R4Q....QY.).Z...x.@.W..xwL..0...N+....6.....X.RF..g&..U...&.jO.I.....J.. .M5..i.kxj...$ec..w.....5.x>.l3\.....$P~i>Q]T..\.~..p.Jg..V..Z...c.z..#:R.....R.J).d...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bpVF3[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	downloaded
Size (bytes):	2048
Entropy (8bit):	7.766807921281022
Encrypted:	false
SSDEEP:	48:xGpuERA30k+pd6kOQrWUleiK9/V6qkfH7t:xGAErzO+WUle5dVm/7t
MD5:	A16D0337FCC938204378279AA74C96C6
SHA1:	578FB21E607785339B1C73CD3F63383630089EBD
SHA-256:	2B2DBAE3D809A3196584EB4325B51DF70E91BC0CBDFFCF68741D61DE10A7A927
SHA-512:	FFF77FDCF35520F9C355768164064B6C85654CDCA43751ECEEBAC3B16C31743CF7FD4ED4A5A72E96E79C49A69A7102068F8AAD0BCF00E6DC58A72CD09063747
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bpVF3.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg&x=535&y=335
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...3m..A....6O...$_)?...k.^....p...+.U..m.....q.y.j.._.+N...:....G0.H.?Q.....Z...F.....6..N...c`@.....U..$.....J..$.`...]s.l..J.....`8..mE]...[.7...4.....j..x....B.....Ue.h<.x..z....q\S..Up.:....%.=.(aQ.;.o.!.n..P.....m..S$...w..>.Su....FG.c.....ei.W...K..#.@Y...:....Y..*.nBy.....n\..2.05.v=Z.E.h..C....m?.#m.*..:..-.....(.....UC.I.+H.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bq2Er[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	11308
Entropy (8bit):	7.9318673423759565
Encrypted:	false
SSDEEP:	192:BYFd9O0DvQ++DgCS0tyIYRnH0CW/aLJlBcyrBxbm46x9JBcKFrWNXcPTxA5kK6R:e8d6lqy91H0+LJLcyYx4Kt4Mt+kn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bq2Er[1].jpg	
MD5:	936D742ADFFB598E15E8F428EFDD557D
SHA1:	8AE38DCA6B1D1D218EECF0CC0B1177E095EB5066
SHA-256:	258746DBDC37CB7B5BB2D2E5222EFBFAAF62B24904CEA082A91D0C6AB606F21B
SHA-512:	F4D463B1715C6985E19A0AD9DDB3679FCE82F8E9E3D8B9F6E014B4C964550A931F7F25CFC15E1384C448837CAF0102A33A06B02AEA9E8FD69E93B43E1AA16FC C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bq2Er.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..".....p...lA..u8J]...GN...E.A.@....Du8ZF.....|..S.....!X.X.5.b.z...q....."...^..r.:.....rkxA..MbE`.n.r .....y8....u.}.....(8 ..T.g..lt.R..GzSvX.....&.H.-.:.}..4..{VY...j...E..PL..n.Vm[sK"..Ej%.K..*.;...+n\%..).a'.+I....c(.Z..Md...EU....e..+LdAh.R.....t...\.[.C...j.3"N..... ..06...(..+b..... i&.....k..k.6.e.a.*sy....8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bqBbD[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	6049
Entropy (8bit):	7.914217534792069
Encrypted:	false
SSDEEP:	96:BGAaEzLGwPHpfj750TofkleR+Z2aVuF27s5SHPYCxMoKDbR2ZM82xikOti4QphTm:BCEjPJXiTkR+s8uF27CSHPYCxM3EZM8F
MD5:	A9F1FE8EFCA8C4D486E9F0C6716E0D60
SHA1:	713355C49B02CA22F33E598F7FB97C56231C3D9E
SHA-256:	AF19A6045DFB0DD1DFA76FB28EF31AD0B877F9C10887FB0EC1EAA20938474289
SHA-512:	9872B15797A27C22099381E319016F6D1C18CD812E8BA657F433CD8162695C62DDBF3404214398E821FFAF845175FE27531BB1942E9F8E1D9E41E34FDF77E1AF
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqBbD.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=386&y=230
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..n...<.....I.u.u..FL.F.:k..QZ.8.V. ..W..4C.8R....,...R...G5 ..H.*.B*D4.....n..Au..H...M.3.du.@.~.....C...@.....}..E g\.....j.Q.C8.sM.e.a..X...\.^@.H.rW.yY..~..%.#..9...F. S..p..i.....8,l9...4.....QN.....a..N.}1]....0....9.....n3.`.;...h.V...5.T{..q...A..x.A...,..q.&X.....Y..p:..... .1.p5..D[.....?.>..F... .]...m....S-.m.0>.6e&_.=.wq.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bqfgC[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	9352
Entropy (8bit):	7.939937183677365
Encrypted:	false
SSDEEP:	192:xCnQkjuIR4q19ef4+cyjayPBXFN0wtugG4YbOZoXmHaS2tM8i2SkO2u:Un2Vqv+cyWyZXb0MuhOqeaS2md
MD5:	5B9AFB699D49D2C2D9F95ABCA950FFD3
SHA1:	9F8EB3A6661D51053318959C784BFA6E0BC07D4E
SHA-256:	1A483EE24DBF65B1C76A1AA06A74775AB53899855B2131F31E9748778A1B6D55
SHA-512:	A9B015DB567423B25E0C9A67785B374E708EA73D4F14AA4BC11FAB29AD9FA40784AA9736D8A75E12C581D205DBF5B461EBD1BAAB9825B08C93CD43F7E0181E 74
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqfgC.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=566&y=214
Preview:	.....JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..*(..AKE..QE.....r...V.BqL...qU%....>j.YC..;..W.%..c>..$..V...V.:}.. ..J.[H..<X..z.s.+.[...l.q.....h.7...V8..r ...H...'...c..E...`"DS..*..F....Q...N*..z.E....]G.2?>.U...e.i.+...E. 2@.fx..FS.....Tl.bD.....h..d.q.R...R(...~)..eiz.u,.j*C.(...-%-..(...(.....`+^. .k2.r.....f4....u..[X...dzz.J..&.....z..U... .9Q..ObR./}.Ye*...x...AZ..r.@...q.y.4.x....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bqlzp[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	8972
Entropy (8bit):	7.902533757207737
Encrypted:	false
SSDEEP:	192:xYE+HFK5QdeFT8RmdCICXRgBH/hWwtMrrTG2LEHvMU7yFdWm+u:OE0DooR+xYgBHEoM/Thiv57yCa
MD5:	2BA06694E9FD62572C80DE1E7A1FAD0A
SHA1:	7048933DA1DAC457E21CFD086FDBEEBAADAF01DA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bqlzp[1].jpg	
SHA-256:	C6901820E7F9942B2BD92C6E1AD4557A90A9B075040BE55AC4678D6A0ECD335E
SHA-512:	DA14FB3708A2A80E099C1FE62242C5D4A4C9A39184B4355D8DCEEFE6ACBD4322553F092115BD447E179079F163A2CB4238E5F9DC744953219998C670E53B752
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqlzp.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..QS..PT.).....[.P".Uv..N!W..(.j1..W....L.(..T.@...M..@...H)h.h..@-%-%..QE..JZ(.))h.....KI.. LRS...%%-%.%%-...R.u..m%:....(..*AS.D..AT...\.UX.\.P...J..S.t..v.E..XJ..YJ..jU.....).)...:.QH.....RR.@.E-%..(...RR.@.i)i(.)1N....KI@.IN...b...J.JJZ)..E-..i...@yR....R.AT....UR!... .]...T..v.@.Q.....).).@.....-.P0..(...(...(.RR.@.....RP.RR.J@%%:...4R.R..S.!...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bqn7Z[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	9504
Entropy (8bit):	7.948783800848245
Encrypted:	false
SSDEEP:	192:BClgjVI8V+cScfPTTauAzWBQ5cICXkfj63Ehd2ikky0Dqcf:klufFSCPXaDq7IfGghgS5f
MD5:	D5D0FB601211DAC92905D544302A464F
SHA1:	38C70EBFCD8A1CFF0EB88D3C7F3BB6C71736D0DB
SHA-256:	43FB29B509C16591325DCE773073C97A2D2C37DB862A80D027A60C5F7D1A3BF7
SHA-512:	D55A723EB30344C8F02C5F88CC75101F0050D095628189884DFE5E2FD60C556CCD57E8D4169E729DF537FD33A6D2EE9A2F2A99DDC9D30C78241004AFC8F0B0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqn7Z.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=329&y=65
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?.....+1b@Q..?.....1.....8f..o.#r..s....a6..)...+....!vVm;T...38.9C^...kv.^...+..*A9...b.-oc.r.WgS.G.]....O....I.q.. #..uQ..c.M%t....b....'i.....q..Apa.Vi..FJ..Y..D.=+...t.2k..6.....A^9.j.....c..^.I#..../....[....b.g.>..==kJ..+C8....n@...^mm.{.].x..p..@.7q.....S.....r..e.i....f>..J..F.JH...C.(.....QE..QE ..QE..QE..W...].?...F...w.<_N?...F..=b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bqoeM[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	13180
Entropy (8bit):	7.901265706404518
Encrypted:	false
SSDEEP:	384:e6xgTYLqt0j1tplfsyamYD1m6xjNJa/qr:emaY00j1tplfsyWHair
MD5:	59C7793A67BAC4742AE51C33AA1491EA
SHA1:	AAD3B0336958A90FA46A30389C346B5FE014EDC2
SHA-256:	32E00D733ACD8EDCC72630A09E0A8ED928F296723D4450B5438CBB936458045D
SHA-512:	C476A79C45A21CDFE7337EC68C22448E506F4FFE62FA98C8FFB61380848BDFC0CAD03379508CFCEB637A870018FD7A93A0CA6C79280E536DC30BC0A9CB0F24 C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqoeM.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..Y.zP...!...<..+2.m>..H.O....A.....A.Q...(...J].....Q..;.@3.J1.i..h>....A.P.9.4.>.....{z..NG@.*9.4.;z. <.....}.7.....Q.A@.`..0}.I..AG.....;.oj_.7..&.....7..G....*.zS.1.j.4...W?.@..l{...s.M?....<.?.i..._.w.'.i.I.F4.6_..5..D...d.....x..$..!..=).L...c..x.....=...Oj`f.?.&..h.0.s.~t.C....$w..=.. ?.....@.....`*..(..`5.....L.....&h../.....4.../

