Toggle navigation JoeSandbox Cloud BASIC

- Overview
- Screenshots
- Behavior Graph
- Classification
- Network Map

General Information

- **Date:**25.08.2020
- **Duration:**0h 7m 27s
- **Sample file name:**GUIControlSoftware-setup.exe
- **Cookbook:**default.jbs
- **Icon:**
- **Filetype:**exe

Detection

SUSPICIOUS

-
    - Found **3** malicious signatures
    - Contacts **3** domains/IPs
    - Launches **3** processes
    - Drops **88** files

Signature Overview

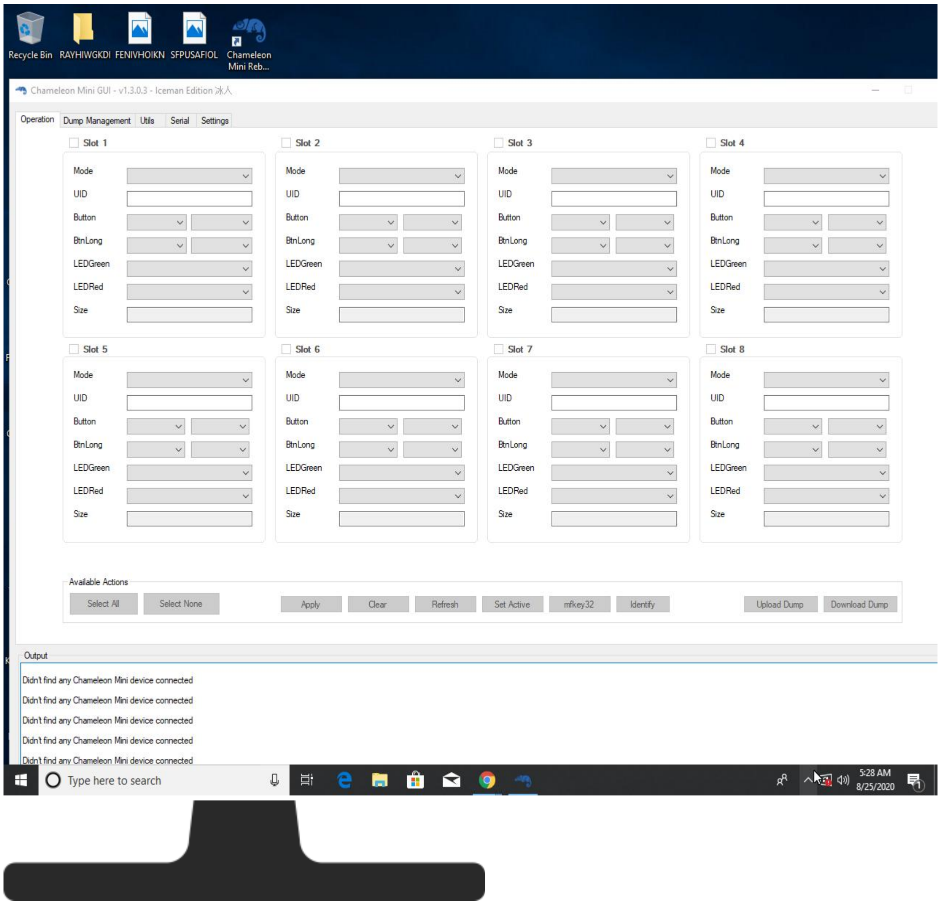
Networking	9
Malware Analysis System Evasion	9
Anti Debugging	6
Language, Device and Operating System Detection	5
Data Obfuscation	3
Hooking and other Techniques for Hiding and Protection	3

Show File Information

Show Signature Information

Screenshots

Behavior



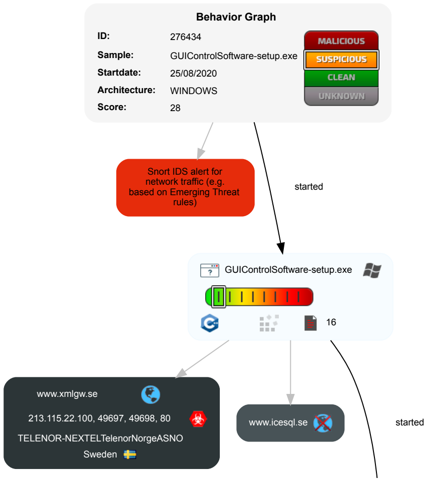
```
Didn't find any Chameleon Mini device connected
Didn't find any Chameleon Mini device connected
Didn't find any Chameleon Mini device connected
Didn't find any Chameleon Mini device connected
Didn't find any Chameleon Mini device connected
```