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bqpyN[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	6916
Entropy (8bit):	7.920973995347589
Encrypted:	false
SSDEEP:	192:BF66V12p5Ht4SfoPe5PwvtrncT6SsrCaj:v6s8CTPe5ohcT6Ss+aj
MD5:	74155A4A83A3FF51D9048AE028342CFF
SHA1:	3BDBCC0E54687D70548264D34F683F6E830AFC00
SHA-256:	CDB410E24227AC7B2EC50D9D0B0DCD7EE61F83393A3D4D6B821AD5CB36253BE7
SHA-512:	AF95EBD0AA6813CEEDE48A9DB35599E567F436B4E4795BD93387FF987A3DAF38C8B4ECA636A7DC93A1F978B50525429E00C33DE7E4093E5A90DDE5558887C4 A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bqpyN[1].jpg	
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqpyN.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg&x=612&y=290
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....T..*X.S.|...c=i....U...l.b.....T.8..r.J.....U=..q.Q;....g..y#.R.g=..`\q.....S...c.g...1.T.H..+Z+8.].H#..4.r.c.;{.y.C.9....|...I.WT.P..3|.....SR...VO....N)...j..dS..`..Z.!.A.L..8...1Z.6.\Q.`%-...!.KF)q@.E.(..%.....R..JZ\Rb..Z)(.sFi)3@.i3Fi(.f.4Q@.i3E%...f....4QE.b.....<=...f...k...+z..p?.?.....1.}+b.~.O.g...|.h.._.Z..u...G..[....|.:...l....]~o.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bqu5r[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	12586
Entropy (8bit):	7.932688059393912
Encrypted:	false
SSDEEP:	192:BYajqmhgVQHJZwYpupIUQA0hAqmnIV/C/OPtz3Qs7MsM/XtOW0aOYafFrphC:eajvCVQHJzpiw/K7W3Q+StMvVk
MD5:	0CA0C3420648505D8ED7808BCAE33914
SHA1:	DCAFEEFEDD1746566DEB57DD77BAE5C36C7CFB21
SHA-256:	26029D5D109845BF1DECB2B51CA86AA58D05E058DEDF6A4D63B8336272DAB1E0
SHA-512:	2D361D905FB5ABA2AEC32016D800460AA5A70865A90B332A2B09E4131EE365ED17A80FD4420B7297441635EA3FE359995D04F5F4D1773CCA15017C239B3DEA7D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqu5r.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....<qP..a..*.@.O..m:?.(..SV.V.)i.- .....xVwj.....~..@`...Z....j...p./A.....KJ.5...Fv.5H.8(?3Z.u.F....XG.....i=.t.Z.t.T..*IS.....u..NH...k.mN.$..B.....{g..[.....)...x.8.T$.^....0_1.'..?J....1k9...6..8.e.k...Vx...a....}qT..w...S.....Mj4t..OQ.H.5F....#..B.i....[.a....?{....mU....II1.c..:.....$."W8'.M.Tlj\L_.\.6..n?v...>....P.D..0.x.....D..U..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1bqyAI[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	10313
Entropy (8bit):	7.9203959266112625
Encrypted:	false
SSDEEP:	192:BYI+Qt00r54TE8EVgKXTSXDFgodBS+dv+mFWfARVkYt/aAoXTpHJa6dHW/Qn6B:eshyTvAg4ShPbdmmFW8KO/aAwDaAWIE
MD5:	E30B23413044E6E1C61B6578402C7FB4
SHA1:	F55B4C5C80442F4C45D780AA597917103F402942
SHA-256:	C6C8D74C2C3F2B8F7EEC85DD02B8349748F52D6D13330F05CC203CFBBDD37A80
SHA-512:	6C514BCEB4953C41A50B200FC83291C08997D1EC4A82DF00979050C55F4DB8C9843E18E1A020C0011570A0B115F5F621549F490D9BB7AA4CFCCD355E91C5726
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bqyAI.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...{S{S.W!.<U7sPE.w..^.....M.`x..e@.c.k.(.t.j.1.y..g...zV.+.5.9...h.@~nq.5`8*7.@.S....Q"34|....T0."...|..F+....%h.&.g5Y.t.....{z..Bwr{.....c.||.sH.rS.jf.A9.A$.E..=j)Z7..>....z.c..G#.+..N1....L. .Qd.+T..+...}.oxb...O..5..QWt.?.!.H..Jb=1..P.$.8a.j.}.U...Y..E#....A..S.M..(?*..'=..[..*2N.m'.....m....k...R:n.5j.....1..j..-E....n3.....Kg...N...v0d..g.w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB7hg4[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	458
Entropy (8bit):	7.172312008412332
Encrypted:	false
SSDEEP:	12:6v/78/kFj13TC93wFdwrWZdLCUYzn9dct8CZsWE0oR0Y8/9ki:u138apdLXqxCS7D2Y+
MD5:	A4F438CAD14E0E2CA9EEC23174BBD16A
SHA1:	41FC65053363E0EEE16DD286C60BEDE6698D96B3
SHA-256:	9D9BCADE7A7F486C0C652C0632F9846FCFD3CC64FEF87E5C4412C677C854E389
SHA-512:	FD41BCD1A462A64E40EEE58D2ED85650CE9119B2BB174C3F8E9DA67D4A349B504E32C449C4E44E2B50E4BEB8B650E6956184A9E9CD09B0FA5EA2778292B01EA5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7hg4.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB7hg4[1].png	
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J...._IDAT8O.RMJ.@...&.....B%PJ.-..... ...7..P..P....JhA..*$Mf..j.*n.*~.y...}...:...b...b.H<.)...f.U...f s`.rL....}.v.B..d.15..\T.*.Z_..'.}..rc....(...9V.&.....|.qd...8.j..... J...^..q.6..KV7Bg.2@).S.I#R.eE.. ..:_....l.....FR.....r...y...eIC.....D.c.....0.0..Y..h....t....k.b..y^..1a.D..|...#.ldra.n .0.....:@.C.Z..P....@...*.....z.....p....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BBIbTiS[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	820
Entropy (8bit):	7.627366937598049
Encrypted:	false
SSDEEP:	24:U/6gJ+qQtUHyxNAM43wuJFnFMDF3AJ12DG7:U/6gMqQtUSxNT43BFnsRACC
MD5:	9B7529DFB9B4E591338CBD595AD12FF7
SHA1:	0A127FA2778A1717D86358F59D9903836FCC602E
SHA-256:	F1A3EA0DF6939526DA1A6972FBFF8844C9AD8006DE61DD98A1D8A2FB52E1A25D
SHA-512:	4154EC25031ED6BD2A8473F3C3A3A92553853AD4DEFBD89DC4DD72546D8ACAF8369F0B63A91E66DC1665CE47EE58D9FDD2C4EEFCC61BF13C87402972811AB 27
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBIbTiS.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O.S.K.Q....m.[.L\.,%I*..S.....^.^.z..^..{..-.Bz.....MA+.....{W....p.9..;.s....^..z..!...+..#....3.P.. p.z5.~..x>.D.].h.~m..Z..c.5..n..w...S."..U.....X.o...;}.f..:.}]`..<S...7.P{k..T.*....K.._.E..%x.?eRp..{.....9.....,,..L..... .....})..._ TM)..Z.mdQ.....sY .q..,.T1.y.,lJ.y...'?...H..Y...SB. .2..b.v.ELp....~.u.S...."8..x1{O....U..Q...._.aO.KV.D\..H..G..#..G.@.u.....3...'...sXc.2s.D.B...^z....I....y...E..v.l.M0.&k`.g....C.`..*..Q..L.6.O&`.t@..|..7.$Zq...J.. X..ib?,.;&.....?..q. Q.,Bq.&.....:#O....o..5.A.K..<..'.+.z...V...&. .....r...4t.....g.....B.+-..L3....;ng>..}(.....y.....PP.-.q.....TB.....|HR..w..-....F.....p...3.,..x..q..O..D.....)..Vd.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BBPfCZL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 50 x 50
Category:	downloaded
Size (bytes):	2313
Entropy (8bit):	7.594679301225926
Encrypted:	false
SSDEEP:	48:5Zvh21Zt5SkY33fS+PuSsgSrrVi7X3ZgMjkCqBn9VKg3dPnRd:vkrrS333q+PagKk7X3ZgaI9kMpRd
MD5:	59DAB7927838DE6A39856EED1495701B
SHA1:	A80734C857BFF8FF159C1879A041C6EA2329A1FA
SHA-256:	544BA9B5585B12B62B01C095633EFC953A7732A29CB1E941FDE5AD62AD462D57
SHA-512:	7D3FB1A5CC782E3C5047A6C5F14BF26DD39B8974962550193464B84A9B83B4C42FB38B19BD0CEF8247B78E3674F0C26F499DAFCF9AF780710221259D2625DB86
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBPfCZL.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	GIF89a2.2.....7..;..?..C..I..H..<..9.....8..F..7..E..@..C..@..6..9..8..J..*z.G..>..?..A..6..>..8..:..A..=..B..4..B..D..=..K..=..@..<..:..3~.B..D.....,|.4..2..6..:...J..;..G....Fl..1}.4..R.... .Y..E..>..9..5..X..A..2..P..J../|.9.....T.+Z.....+..<.Fq.Gn..V..;..7.Lr..W..C..<.Fp.]......A.....0{.L..E..H..@.....3..3..O..M..K....#[.3i..D..>.....I....<n..;..Z..1..G..8..E....Hu..1..>.. T..a.Fs..C..8..0}....;..6..t.Ft..5.Bi..:..x...E.....'z^~.....[....8`..........;..@..B.....7.....<.....F.....6..........>..?.n.....g.....s...)a.Cm....'a.0Z..7....3f..<.:e.....@.q.....Ds..B....!P .n...J.....Li..=.....F.....B.....:r....w..|.....`..[}.g...J.Ms..K.Ft....'..>.....Ry.Nv.n..]..Bl.....S..;....Dj.....=.....O.y.....6..J.....)V..g..5.....!..NETSCAPE2.0.....!...d...,....2.2..... ..3.`..9.(|.d.C .wH.(."D...(D.....d.Y.....<.(PP.F...dL.@.&.28..$1S....*TP.....>...L..!T.X!.(..@a..IsgM..|..Jc(Q.+.....2.:.)y2.J.....W,..eW2.!....!....C.....d...zeh....P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\a5ea21[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/2b/a5ea21.ico
Preview:	.PNG.....IHDR... ... .pHYs.....vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....< ...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d...LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@ lA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq |....gz_Z...x..0F'.....x..=Y}..jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\de-ch[1].json	
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	74702
Entropy (8bit):	5.345294167813595
Encrypted:	false
SSDEEP:	768:hVAyLXfhINb6yvz6Ix1wTpCUVkhB1Ct4AityQ1NEDEEvCDcRiZfWUcU5Jfoc:hVhEvxaEC+biAEv3RiEkz
MD5:	754F6C92A735B47A2CC5E7D03C2102D1
SHA1:	71DDB35ED5E57812B895A939C77A0196B538AF40
SHA-256:	491BF15460B5FEF7B972E48841BACADA7549A01CA52E46297E9F91B2E978132D
SHA-512:	D3A859DBB25BA28D0401428A6C68B87F0BE3825DAA773B161A86D33164846FF67ADD99FD4A1CF3CA4613293DD2F629C5CE2E9A3E6E8A7C796A361F02CEFA3C8
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/6f0cca92-2dda-4588-a757-0e009f333603/de-ch.json
Preview:	{"DomainData":{"cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir teilen diese Informationen mit unseren Partnern auf der Grundlage einer Einwilligung und berechtigter Interessen. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAllText":"Einstellungen speichern","CookiesUsedText":"Verwendete Cookies","AboutLink":"https://go.microsoft.com/fwlink/?LinkId=521839","H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\e151e5[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/9b/e151e5.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\fcmain[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	36931
Entropy (8bit):	5.1350687316590005
Encrypted:	false
SSDEEP:	768:21avo7Ub8Dn/eBW94hMIXQYXf9wOBEZn3SQN3GFl295oAclyK/Ulusq:yQ+UbO4WmhMIXQYXf9wOBEZn3SQN3GF7
MD5:	BD20C297F779D3B921C11D4A5A879203
SHA1:	CE1D4FCD8861FA16C95B4DF41583C25B87AA90EF
SHA-256:	D48AB7075D0AAD956430087A9B9775BC25AFB627C93AB3C1CC9A7624BA4DB912
SHA-512:	3352756445ECF9F689F0A360521622FB53199E650560CC3AF6DB62E74AE3A5F6AA85D2419B9D3099D1B9CEEC8D8DB663D1675EE8ECF9AB9AD91779591E3409C
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/803288796/fcmain.js?&gdpr=0&cid=8CU157172&cpcd=pC3JHgSCqY8UHihgrvGr0A%3D%3D&crid=858412214&size=306x271&cc=CH&https=1&vif=2&requrl=https%3A%2F%2Fwww.msn.com%2Fde-ch%2F%3Focid%3Diehp&nse=5&vi=1606513416135356601&ugd=4&rtbs=1&nb=1&cb=window._mNDetails.initAd
Preview:	;window._mNDetails.initAd({"vi":"1606513416135356601","s":{"_mNL2":{"size":"306x271","viComp":"1606511891669204310","hideAdUnitABP":true,"abpl":"3","custHt":"","setL3100":"1"},"lhp":{"l2wsip":"2887305228","l2ac":""},"_mNe":{"pid":"8PO8WH2OT","requrl":"https://www.msn.com/de-ch/?ocid=iehp#mnetcrid=858412214#"},"_md":[],"ac":{"content":"<!DOCTYPE HTML PUBLIC \"-\/\/W3C\/\/DTD HTML 4.01 Transitional\/\/EN\" \"http:\/\/www.w3.org\/TR\/html4\/loose.dtd\">\r\n<html xmlns=\"http:\/\/www.w3.org\/1999\/xhtml\">\r\n<head><meta http-equiv=\"x-dns-prefetch-control\" content=\"on\"><style type=\"text\/css\">body{background-color: transparent;}<\/style><meta name=\"tids\" content=\"a='800072941' b='803767816' c='msn.com' d='entity type'\" \/><script type=\"text\/javascript\">try{window.locHash = (parent._mNDetails && parent._mNDetails.getLocHash && parent._mNDetails.getLocHash(\"858412214\",\"1606513416135356601\")) || (parent._mNDetails[\"locHash\"] && parent._mNDetails[\"locHash\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\iab2Data[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	180232