Click here to start
Slideshow Behavior Animation

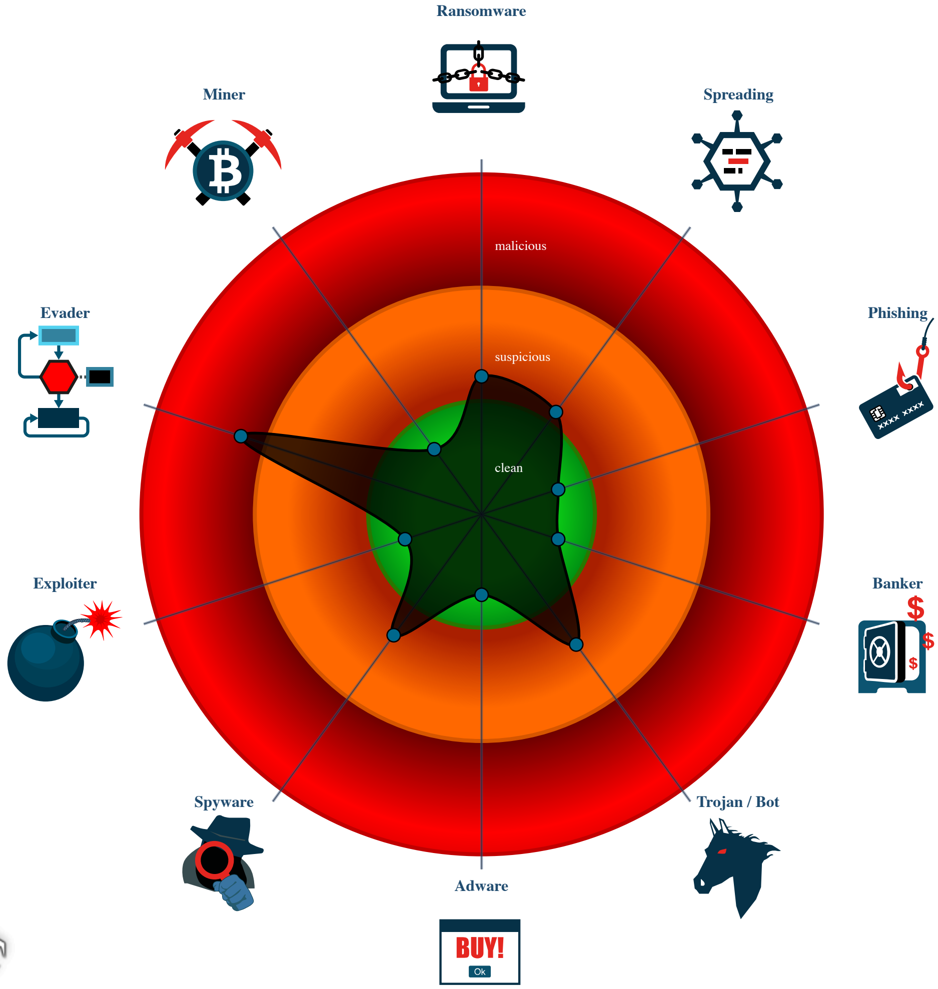
Behavior Graph

Legend:

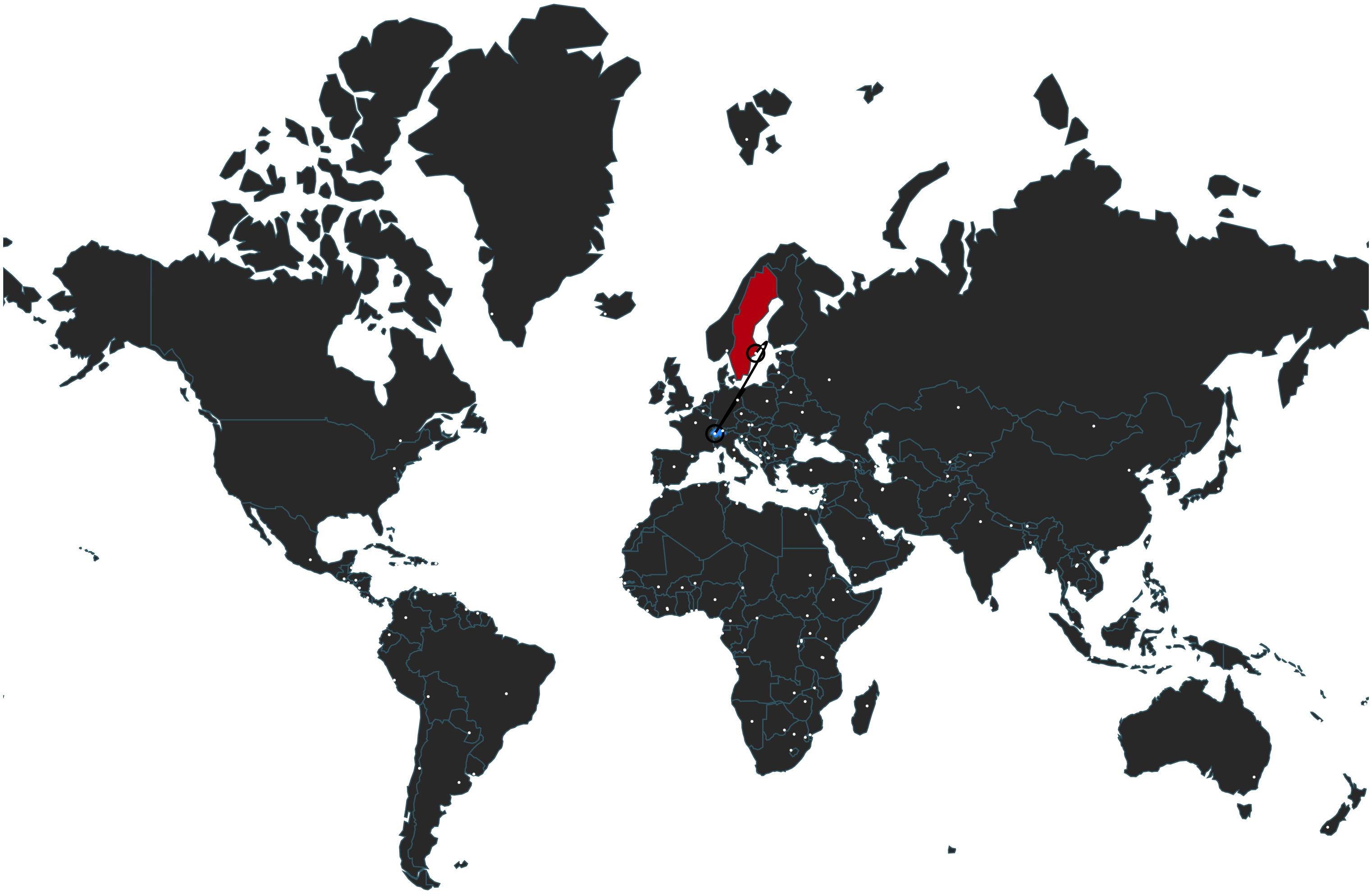
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet



Classification


Ransomware
Spreading
Phishing
Banker
Trojan / Bot
Adware
Spyware
Exploiter
Evader
Miner
malicious
suspicious
clean
xxxx xxxx
$
$
$
BUY!
Ok

[Network Map](#)



- No. of IPs < 25%
- 25% < No. of IPs < 50%
- 50% < No. of IPs < 75%
- 75% < No. of IPs

Contacted Public IPs

IP	Country	Flag	ASN	ASN Name	Malicious
213.115.22.100	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	true