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\iab2Data[1].json	
Entropy (8bit):	5.115010741936028
Encrypted:	false
SSDEEP:	768:l3JqIWlR2TryukPPnLLuAlGpWAowa8A5NbNQ8nYHv:l3JqIcATDELLxGpEw7Aq8YP
MD5:	EC3D53697497B516D3A5764E2C2D2355
SHA1:	0CDA0F66188EBF363F945341A4F3AA2E6CFE78D3
SHA-256:	2ABD991DABD5977796DB6AE4D44BD600768062D69EE192A4AF2ACB038E13D843
SHA-512:	CC35834574EF3062CCE45792F9755F1FB4B63DDD399A5B44C40555D191411F0B8924E5C2FEFCD08BAC69E1E6D6275E121CABB4A84005288A7452922F94BE565
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/iab2Data.json
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with y our online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices ","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otFlat[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	12588
Entropy (8bit):	5.376121346695897
Encrypted:	false
SSDEEP:	192:RtmLMzybpgtNs5YdGgDaRBYw6Q3gRUJ+q5iwJlLd+JmMqEb5mfPPenUpoQuQJ/Qq:RgI14jbK3e85csXf+oH6iAHyP1MJAk
MD5:	AF6480CC2AD894E536028F3FDB3633D7
SHA1:	EA42290413E2E9E0B2647284C4BC03742C9F9048
SHA-256:	CA4F7CE0B724E12425B84184E4F5B554F10F642EE7C4BE4D58468D8DED312183
SHA-512:	A970B401FE569BF10288E1BCDAA1AF163E827258ED0D7C60E25E2D095C6A5363ECAE37505316CF22716D02C180CB13995FA808000A5BD462252F872197F4CE9
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/assets/otFlat.json
Preview:	.. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCI+PGRpdiBjbGFzcz0ib3Qtc2R rLWNvbnRhaW5lciI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyI+PGRpdiBpZD0ib25ldHJ1c3QtZ3JvdXAtY29udGFpbmVyIiBjbGFzcz0ib3Qtc2RrLWVpZ2h0IG90LXNka y1jb2x1bW5zIj48ZGl2IGNsYXNzPSJiYW5uZXJfbG9nbyI+PC9kaXY+PGRpdiBpZD0ib25ldHJ1c3QtcG9saWN5Ij48aDMgaWQ9Im9uZXRydXN0LXBvbGljeS10aXRsZSI +VGhpcyBzaXRlIHVzZXMgY29va2llczwvaDM+PCEtLSBNb2JpbGUgQ2xvc2UgQnV0dG9uIC0tPjxkaXYgaWQ9Im9uZXRydXN0LWNsb3NlLWJ0bi1jb250YWluZXItbW9ia WxlIiBjbGFzcz0ib3QtaGlkZS1sYXJnZSI+PGJ1dHRvbiBjbGFzcz0ib25ldHJ1c3QtY2xvc2UtYnRuLWhhbmRsZXIgb25ldHJ1c3QtY2xvc2UtYnRuLXVpIGJhbm5lci1 jbG9zZS1idXR0b24gb3QtbW9iaWxlIG90LWNsb3NlLWljb24iIGFyaWEtbGFiZWw9IkNsb3NlIEJhbm5lciBidGFiaWw9IjwvYnV0dG9uPjwvZGl2PjwhLS0gT W9iaWxlIENsb3NlIEJ1dHRvbiBFTkQtLT48cCBpZD0ib25ldHJ1c3QtcG9saWN5LXRleHQiPldlIHVzZSBjb29raWVzIHRvIGltcHJvdmUgeW91ciBleHBlcmllbmNlLCB 0byByZW1lbWJlciBsb2ctaW4gZGV0YWlscywgcHJvdmlkZSBzZWN1cmUgbG9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otPcCenter[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	46394
Entropy (8bit):	5.58113620851811
Encrypted:	false
SSDEEP:	384:oj+X+jzgBCL2RAAaRKXWSU8zVrX0eQna41wFpWge0bRApQZInjatWLGuD3eWrwAs:4zgEFAJXWeNeIpW4lzZInuWjlHoQthI
MD5:	145CAF593D1A355E3ECD5450B51B1527
SHA1:	18F98698FC79BA278C4853D0DF2AEE80F61E15A2
SHA-256:	0914915E9870A4ED422DB68057A450DF6923A0FA824B1BE11ACA75C99C2DA9C2
SHA-512:	D02D8D4F9C894ADAB8A0B476D223653F69273B6A8B0476980CD567B7D7C217495401326B14FCBE632DA67C0CB897C158AFCB7125179728A6B679B5F81CADEB5
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/assets/v2/otPcCenter.json
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImRpYWxvZyIgYXJpYS1sYWJlbGxlZGJ5PSJvdC1wYy10aXRsZSI+PCEtLSBDbG9zZSBCdXR0b24gLS0+PGRpd iBjbGFzcz0ib3QtcGMtaGVhZGVyIj48IS0tIExvZ28gVGFnIC0tPjxkaXYgY2g9Im90LXBjLWxvZ28iIHJvbGU9ImltZyIgYXJpYS1sYWJlbD0iQ29tcGFueSBMb2d vIj48L2Rpdj48YnV0dG9uIGlkPSJjbG9zZS1wYy1idG4taGFuZGxlciIgY2xhc3M9Im90LXBjLXRpdGxlIj5Zb3VyIFByaXZhY3k8L 2gzPjxkaXYgaWQ9Im90LXBjLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGFuZGxlciI+QWxsb3cgYWxsPC9idXR0b24+PHNlY3R pb24gY2xhc3M9Im90LXNkay1yb3cgb3QtY2F0LWdycCI+PGgzIGlkPSJvdC1jYXRlZ29yeS10aXRsZSI+TWFuYWdlIENvb2tpZSBQcmVmZXJlbmNlczwvaDM+PGRpdiBjb GFzcz0ib3QtcGxpLWhkciI+PHNwYW4gY2xhc3M9Im90LWxpLXRpdGxlIj5Db25zZW50PC9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otTCF-ie[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	102879
Entropy (8bit):	5.311489377663803