Contacted Domains

Name	IP	Active
www.xmlgw.se	213.115.22.100	true
www.icesql.se	unknown	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/Ultralight-EV1-164B-Black.txt.deploy	true	• Avira URL Cloud: safe	unknown

http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Greek.txt.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Svenska.txt.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/ChameleonMiniGUI.exe.manifest	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/Chameleon-RevG.hex.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/MIfare-S20-320b.txt.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Be.Windows.Forms.HexBox.dll.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/German.txt.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/myfile.bin.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/avrdude.exe.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/BOOT_LOADER_EXE.exe.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/Chameleon-RevG.eep.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/English.txt.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/ChameleonMiniGUI.exe.config.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/chameleon.ico.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Dutch.txt.deploy	true	• Avira URL Cloud: safe	unknown
http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Chinese.txt.deploy	true	• Avira URL Cloud: safe	unknown

×

File Information

ID:	276434
Product:	CloudBasic
Start time:	05:21:04
Start date:	25.08.2020
Sample:	GUIControlSoftware-setup.exe
Cookbook:	default.jbs
System description:	w10x64 Windows 10 64 bit v1803 with Office Professional Plus 2016, IE 11, Adobe Reader DC 19, Java 8 Update 211
Architecture:	WINDOWS
MD5:	9dac98579289a7e0ffbad3fef093f279
SHA1:	76d0be23ecc12b0b649038f354ddd8a5ec54c63d
SHA256:	7281dd9d7080a70931272a1e576c80db1f802fa68cfa65f967cfc8a4b00467f8
Filetype:	Win32 Executable (generic) a (10002005/4) 99.96%

Close

×

Dropped Files

Name	Type	MD5	SHA1	SHA256
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\				

T3ZWOO1X.DKT\be.w..xbox_e0e5adf0ebc99863_0001.0006_none_3d4df2ccf20aaec3\Be.Windows.Forms.HexBox.dll	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows	A1828AC02274E73FD9CFC96FA04A92AF	E64591DBAA2[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\ChameleonMiniGUI.exe.config	XML 1.0 document, ASCII text, with CRLF line terminators	D6AA6083902DC2BCF05C083742F72C74	21BB23A5E428[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\BOOT_LOADER_EXE.exe	PE32 executable (console) Intel 80386, for MS Windows	9336F38067916D970B4811ED2D0AE7FD	D634F67D654C[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\Chameleon-RevG.eep	ASCII text, with CRLF line terminators	525CCBD0B903344411F9AEA50977A75A	70DCDCF574A[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\Chameleon-RevG.hex	ASCII text, with CRLF line terminators	1ACCA9233C8C2844135A54E45064D63A	F95D2B8F848D[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\avrdude.conf	ASCII text, with CRLF line terminators	5DC41B4E8644F5AA8634F2E9E8699593	E90ADB3DBE[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\avrdude.exe	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows	062882BCDE44E383ADE949BBCCE808C2	07987F77A9834[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\myfile.bin	data	C7DEDCBBE2AABCFED7559BA8CDD14B4A	81961C742A3F[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\myfilee.bin	data	FFA59126BB444788528E32899B70EE10	D6827EA28484[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Languages\Chinese.txt	UTF-8 Unicode text, with CRLF line terminators	8C08CB7A94CF1969105D8E1877752959	B388ECA1A001[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Languages\Dutch.txt	ASCII text, with CRLF line terminators	14954CE90FE4E4C5F7F6CBB847C785C0	C6674192BB32[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Languages\English.txt	ASCII text, with CRLF line terminators	81D2595D422B66B3F01565765A6475C9	0B640450F6E5[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\			