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otTCF-ie[1].js	
Encrypted:	false
SSDEEP:	768:ONkWT0m7r8N1qpPVsjvB6z4Yj3RCjnugKtLEdT8xJORONTMC5GkkJ0XcJGk58:8kunecpuj5QRCjnrKxJg0TMC5ZW8
MD5:	52F29FAC6C1D2B0BAC8FE5D0AA2F7A15
SHA1:	D66C777DA4B6D1FEE86180B2B45A3954AE7E0AED
SHA-256:	E497A9E7A9620236A9A67F77D2CDA1CC9615F508A392ECCA53F63D2C8283DC0E
SHA-512:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168BA
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/otTCF-ie.js
Preview:	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports)}function n(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return I(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.871131493070463
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	2020-11-27-ZLoader-DLL-example-01.dll
File size:	268288
MD5:	4a64b13ff53aebbab00504f6655ba846
SHA1:	7e75f220f6c9e6be9abd0def54f7d9957540598c
SHA256:	66ec83aa3631d71cba16fd34d1c0b8669009418a92ba683b8a348cd130150b5b
SHA512:	9ab8698724668662bade4fe40cc50bfbd1a3475834d8be1719f2d6ec4b61b0e1848021c0a9444e20e2d0097d46c0e2cc25bf90e25802ad96dc02f84d394735e
SSDEEP:	6144:44GVCjEhWSbz8wyCxxnNz3BGeLprjLnapp:bjH0zH97nNz3BVtAp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...d..:X.....!.....].....@.....@.....k..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x42e15d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x583AB964 [Sun Nov 27 10:45:56 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0

General

File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	ce89ef5fd9b6be62e62903524a066354

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F3BA0CFA937h
call 00007F3BA0CFAEBAh
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007F3BA0CFA7F3h
add esp, 0Ch
pop ebp
retn 000Ch
push ebp
mov ebp, esp
push 00000000h
call dword ptr [00493068h]
push dword ptr [ebp+08h]
call dword ptr [00493064h]
push C0000409h
call dword ptr [0049306Ch]
push eax
call dword ptr [00493070h]
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 00000324h
push 00000017h
call 00007F3BA0D07CB5h
test eax, eax
je 00007F3BA0CFA937h
push 00000002h
pop ecx
int 29h
mov dword ptr [0043F850h], eax
mov dword ptr [0043F84Ch], ecx
mov dword ptr [0043F848h], edx
mov dword ptr [0043F844h], ebx
mov dword ptr [0043F840h], esi
mov dword ptr [0043F83Ch], edi
mov word ptr [0043F868h], ss
mov word ptr [0043F85Ch], cs
mov word ptr [0043F838h], ds
mov word ptr [0043F834h], es
mov word ptr [0043F830h], fs
mov word ptr [0043F82Ch], gs
pushfd
pop dword ptr [0043F860h]
mov eax, dword ptr [ebp+00h]
mov dword ptr [0043F854h], eax
mov eax, dword ptr [ebp+04h]
mov dword ptr [0043F858h], eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3c9f0	0x6b	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x93158	0x28	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x96000	0x558	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x97000	0x1b74	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x10150	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x10204	0x18	.text
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x101a8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x93000	0x154	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3ba5b	0x3bc00	False	0.719636669718	data	6.9029384473	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x3d000	0x5506c	0x2800	False	0.60849609375	data	6.02990562645	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x93000	0x8de	0xa00	False	0.425390625	data	5.09666732564	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0x94000	0x9	0x200	False	0.033203125	data	0.0203931352361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x95000	0xf0	0x200	False	0.265625	data	1.25905126765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x96000	0x558	0x600	False	0.419921875	data	3.85032121203	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x97000	0x1b74	0x1c00	False	0.796316964286	data	6.62208464536	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x960a0	0x338	data	English	United States
RT_MANIFEST	0x963d8	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	FindFirstFileW, TlsSetValue, FindNextFileW, GetShortPathNameW, WaitForMultipleObjects, GetEnvironmentVariableW, GetTempPathW, FindClose, GetFileAttributesW, GetSystemDirectoryW, Sleep, TlsAlloc, CloseHandle, VirtualProtectEx, CopyFileW, OpenMutexW, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, WaitForSingleObjectEx, CreateEventW, GetModuleHandleW, GetProcAddress, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetStartupInfoW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, EncodePointer, GetLastError, InitializeCriticalSectionAndSpinCount, TlsGetValue, TlsFree, FreeLibrary, LoadLibraryExW, RaiseException, InterlockedFlushSList, SetLastError, RtlUnwind, CreateFileW, GetFileType, DuplicateHandle, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, HeapFree, HeapAlloc, HeapReAlloc, WriteFile, GetConsoleCP, GetConsoleMode, MultiByteToWideChar, LCMapStringW, SetStdHandle, SetEndOfFile, ReadFile, ReadConsoleW, SetFilePointerEx, GetStdHandle, FindFirstFileExW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetProcessHeap, GetStringTypeW, HeapSize, FlushFileBuffers, WriteConsoleW, DecodePointer

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x428be2
DllUnregisterServer	2	0x42901c

Version Infos

Description	Data
LegalCopyright	Copyright 1998-2014 End Dead market, Inc
InternalName	Materialboard
FileVersion	2.4.8.142
CompanyName	End Dead market
ProductName	End Dead market
ProductVersion	2.4.8.142
FileDescription	Materialboard
SaidSimple	DanceDevelop
OriginalFilename	East.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 94

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 22:43:39.954159975 CET	49745	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:39.955037117 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:39.987709999 CET	443	49745	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:39.987848997 CET	49745	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:39.988295078 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:39.988415003 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.004946947 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.021687031 CET	49745	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.023526907 CET	49747	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.024178982 CET	49748	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.024346113 CET	49749	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.024400949 CET	49750	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.027093887 CET	49751	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.027453899 CET	49752	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.038425922 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.038578033 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.038646936 CET	443	49746	87.248.118.23	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 22:43:40.038691044 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.038696051 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.038718939 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.038732052 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.038738012 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.038768053 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.038794041 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.038846970 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.042654037 CET	443	49747	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.042762995 CET	49747	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.043123007 CET	443	49748	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.043222904 CET	443	49749	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.043226004 CET	49748	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.043308973 CET	49749	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.043350935 CET	443	49750	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.043634892 CET	49750	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.046005964 CET	443	49751	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.046310902 CET	49751	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.046366930 CET	443	49752	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.046447992 CET	49752	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.054758072 CET	49748	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.054848909 CET	49747	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.055277109 CET	443	49745	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.055311918 CET	49749	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.055392981 CET	49750	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.055443048 CET	443	49745	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.055485010 CET	443	49745	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.055522919 CET	443	49745	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.055541039 CET	49745	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.055558920 CET	443	49745	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.055562973 CET	49745	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.055577993 CET	49745	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.055609941 CET	49745	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.055670977 CET	443	49745	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.055727005 CET	49745	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.073807955 CET	443	49748	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.073865891 CET	443	49747	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.074152946 CET	443	49749	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.074559927 CET	443	49750	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.074771881 CET	443	49748	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.074822903 CET	443	49748	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.074861050 CET	443	49748	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.074861050 CET	49748	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.074901104 CET	49748	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.074908018 CET	49748	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.075171947 CET	443	49747	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.075212002 CET	443	49747	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.075248003 CET	443	49747	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.075310946 CET	49747	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.075346947 CET	49747	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.075351954 CET	49747	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.075717926 CET	443	49749	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.075757980 CET	443	49749	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.075782061 CET	49749	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.075799942 CET	443	49749	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.075822115 CET	49749	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.075850010 CET	49749	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.077092886 CET	443	49750	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.077143908 CET	443	49750	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.077178001 CET	443	49750	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.077229977 CET	49750	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.077327013 CET	49750	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.077339888 CET	49750	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.088140965 CET	49746	443	192.168.2.5	87.248.118.23

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 22:43:40.088558912 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.088828087 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.096708059 CET	49751	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.112453938 CET	49745	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.115772009 CET	443	49751	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.116847038 CET	443	49751	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.116894007 CET	443	49751	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.116919994 CET	443	49751	151.101.1.44	192.168.2.5
Nov 27, 2020 22:43:40.116981983 CET	49751	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.117014885 CET	49751	443	192.168.2.5	151.101.1.44
Nov 27, 2020 22:43:40.121752024 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.121783972 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.121819019 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.121826887 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.121862888 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.121876955 CET	49746	443	192.168.2.5	87.248.118.23
Nov 27, 2020 22:43:40.124722958 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.124763966 CET	443	49746	87.248.118.23	192.168.2.5
Nov 27, 2020 22:43:40.124798059 CET	49746	443	192.168.2.5	87.248.118.23

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 22:43:26.442961931 CET	49992	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:26.469876051 CET	53	49992	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:28.371172905 CET	60075	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:28.406888008 CET	53	60075	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:32.645215034 CET	55016	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:32.691129923 CET	53	55016	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:33.767894030 CET	64345	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:33.805332899 CET	53	64345	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:34.087158918 CET	57128	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:34.114376068 CET	53	57128	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:34.402322054 CET	54791	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:34.418205976 CET	50463	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:34.429546118 CET	53	54791	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:34.455298901 CET	53	50463	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:35.929205894 CET	50394	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:35.973325968 CET	53	50394	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:36.303648949 CET	58530	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:36.349704981 CET	53	58530	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:38.138708115 CET	53813	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:38.181657076 CET	53	53813	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:38.527992964 CET	63732	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:38.573672056 CET	53	63732	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:38.745105028 CET	57344	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:38.782107115 CET	53	57344	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:39.110991001 CET	54450	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:39.138144970 CET	53	54450	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:39.925379038 CET	59261	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:39.942768097 CET	57151	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:39.952429056 CET	53	59261	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:39.979986906 CET	53	57151	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:50.823227882 CET	59413	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:50.860728979 CET	53	59413	8.8.8.8	192.168.2.5
Nov 27, 2020 22:43:54.207802057 CET	60516	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:43:54.234891891 CET	53	60516	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:02.613064051 CET	51649	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:02.648988962 CET	53	51649	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:03.625961065 CET	65086	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:03.636225939 CET	51649	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:03.661459923 CET	53	65086	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:03.671375990 CET	53	51649	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:04.642029047 CET	65086	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 22:44:04.642143011 CET	51649	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:05.656749010 CET	65086	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:06.428375006 CET	53	65086	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:06.428994894 CET	53	65086	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:06.433094025 CET	53	51649	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:06.645351887 CET	51649	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:06.672538042 CET	53	51649	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:07.645775080 CET	65086	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:07.685091019 CET	53	65086	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:10.667717934 CET	51649	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:10.703241110 CET	53	51649	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:11.653943062 CET	65086	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:11.681076050 CET	53	65086	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:15.701215029 CET	56432	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:15.738240004 CET	53	56432	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:15.779808044 CET	52929	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:15.816874027 CET	53	52929	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:15.861572027 CET	64317	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:15.896979094 CET	53	64317	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:17.185578108 CET	61004	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:17.223473072 CET	53	61004	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:20.435095072 CET	56895	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:20.485733986 CET	53	56895	8.8.8.8	192.168.2.5
Nov 27, 2020 22:44:21.373703957 CET	62372	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:44:21.410890102 CET	53	62372	8.8.8.8	192.168.2.5
Nov 27, 2020 22:45:04.724030972 CET	61515	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:45:04.759596109 CET	53	61515	8.8.8.8	192.168.2.5
Nov 27, 2020 22:45:05.874866009 CET	56675	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:45:06.011146069 CET	53	56675	8.8.8.8	192.168.2.5
Nov 27, 2020 22:45:06.927138090 CET	57172	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:45:06.963017941 CET	53	57172	8.8.8.8	192.168.2.5
Nov 27, 2020 22:45:07.966116905 CET	55267	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:45:08.001595974 CET	53	55267	8.8.8.8	192.168.2.5
Nov 27, 2020 22:45:09.232788086 CET	50969	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:45:09.389892101 CET	53	50969	8.8.8.8	192.168.2.5
Nov 27, 2020 22:45:10.293409109 CET	64362	53	192.168.2.5	8.8.8.8
Nov 27, 2020 22:45:10.328844070 CET	53	64362	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 22:43:34.087158918 CET	192.168.2.5	8.8.8.8	0x539e	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:35.929205894 CET	192.168.2.5	8.8.8.8	0x9695	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:36.303648949 CET	192.168.2.5	8.8.8.8	0x4b0a	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:38.138708115 CET	192.168.2.5	8.8.8.8	0x12bf	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:38.527992964 CET	192.168.2.5	8.8.8.8	0x669b	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:38.745105028 CET	192.168.2.5	8.8.8.8	0xb63	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:39.110991001 CET	192.168.2.5	8.8.8.8	0xe549	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:39.925379038 CET	192.168.2.5	8.8.8.8	0xa371	Standard query (0)	s.yimg.com	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:39.942768097 CET	192.168.2.5	8.8.8.8	0xa8af	Standard query (0)	img.img-ta boola.com	A (IP address)	IN (0x0001)
Nov 27, 2020 22:44:20.435095072 CET	192.168.2.5	8.8.8.8	0x1206	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:04.724030972 CET	192.168.2.5	8.8.8.8	0x5c98	Standard query (0)	hac3r.com	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:05.874866009 CET	192.168.2.5	8.8.8.8	0xe2ab	Standard query (0)	womtools.com	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:06.927138090 CET	192.168.2.5	8.8.8.8	0x5191	Standard query (0)	valitec.co	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 22:45:07.966116905 CET	192.168.2.5	8.8.8.8	0xbfec	Standard query (0)	empresascr eciendobien.com	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:09.232788086 CET	192.168.2.5	8.8.8.8	0xaf77	Standard query (0)	smartat.co	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:10.293409109 CET	192.168.2.5	8.8.8.8	0x1fe8	Standard query (0)	teamearent topdiaty.ga	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 22:43:34.114376068 CET	8.8.8.8	192.168.2.5	0x539e	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 22:43:35.973325968 CET	8.8.8.8	192.168.2.5	0x9695	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 22:43:36.349704981 CET	8.8.8.8	192.168.2.5	0x4b0a	No error (0)	contextual.media.net		23.57.80.37	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:38.181657076 CET	8.8.8.8	192.168.2.5	0x12bf	No error (0)	hblg.media.net		23.57.80.37	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:38.573672056 CET	8.8.8.8	192.168.2.5	0x669b	No error (0)	lg3.media.net		23.57.80.37	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:38.782107115 CET	8.8.8.8	192.168.2.5	0xb63	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 22:43:39.138144970 CET	8.8.8.8	192.168.2.5	0xe549	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 22:43:39.138144970 CET	8.8.8.8	192.168.2.5	0xe549	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 22:43:39.952429056 CET	8.8.8.8	192.168.2.5	0xa371	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 22:43:39.952429056 CET	8.8.8.8	192.168.2.5	0xa371	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:39.952429056 CET	8.8.8.8	192.168.2.5	0xa371	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:39.979986906 CET	8.8.8.8	192.168.2.5	0xa8af	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 22:43:39.979986906 CET	8.8.8.8	192.168.2.5	0xa8af	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:39.979986906 CET	8.8.8.8	192.168.2.5	0xa8af	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:39.979986906 CET	8.8.8.8	192.168.2.5	0xa8af	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Nov 27, 2020 22:43:39.979986906 CET	8.8.8.8	192.168.2.5	0xa8af	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Nov 27, 2020 22:44:20.485733986 CET	8.8.8.8	192.168.2.5	0x1206	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 22:45:04.759596109 CET	8.8.8.8	192.168.2.5	0x5c98	No error (0)	hac3r.com		70.32.23.26	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:06.011146069 CET	8.8.8.8	192.168.2.5	0xe2ab	No error (0)	womtools.com		70.32.23.26	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:06.963017941 CET	8.8.8.8	192.168.2.5	0x5191	No error (0)	valitec.co		70.32.23.26	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:08.001595974 CET	8.8.8.8	192.168.2.5	0xbfec	No error (0)	empresascr eciendobien.com		70.32.23.26	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:09.389892101 CET	8.8.8.8	192.168.2.5	0xaf77	No error (0)	smartat.co		70.32.23.26	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 22:45:10.328844070 CET	8.8.8.8	192.168.2.5	0x1fe8	No error (0)	teamearent topdiaty.ga		172.67.155.205	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:10.328844070 CET	8.8.8.8	192.168.2.5	0x1fe8	No error (0)	teamearent topdiaty.ga		104.27.142.240	A (IP address)	IN (0x0001)
Nov 27, 2020 22:45:10.328844070 CET	8.8.8.8	192.168.2.5	0x1fe8	No error (0)	teamearent topdiaty.ga		104.27.143.240	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 22:43:40.038794041 CET	87.248.118.23	443	192.168.2.5	49746	CN=*.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Nov 15 01:00:00 CET 2020	Wed Dec 30 00:59:59 CET 2020	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 27, 2020 22:43:40.055670977 CET	87.248.118.23	443	192.168.2.5	49745	CN=*.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Nov 15 01:00:00 CET 2020	Wed Dec 30 00:59:59 CET 2020	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 27, 2020 22:43:40.074861050 CET	151.101.1.44	443	192.168.2.5	49748	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Nov 27, 2020 22:43:40.075248003 CET	151.101.1.44	443	192.168.2.5	49747	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