T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Languages\Fran ais.txt	UTF-8 Unicode text, with CRLF line terminators	E840AC6FF75BA4F6A83F13C4697A7DD8	D2FE422DFAC[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Languages\German.txt	UTF-8 Unicode text, with CRLF line terminators	BB198E5B6CB7CC7CD49E4CED130874E7	4CDCEB2BF4B[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Languages\Greek.txt	UTF-8 Unicode text, with CRLF line terminators	787F030B3346EA34B7CB39A2BAA2F58B	A2B5919A27CE[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Languages\Italiano.txt	UTF-8 Unicode text, with CRLF line terminators	1B70D196A83CFDDEAC03BEDB369A914E	CF4FBB112B69[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Languages\Spanish.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	5B4C2085AAB705EFBDC9FEE5F08A3193	5F1C4F4C0391[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Languages\Svenska.txt	UTF-8 Unicode text, with CRLF line terminators	E8E1B7E28910847B9BA5D4624D2CE784	5EAB9DDDAD[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Resources\chameleon.png	PNG image data, 522 x 304, 8-bit/color RGB, non-interlaced	DDEFB2513A3DF9AF6156EE4AF6B0F00C	915D1B57FB07[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Resources\warning.png	PNG image data, 96 x 96, 8-bit/color RGB, non-interlaced	6C60BB4AE39699E40FDB4D54301360C8	3F243036671A[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Templates\MIfare-S20-320b-Black.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	BF8B3BDF35CF7A121CF99FDDC7F5984C	3897C7A5BFDD[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Templates\MIfare-S20-320b.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	DAF6DCA785E4EC2358D4DE8936BB35BE	8AC23295F4E5[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Templates\MIfare-S50-1k-Black.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	CB06CB7F6AFEE00BCDBB1871492BE4F1	2BCD1BFD18E[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Templates\MIfare-S50-1k.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	C867AE3CE1A1C8BEB0C6AEF632F5F887	B90FF1006652[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...	ASCII text, with CRLF line terminators	2B5343AB1B756ABE287CFA1E846CFEBB	283ABEA7C55[illegible]

exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Templates\Ultralight-EV1-164B-Black.txt			
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Templates\Ultralight-EV1-164B.txt	ASCII text, with CRLF line terminators	E07A188DCEC33688E5478AAFF6100DDE	76F19D18DB50[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Templates\iClass-Black.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	EC0A9552E214746B80EEB3F3A83E4D42	D93D7FD7D47[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\chameleon.ico	MS Windows icon resource - 5 icons, 16x16, 32 bits/pixel, 24x24, 32 bits/pixel	A8CDC41DEE0A3B0276A86967740CEC1C	FA3CA885022[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.cdf-ms	data	AAEA6A7C069FB6F82A3BAD1FC7701538	D19F4E83461[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows	C1DC94E08FA2F6B430A2A9D4D961FB4E	DCF737BAA7A[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe:Zone.Identifier	ASCII text, with CRLF line terminators	FBCCF14D504B7B2DBCB5A5BDA75BD93B	D59FC84CDD5[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.manifest	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	CC034830423CE35192F00FEE372261A0	D5929807119F0[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\Crapto1Sharp.cdf-ms	data	0782F8861969D9ED9F8D0DC3DE2F911B	4B6CE55348E4[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\Crapto1Sharp.dll	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows	C8903D18A45AB817D572B6B2CF426084	E60C20EF3EA6[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\Crapto1Sharp.manifest	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	3918271C7C34CA2633C8A254BE7A20E4	0BA1A92B5C1[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\DynamicExpresso.Core.cdf-ms	data	FBB0176395DAEAA621EEEA12661E62AC	4D44899ED0C1[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows	8634D7E93D203B7DF8DBFCC450A30819	50830F589277[illegible]

_dd81ee9d302ebe52\DynamicExpresso.Core.dll			
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\DynamicExpresso.Core.manifest	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	684219693C94A1E7C4E0D2ED8B045C13	CCB3268DB14[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\manifests\be.w..xbox_e0e5adf0ebc99863_0001.0006_none_3d4df2ccf20aaec3.cdf-ms	data	1ECFE58E0563C189160E5787CB740A31	1342ADD4E07[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\manifests\be.w..xbox_e0e5adf0ebc99863_0001.0006_none_3d4df2ccf20aaec3.manifest	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	7D86B5B24B40036A94527B9C4DB07BF4	77973B241BAB[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\manifests\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5.cdf-ms	data	57F209E567265A7AC27A3460C3A27A58	158DE1E29E05[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\manifests\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5.manifest	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, LF line terminators	C5DB6210746FAEE129505FD337E5E319	C4F582E11D61[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\manifests\cham..tion_0000000000000000_0001.0003_none_d5701622488d1f04.cdf-ms	data	2F1F964CD68E0476AC6556E81DF90420	23B6A2F509D[illegible]
C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\manifests\cham..tion_0000000000000000_0001.0003_none_d5701622488d1f04.manifest	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	99CE18B2332A388939C09CA7BE98D1D8	C97CFB611DF[illegible]
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\SD6J871E.log	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators	EDF9A3CE348F8CD269E4752B3F87D7E2	A794596D4C06[illegible]
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ChameleonMiniGUI[1].application	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	2E7D695479ACDA3AA1AE3F62A291C0D2	30E2B6A87570[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\2AM6TJA6.K8O\MRBMTQ3K.1Y7.application	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	99CE18B2332A388939C09CA7BE98D1D8	C97CFB611DF[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Be.Windows.Forms.HexBox.dll	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows	A1828AC02274E73FD9CFC96FA04A92AF	E64591DBAA2[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Be.Windows.Forms.HexBox.dll.genman	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	7D86B5B24B40036A94527B9C4DB07BF4	77973B241BAB[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\ChameleonMiniGUI.exe	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows	C1DC94E08FA2F6B430A2A9D4D961FB4E	DCF737BAA7A[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\ChameleonMiniGUI.exe.config	XML 1.0 document, ASCII text, with CRLF line terminators	D6AA6083902DC2BCF05C083742F72C74	21BB23A5E428[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\ChameleonMiniGUI.exe.genman	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	CC034830423CE35192F00FEE372261A0	D5929807119F0[illegible]
C:\Users\user\AppData\Local\Te			

mp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\ChameleonMiniGUI.exe.manifest	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, LF line terminators	C5DB6210746FAEE129505FD337E5E319	C4F582E11D61 [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\ChameleonMiniGUI.exe:Zone.Identifier	ASCII text, with CRLF line terminators	FBCCF14D504B7B2DBCB5A5BDA75BD93B	D59FC84CDD5 [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Crapto1Sharp.dll	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows	C8903D18A45AB817D572B6B2CF426084	E60C20EF3EA [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Crapto1Sharp.dll.genman	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	3918271C7C34CA2633C8A254BE7A20E4	0BA1A92B5C1 [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\DynamicExpresso.Core.dll	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows	8634D7E93D203B7DF8DBFCC450A30819	50830F589277 [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\DynamicExpresso.Core.dll.genman	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	684219693C94A1E7C4E0D2ED8B045C13	CCB3268DB14 [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\BOOT_LOADER_EXE.exe	PE32 executable (console) Intel 80386, for MS Windows	9336F38067916D970B4811ED2D0AE7FD	D634F67D654C [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\Chameleon-RevG.eep	ASCII text, with CRLF line terminators	525CCBD0B903344411F9AEA50977A75A	70DCDCF574A [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\Chameleon-RevG.hex	ASCII text, with CRLF line terminators	1ACCA9233C8C2844135A54E45064D63A	F95D2B8F848D [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\avrdude.conf	ASCII text, with CRLF line terminators	5DC41B4E8644F5AA8634F2E9E8699593	E90ADB3DBE [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\avrdude.exe	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows	062882BCDE44E383ADE949BBCCE808C2	07987F77A9834 [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\myfile.bin	data	C7DEDCBBE2AABCFED7559BA8CDD14B4A	81961C742A3F [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\myfilee.bin	data	FFA59126BB444788528E32899B70EE10	D6827EA28484 [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Languages\Chinese.txt	UTF-8 Unicode text, with CRLF line terminators	8C08CB7A94CF1969105D8E1877752959	B388ECA1A001 [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Languages\Dutch.txt	ASCII text, with CRLF line terminators	14954CE90FE4E4C5F7F6CBB847C785C0	C6674192BB32 [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Languages\English.txt	ASCII text, with CRLF line terminators	81D2595D422B66B3F01565765A6475C9	0B640450F6E5 [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Languages\Fran ais.txt	UTF-8 Unicode text, with CRLF line terminators	E840AC6FF75BA4F6A83F13C4697A7DD8	D2FE422DFAC [illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Languages\German.txt	UTF-8 Unicode text, with CRLF line terminators	BB198E5B6CB7CC7CD49E4CED130874E7	4CDCEB2BF4B [illegible]