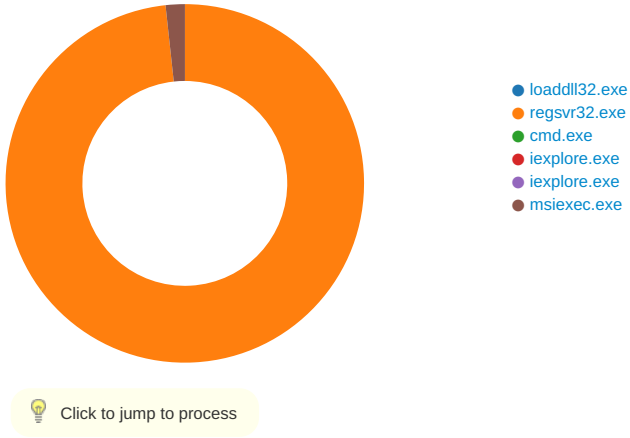
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 22:43:40.075799942 CET	151.101.1.44	443	192.168.2.5	49749	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Nov 27, 2020 22:43:40.077178001 CET	151.101.1.44	443	192.168.2.5	49750	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Nov 27, 2020 22:43:40.116919994 CET	151.101.1.44	443	192.168.2.5	49751	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Nov 27, 2020 22:43:40.149697065 CET	151.101.1.44	443	192.168.2.5	49752	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Nov 27, 2020 22:45:05.084462881 CET	70.32.23.26	443	192.168.2.5	49768	CN=webmail.hac3r.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 30 09:14:58 CET 2020	Thu Jan 28 09:14:58 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 22:45:06.270901918 CET	70.32.23.26	443	192.168.2.5	49769	CN=webdisk.womtools.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 30 17:34:03 CET 2020	Thu Jan 28 17:34:03 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 27, 2020 22:45:07.227643967 CET	70.32.23.26	443	192.168.2.5	49770	CN=cpcalendars.valitec.co CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 30 17:31:53 CET 2020	Thu Jan 28 17:31:53 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 27, 2020 22:45:08.435188055 CET	70.32.23.26	443	192.168.2.5	49771	CN=webmail.empresascreciendobien.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 30 09:11:40 CET 2020	Thu Jan 28 09:11:40 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 27, 2020 22:45:09.647250891 CET	70.32.23.26	443	192.168.2.5	49772	CN=smartat.co CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 30 17:20:08 CET 2020	Thu Jan 28 17:20:08 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 27, 2020 22:45:10.381675959 CET	172.67.155.205	443	192.168.2.5	49773	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Sep 28 02:00:00 CEST 2020	Tue Sep 28 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 4748 Parent PID: 5604

General

Start time:	22:43:31
Start date:	27/11/2020
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\2020-11-27-ZLoader-DLL-example-01.dll'
Imagebase:	0xbd0000
File size:	119808 bytes
MD5 hash:	76E2251D0E9772B9DA90208AD741A205
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 4696 Parent PID: 4748

General

Start time:	22:43:31
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\2020-11-27-ZLoader-DLL-example-01.dll
Imagebase:	0x1010000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW
C:\Users\user\AppData\Local\Temp\1.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDACD25	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW
C:\Users\user\AppData\Local\Temp\1.log	success or wait	1	6DDAC963	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	01 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	02 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	03 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	04 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	05 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	06 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	07 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	08 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	09 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0a 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0b 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0c 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0d 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0e 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0f 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	10 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	11 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	12 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	13 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	14 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	15 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	16 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	17 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	18 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	19 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1a 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1b 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1c 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1d 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1e 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1f 00 00 00	....	success or wait	1	6DDACD4D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	20 00 00 00	...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	21 00 00 00	!...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	22 00 00 00	"...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	23 00 00 00	#...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	24 00 00 00	$...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	25 00 00 00	%...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	26 00 00 00	&...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	27 00 00 00	'...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	28 00 00 00	(...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	29 00 00 00	)...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2a 00 00 00	*...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2b 00 00 00	+...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2c 00 00 00	,...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2d 00 00 00	-...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2e 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2f 00 00 00	/...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	30 00 00 00	0...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	31 00 00 00	1...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	32 00 00 00	2...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	33 00 00 00	3...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	34 00 00 00	4...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	35 00 00 00	5...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	36 00 00 00	6...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	37 00 00 00	7...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	38 00 00 00	8...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	39 00 00 00	9...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3a 00 00 00	:...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3b 00 00 00	;...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3c 00 00 00	<...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3d 00 00 00	=...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3e 00 00 00	>...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3f 00 00 00	?...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	40 00 00 00	@...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	41 00 00 00	A...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	42 00 00 00	B...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	43 00 00 00	C...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	44 00 00 00	D...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	45 00 00 00	E...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	46 00 00 00	F...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	47 00 00 00	G...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	48 00 00 00	H...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	49 00 00 00	I...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4a 00 00 00	J...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4b 00 00 00	K...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4c 00 00 00	L...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4d 00 00 00	M...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4e 00 00 00	N...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4f 00 00 00	O...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	50 00 00 00	P...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	51 00 00 00	Q...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	52 00 00 00	R...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	53 00 00 00	S...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	54 00 00 00	T...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	55 00 00 00	U...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	56 00 00 00	V...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	57 00 00 00	W...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	58 00 00 00	X...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	59 00 00 00	Y...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5a 00 00 00	Z...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5b 00 00 00	[...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5c 00 00 00	\...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5d 00 00 00	]...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5e 00 00 00	^...	success or wait	1	6DDACD4D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5f 00 00 00	_...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	60 00 00 00	`...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	61 00 00 00	a...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	62 00 00 00	b...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	63 00 00 00	c...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	64 00 00 00	d...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	65 00 00 00	e...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	66 00 00 00	f...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	67 00 00 00	g...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	68 00 00 00	h...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	69 00 00 00	i...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6a 00 00 00	j...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6b 00 00 00	k...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6c 00 00 00	l...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6d 00 00 00	m...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6e 00 00 00	n...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6f 00 00 00	o...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	70 00 00 00	p...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	71 00 00 00	q...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	72 00 00 00	r...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	73 00 00 00	s...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	74 00 00 00	t...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	75 00 00 00	u...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	76 00 00 00	v...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	77 00 00 00	w...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	78 00 00 00	x...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	79 00 00 00	y...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7a 00 00 00	z...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7b 00 00 00	{...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7c 00 00 00	|...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7d 00 00 00	}...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7e 00 00 00	~...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7f 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	80 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	81 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	82 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	83 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	84 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	85 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	86 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	87 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	88 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	89 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8a 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8b 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8c 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8d 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8e 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8f 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	90 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	91 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	92 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	93 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	94 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	95 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	96 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	97 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	98 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	99 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9a 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9b 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9c 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9d 00 00 00	....	success or wait	1	6DDACD4D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9e 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9f 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a0 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a1 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a2 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a3 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a4 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a5 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a6 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a7 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a8 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a9 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	aa 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ab 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ac 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ad 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ae 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	af 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b0 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b1 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b2 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b3 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b4 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b5 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b6 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b7 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b8 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b9 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ba 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	bb 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	bc 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	bd 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	be 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	bf 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c0 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c1 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c2 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c3 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c4 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c5 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c6 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c7 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c8 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c9 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ca 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	cb 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	cc 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	cd 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ce 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	cf 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d0 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d1 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d2 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d3 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d4 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d5 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d6 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d7 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d8 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d9 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	da 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	db 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	dc 00 00 00	....	success or wait	1	6DDACD4D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	dd 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	de 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	df 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e0 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e1 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e2 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e3 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e4 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e5 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e6 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e7 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e8 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e9 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ea 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	eb 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ec 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ed 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ee 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ef 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f0 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f1 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f2 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f3 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f4 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f5 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f6 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f7 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f8 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f9 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	fa 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	fb 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	fc 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	fd 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	fe 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ff 00 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	00 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	01 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	02 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	03 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	04 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	05 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	06 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	07 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	08 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	09 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0a 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0b 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0c 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0d 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0e 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	0f 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	10 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	11 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	12 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	13 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	14 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	15 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	16 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	17 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	18 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	19 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1a 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1b 01 00 00	....	success or wait	1	6DDACD4D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1c 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1d 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1e 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	1f 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	20 01 00 00	...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	21 01 00 00	!...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	22 01 00 00	"...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	23 01 00 00	#...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	24 01 00 00	$...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	25 01 00 00	%...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	26 01 00 00	&...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	27 01 00 00	'...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	28 01 00 00	(...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	29 01 00 00	)...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2a 01 00 00	*...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2b 01 00 00	+...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2c 01 00 00	,...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2d 01 00 00	-...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2e 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	2f 01 00 00	/...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	30 01 00 00	0...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	31 01 00 00	1...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	32 01 00 00	2...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	33 01 00 00	3...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	34 01 00 00	4...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	35 01 00 00	5...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	36 01 00 00	6...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	37 01 00 00	7...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	38 01 00 00	8...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	39 01 00 00	9...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3a 01 00 00	:...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3b 01 00 00	;...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3c 01 00 00	<...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3d 01 00 00	=...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3e 01 00 00	>...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	3f 01 00 00	?...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	40 01 00 00	@...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	41 01 00 00	A...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	42 01 00 00	B...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	43 01 00 00	C...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	44 01 00 00	D...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	45 01 00 00	E...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	46 01 00 00	F...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	47 01 00 00	G...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	48 01 00 00	H...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	49 01 00 00	I...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4a 01 00 00	J...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4b 01 00 00	K...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4c 01 00 00	L...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4d 01 00 00	M...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4e 01 00 00	N...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	4f 01 00 00	O...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	50 01 00 00	P...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	51 01 00 00	Q...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	52 01 00 00	R...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	53 01 00 00	S...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	54 01 00 00	T...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	55 01 00 00	U...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	56 01 00 00	V...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	57 01 00 00	W...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	58 01 00 00	X...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	59 01 00 00	Y...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5a 01 00 00	Z...	success or wait	1	6DDACD4D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5b 01 00 00	[...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5c 01 00 00	\...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5d 01 00 00	]...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5e 01 00 00	^...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	5f 01 00 00	_...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	60 01 00 00	`...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	61 01 00 00	a...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	62 01 00 00	b...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	63 01 00 00	c...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	64 01 00 00	d...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	65 01 00 00	e...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	66 01 00 00	f...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	67 01 00 00	g...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	68 01 00 00	h...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	69 01 00 00	i...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6a 01 00 00	j...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6b 01 00 00	k...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6c 01 00 00	l...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6d 01 00 00	m...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6e 01 00 00	n...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	6f 01 00 00	o...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	70 01 00 00	p...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	71 01 00 00	q...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	72 01 00 00	r...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	73 01 00 00	s...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	74 01 00 00	t...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	75 01 00 00	u...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	76 01 00 00	v...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	77 01 00 00	w...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	78 01 00 00	x...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	79 01 00 00	y...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7a 01 00 00	z...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7b 01 00 00	{...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7c 01 00 00	|...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7d 01 00 00	}...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7e 01 00 00	~...	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	7f 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	80 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	81 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	82 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	83 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	84 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	85 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	86 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	87 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	88 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	89 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8a 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8b 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8c 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8d 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8e 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	8f 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	90 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	91 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	92 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	93 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	94 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	95 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	96 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	97 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	98 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	99 01 00 00	....	success or wait	1	6DDACD4D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9a 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9b 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9c 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9d 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9e 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	9f 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a0 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a1 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a2 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a3 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a4 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a5 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a6 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a7 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a8 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	a9 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	aa 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ab 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ac 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ad 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ae 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	af 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b0 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b1 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b2 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b3 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b4 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b5 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b6 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b7 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b8 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	b9 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ba 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	bb 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	bc 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	bd 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	be 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	bf 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c0 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c1 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c2 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c3 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c4 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c5 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c6 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c7 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c8 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	c9 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ca 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	cb 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	cc 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	cd 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ce 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	cf 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d0 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d1 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d2 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d3 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d4 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d5 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d6 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d7 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d8 01 00 00	....	success or wait	1	6DDACD4D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	d9 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	da 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	db 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	dc 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	dd 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	de 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	df 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e0 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e1 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e2 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e3 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e4 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e5 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e6 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e7 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e8 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	e9 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ea 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	eb 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ec 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ed 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ee 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	ef 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f0 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f1 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f2 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f3 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f4 01 00 00	....	success or wait	1	6DDACD4D	WriteFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	f5 01 00 00	....	success or wait	1	6DDACD4D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile
C:\Users\user\AppData\Local\Temp\1.log	unknown	4	success or wait	1	6DDACA47	ReadFile

Analysis Process: cmd.exe PID: 3940 Parent PID: 4748

General

Start time:	22:43:31
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe'
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 3868 Parent PID: 3940

General

Start time:	22:43:32
Start date:	27/11/2020

Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff7231f0000
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: 5976 Parent PID: 3868

General

Start time:	22:43:32
Start date:	27/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3868 CREDAT:17410 /prefetch:2
Imagebase:	0xff0000
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

Registry Activities

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

Analysis Process: msiexec.exe PID: 2028 Parent PID: 4696

General

Start time:	22:45:00
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe
Imagebase:	0xda0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Wigy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Zeofo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Voso	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Boy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Figyf	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Oly	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Awum	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Onurg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Paa	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ivorq	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ogoq	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ewta	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Obg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Myam	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3810B9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Wigy\fihoa.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3882CD	CreateFileW
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	3826DF	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3826DF	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3826DF	HttpSendRequestA
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	3826DF	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3826DF	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3826DF	HttpSendRequestA
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	3826DF	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3826DF	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3826DF	HttpSendRequestA
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	3826DF	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3826DF	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3826DF	HttpSendRequestA

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Wigy\fihoa.dll	unknown	268288	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 64 b9 3a 58 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 00 00 bc 03 00 00 82 05 00 00 00 00 00 5d e1 02 00 00 10 00 00 00 d0 03 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 90 09 00 00 04 00 00 00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f0 c9 03 00 6b 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...d.:X.......... .!................]........... ..@........................... ....@................. ....k..	success or wait	1	3882FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\2020-11-27-ZLoader-DLL-example-01.dll	unknown	268288	success or wait	1	37A63A	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Otnyop	success or wait	1	384463	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\brya	success or wait	1	37CEB1	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\brya	ilyo	binary	42 AD AA 2C 0E 53 59 8A 3C 8D 46 81 A3 3C 7C 8D 4A 1F 61 0E E7 99 95 31 14 FF D2 E8 2F 68 EA E1 FD 8F 7A CE 0C D0 01 EA 48 AD 90 9E DC D7 3D 30 5A F1 DD 19 BD 35 BB 5B 4F A7 F4 5E BB 47 C0 62 D4 C6 EE 1E FD DA 23 70 9C 6C C7 0D D7 34 B0 25 23 3D 74 D6 AD 06 A7 D5 C4 F5 2E E3 1E 54 2E 03 26 DB 6D 1C 4C FC 60 14 97 95 9F 43 92 54 2F F0 C0 6F 6F 97 CF CB 0A 5D AB EC 89 B5 4A 1E 4E 73 74 C7 0E 6A AF 93 22 6B 56 77 70 16 74 2D 00 0D 17 E8 B8 8D C5 1C 24 67 F2 F6 39 59 4A EC 58 AD C4 4A 98 D0 F1 C8 E3 EE F9 24 AB CA 2F 65 CD 31 10 13 ED 74 15 89 FE F1 DF FF FE DC 86 78 55 35 04 E5 04 5D 9C 8D E0 BE 78 EC B0 47 D9 A0 29 CC 57 4E F8 E7 81 CC B2 CC 21 86 7A 32 DF 48 30 D9 A1 06 2E 33 C6 1B C0 A9 CF 26 D3 DC 93 BC EC E1 B7 77 28 7D 58 55 8B 35 09 1F 14 DA E9 82 4F 42 83 05 15 2A EC 84 E9 CA 06 2D DA 1A BD 91 2B C7 41 2A B6 4B E5 E0 F1 AA FD 60 CB B6 64 CA 3C 94 CF 47 D8 BD 2E 9E 40 68 C7 AC 1C D5 D1 31 80 A3 17 3E FF C9 CA AE EE 7C CB 4C C2 F7 E4 8F 23 40 83 29 52 7D C2 EB 2D 94 4C D7 94 82 3A B2 36 E2 3F BB 96 A6 D8 CD B4 01 1E F1 86 DF 44 68 6C 02 BD 83 D8 90 8C 97 26 82 1F B4 E1 E8 28 71 12 07 59 4B 85 29 15 7E 3E A5 2C B0 1B 41 F3 66 CA 7C C2 85 14 46 2B 8E FD 98 BB F9 2F F8 5D 02 23 84 65 7A 9C FA 65 29 DA 73 5A A3 12 8E F7 E2 FA 16 0B 41 68 6B EC 7D E4 72 64 54 97 23 C3 B8 2E A4 21 6E AB B0 10 22 5A 7B 92 D7 04 13 7F B2 45 63 F7 71 1D 08 3D F8 F2 CF 71 E4 5F 8E 37 02 AE 8A 76 54 89 C7 49 E4 2F 25 02 2F FC 26 49 58 B4 71 4D 5E BB 19 0B 04 05 FE 3E 51 29 24 1F F2 E1 B7 99 28 29 37 18 AD 3F 61 91 87 54 39 3F E7 02 C0 2E 1F BE DB 3B 4E 70 4F 65 F1 21 BF BC 8C 6B 45 C7 9E 17 17 E8 72 74 AF 35 1D 13 7C F4 D8 CA 4C A8 23 26 05 FB 2A FD 8D 24 0E F6 39 0C 69 7A D3 CE 39 6B D9 DE DB E6 30 A4 FA EE 99 3B 3E 6A AB A4 ED D3 21 46 5C BD DD 28 E9 B6 4E C8 18 15 9D 58 97 F8 BC D3 37 73 31 51 41 E0 16 C3 3A C0 F5 AD 90 8D 2D CC 31 68 3E 10 8E 06 79 4B 88 8C 95 A0 08 BD 1A DD 8E BC 96 DC A7 EE FB 77 E4 10 5D 5F BE 56 23 99 94 BC 89 44 F4 C5 42 96 09 BA 16 F0 78 68 A7 04 96 4C 0E A8 E8 03 E9 29 FB BF 4A 6D 6B 74 6C EA 75 4E CC 01 94 D1 36 16 42 B0 B9 84 87 24 D8 B7 D2 97 CC D7 36 3A CD 2A 61 97 A9 3E 20 42 54 1D FA D5 CB E4 2E 71 54 02 95 FC 90 E9 76 CB DA 16 24 A0 8E EA BE 09 FE F7 5A 8D 26 2C 78 0E 1A 98 56 E9 F8 F9 CF 04 3C 0F 14 88 16 58 52 03 27 F9 C5 7B 9D 62 F3 44 1A 2F 37 BA 15 B7 D7 65 EC 5D BE 54 EC 69 F5 B8 C1 6B 4B E5 CE 3A D5 51 C5 CB ED 4A D0 E6 D2 83 9A 22 DD 41 F5 1B 8E 6F 05 98 DD 1B CF 76 54 09 FE 4F BF 72 E9 53 B5 28 B3 9A A9 97 DD 94 37 16 1D 27 FD B7 36 55 D1 34 C9 DB 70 56 93 57 1D 12 65 8B 48 9C 9B 58 64 1F 9B 82 68 D5 3E 5D 8C 01 86 30 96 73 67 46	success or wait	1	37CEF4	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			1E D5 F9 32 8A AD E8 30 00 73 46 94 51 13 4A 5E 91 CE 7B FE CD 71 78 49 49 E9 88 20 45 29 3F 22 65 AD 99 88 A8 1A 1D 4D 3F 7A 38 70 9C 48 C0 55 68 02 E3 E9 35 6D 58 91 EB E3 CE 4D 5F E8 C1 3A 11 4A 36 8A 37 8F 7E 58 25 F3 AE 0C EE 67 9E DE 0C 1D 66 18 7D 5E BF FC C3 6E E4 2C 10 3D 46 85 B7 7D B3 B2 7A 3A CD 00 B3 CE 8D 00 78 5D E4 FF 29 C7 E8 19 05 43 B1 7F 00 88 94 AD D6 46 B7 BA AA 08 40 9E 75 BC 39 57 24 21 43 D8 41 FB 0A 98 06 0C E0 4D F7 98 62 C9 1C E4 91 FC 48 84 51 A5 FB 96 CE B3 DC A3 C9 39 E5 C8 EC 77 A4 69 50 6A 0B B1 BF B8 F8 81 FC 17 7D 50 15 6B C3 50 43 1D 15 9E BF 26 69 0D 8E 2C 5C 6B 50 13 A9 D1 F1 E7 4B EF DC 30 71 93 89 6C DC 28 B8 74 F6 FD 04 17 B8 33 D0 F7 47 CA EB 35 DA 22 DB DA B5 11 5C BB FB A1 0D 0D 26 56 13 57 AC DB A8 51 D5 CF 99 C6 AF 52 28 34 BF 53 36 7D 1B 99 1A A6 B7 BB 2D B5 90 4B 2F EE 15 7E 8F 93 29 FF AA D6 74 A8 45 EF E6 D0 9A 7B 99 5C F3 F0 06 D8 1C 80 AE 72 05 E9 2D 30 6B 7C 90 22				
HKEY_CURRENT_USER\Software\Microsoft\Otnyop	akpyinco	binary	BC F2 40 4E CC 22 AD 0E 6B A3 D2 C0 F5 43 DF D3 AF 4A 38 72 AA 2C AF 31 61 DC 8D 3A E8 B0 C6 E3 0C 3A 4F 93 75 31 36 48 AB 57 D9 69 C2 64 A0 64 1E 07 BD B2 6F 94 7F DF 3B B6 66 FB CF C9 3F FC D7 55 BE 4C 39 2E E0 3A A1 86 AB 48 F7 E8 47 14 2E C7 E2 0E 02 B5 23 7F E6 C6 17 8C 62 07 3B EA 68 6E 67 C8 58 37 1D 3D 16 CE 5A 90 7A AF 8A AA DF 9D 81 46 92 3E F7 97 5D 76 64 A6 4E 6E 62 97 DA 5F 5A BB 15 B0 D4 6C 30 C9 3B 8F 9B 40 CB 13 9F 9B 7F C4 74 AF 2F 62 FF 27 10 C1 6F 68 A1 7A 30 2E BB EB 00 C7 E7 09 E7 E9 C5 DC CF 3C 9F 07 26 82 26 3B EE 94 42 23 67 0F 67 8C C1 CD F3 47 57 12 B0 26 29 0F AA 26 A8 4E 29 28 F9 DB 93 E9 79 AF 6E F1 94 28 92 8E 3B 2B 72 8A 6F 54 02 26 81 FD 92 8C 20 45 85 72 EC 02 13 27 77 1C 25 78 39 77 6F 37 C5 A4 32 A8 2F AA 3E 29 C0 2F E7 12 EA 44 B2 FD 52 9F DF 01 45 DA D9 27 9A 34 5B 60 84 6F 51 A0 88 F3 76 0A 60 EE A1 F0 D4 AE 21 A8 CA AA 56 42 81 48 A1 25 66 B9 CD EB 6E 3D 63 B1 57 44	success or wait	1	37CEF4	RegSetValueExW

Key Value Modified

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Otnyop	akpyinco	binary	BC F2 40 4E CC 22 AD 0E 6B A3 D2 C0 F5 43 DF D3 AF 4A 38 72 AA 2C AF 31 61 DC 8D 3A E8 B0 C6 E3 0C 3A 4F 93 75 31 36 48 AB 57 D9 69 C2 64 A0 64 1E 07 BD B2 6F 94 7F DF 3B B6 66 FB CF C9 3F FC D7 55 BE 4C 39 2E E0 3A A1 86 AB 48 F7 E8 47 14 2E C7 E2 0E 02 B5 23 7F E6 C6 17 8C 62 07 3B EA 68 6E 67 C8 58 37 1D 3D 16 CE 5A 90 7A AF 8A AA DF 9D 81 46 92 3E F7 97 5D 76 64 A6 4E 6E 62 97 DA 5F 5A BB 15 B0 D4 6C 30 C9 3B 8F 9B 40 CB 13 9F 9B 7F C4 74 AF 2F 62 FF 27 10 C1 6F 68 A1 7A 30 2E BB EB 00 C7 E7 09 E7 E9 C5 DC CF 3C 9F 07 26 82 26 3B EE 94 42 23 67 0F 67 8C C1 CD F3 47 57 12 B0 26 29 0F AA 26 A8 4E 29 28 F9 DB 93 E9 79 AF 6E F1 94 28 92 8E 3B 2B 72 8A 6F 54 02 26 81 FD 92 8C 20 45 85 72 EC 02 13 27 77 1C 25 78 39 77 6F 37 C5 A4 32 A8 2F AA 3E 29 C0 2F E7 12 EA 44 B2 FD 52 9F DF 01 45 DA D9 27 9A 34 5B 60 84 6F 51 A0 88 F3 76 0A 60 EE A1 F0 D4 AE 21 A8 CA AA 56 42 81 48 A1 25 66 B9 CD EB 6E 3D 63 B1 57 44	11 49 9A 0D 93 43 9F 3E 03 F7 F8 F1 18 F6 69 08 BC D2 AA E0 0D 8B 08 96 C6 7B 2A 9D 4C 14 62 47 3D 19 38 8F 98 F3 59 45 95 AB 6F 12 49 02 87 1C 66 7F C5 CA 17 EC 07 A7 43 CE 1E 83 B7 B1 47 84 AF 2D C6 34 41 56 98 42 D9 FE D3 30 8F 90 3F 6C AD 68 F8 3F 29 51 72 4F 32 9B D2 90 81 94 9E 90 73 B4 2A 12 E1 93 01 85 FF A4 80 AA B1 D0 32 C7 F2 3C 9E 95 80 26 F1 A3 76 A0 47 F2 E9 B8 B7 B8 FE 7C D8 0E 60 FF 3E 3E C2 52 CB 6D 18 C2 54 43 F0 89 BC	success or wait	1	37CEF4	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Otnyop	akpyinco	binary	11 49 9A 0D 93 43 9F 3E 03 F7 F8 F1 18 F6 69 08 BC D2 AA E0 0D 8B 08 96 C6 7B 2A 9D 4C 14 62 47 3D 19 38 8F 98 F3 59 45 95 AB 6F 12 49 02 87 1C 66 7F C5 CA 17 EC 07 A7 43 CE 1E 83 B7 B1 47 84 AF 2D C6 34 41 56 98 42 D9 FE D3 30 8F 90 3F 6C AD 68 F8 3F 29 51 72 4F 32 9B D2 90 81 94 9E 90 73 B4 2A 12 E1 93 01 85 FF A4 80 AA B1 D0 32 C7 F2 3C 9E 95 80 26 F1 A3 76 A0 47 F2 E9 B8 B7 B8 FE 7C D8 0E 60 FF 3E 3E C2 52 CB 6D 18 C2 54 43 F0 89 BC	03 B6 F3 4A FE 04 AE 81 4B 2A 9C 3F B5 1F B5 35 D2 DD E8 8B 7B FD 7E E0 B0 0D 5C EB 3B 63 15 30 B8 8C C4 1E 2E E6 8F 0F 42 E4 AE 6A 16 D0 0E EE 94 8D 37 38 E5 1E F5 55 B1 3C EC 71 45 43 B5 76 5D DF 34 C6 B3 A4 6A B0 2B 0C 21 C2 7D 62 CD 9E 5F 9A 0A CD DB A3 80 BD C0 69 20 62 73 66 6C 62 81 46 D8 E0 13 6B 7F F0 AE 04 0A A8 74 85 56 1A C3 91 AE 09 2B 55 90 EF 75 B7 14 82 B5 04 16 CE BF 31 2A AB 34 BE 3E F4 E3 E8 1E C5 F8 51 2B D1 0E 07 C8 72 FA 3C 7C 12 09 20 B6 1F 22 64 AD C4 8F 98 1E D6 6E 60 44 8D FB CD 22 E2 3E 85 0A EA 34 A4 CD EE F1 68 54 6A 09 EB C0 A3 AB CB E2 75 4D 0B 52 AC 21 84 37 AB 9A FE 56 F0 6C D3 20 D6 F6 22 55 19 EE 7F 9C D8 60 71 E6 55 45 54 6E C5 B6 E0 F6 25 E8 81 05 41 0F 9E A6 14 3B 9A 7E 02 9C 49 22 1D D4 84 E5 C6 B7 03 A8 47 D6 25 A9 E4 2A F0 14 24 A2 DD 91 03 15 9F 26 5F 00 61 BC D8 5E E3 57 DA 72 E2 9F 0B C1 F2 5C EC 98 B8 62 C5 33 07 6F 53 5E 17 19 11 B0 73 F3 5E CD F4 C7 0F DC 48 EB 01 3F EC E6 5E 7A AC 4A 96 F0 8F 06 18 2B 53 F7 06 CB 6A 21 87 CC 28 D6 20 C6 70 AC D9 5A 5C 36 43 FE 10 3A 50 EF 16 36 88 79 4C 17 7B 12 E8 A0	success or wait	1	37CEF4	RegSetValueExW

Disassembly

Code Analysis