C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Languages\Greek.txt	UTF-8 Unicode text, with CRLF line terminators	787F030B3346EA34B7CB39A2BAA2F58B	A2B5919A27C[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Languages\Italiano.txt	UTF-8 Unicode text, with CRLF line terminators	1B70D196A83CFDDEAC03BEDB369A914E	CF4FBB112B69[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Languages\Spanish.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	5B4C2085AAB705EFBDC9FEE5F08A3193	5F1C4F4C0391[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Languages\Svenska.txt	UTF-8 Unicode text, with CRLF line terminators	E8E1B7E28910847B9BA5D4624D2CE784	5EAB9DDDAD[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Resources\chameleon.png	PNG image data, 522 x 304, 8-bit/color RGB, non-interlaced	DDEFB2513A3DF9AF6156EE4AF6B0F00C	915D1B57FB07[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Resources\warning.png	PNG image data, 96 x 96, 8-bit/color RGB, non-interlaced	6C60BB4AE39699E40FDB4D54301360C8	3F243036671A[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Templates\MIfare-S20-320b-Black.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	BF8B3BDF35CF7A121CF99FDDC7F5984C	3897C7A5BFD[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Templates\MIfare-S20-320b.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	DAF6DCA785E4EC2358D4DE8936BB35BE	8AC23295F4E5[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Templates\MIfare-S50-1k-Black.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	CB06CB7F6AFEE00BCDBB1871492BE4F1	2BCD1BFD18E[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Templates\MIfare-S50-1k.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	C867AE3CE1A1C8BEB0C6AEF632F5F887	B90FF1006652[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Templates\Ultralight-EV1-164B-Black.txt	ASCII text, with CRLF line terminators	2B5343AB1B756ABE287CFA1E846CFEBB	283ABEA7C55[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Templates\Ultralight-EV1-164B.txt	ASCII text, with CRLF line terminators	E07A188DCEC33688E5478AAFF6100DDE	76F19D18DB50[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Templates\iClass-Black.txt	UTF-8 Unicode (with BOM) text, with CRLF line terminators	EC0A9552E214746B80EEB3F3A83E4D42	D93D7FD7D47[illegible]
C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\chameleon.ico	MS Windows icon resource - 5 icons, 16x16, 32 bits/pixel, 24x24, 32 bits/pixel	A8CDC41DEE0A3B0276A86967740CEC1C	FA3CA885022[illegible]
C:\Users\user\AppData\Local\Temp\VSD97F8.tmp\install.log	data	C3A465B809F84B5EB804E8C0284E0F4F	7CD41F2B0BB[illegible]
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Christian Herrmann\The rebooted suite\Chameleon Mini Rebooted GUI online support.url	MS Windows 95 Internet shortcut text (URL= <https://github.com/iceman1001/ChameleonMini-rebootedGUI/issues>), ASCII text, with CRLF line terminators	7B84738C6B90D709EA15859C70D959D5	D526983D1C12[illegible]
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Christian Herrmann\The rebooted suite\Chameleon Mini Rebooted GUI.appref-ms	Little-endian UTF-16 Unicode text, with no line terminators	B4E81C9C589737581DB2BD8ACBBAA5DE	0690F63EB572[illegible]
C:\Users\user\Desktop\Chameleon Mini Rebooted GUI.appref-ms	Little-endian UTF-16 Unicode text, with no line terminators	B4E81C9C589737581DB2BD8ACBBAA5DE	0690F63EB572[illegible]

Close

×

Signature Information

Show All Signature Results

Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BA3DDD __EH_prolog3_GS,char_traits,char_traits,FindFirstFileW,char_traits,FindNextFileW,FindClose,FindClose,	0_2_00BA3DDD
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\AppData\Local\Apps\2.0\	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\AppData\Local\	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\AppData\Local\Apps\	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\AppData\	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\	Jump to behavior

Networking:

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

Source: Traffic	Snort IDS: 2067 WEB-MISC Lotus Notes .exe script source download attempt 192.168.2.4:49698 -> 213.115.22.100:80
Source: global traffic	HTTP traffic detected: HTTP/1.1 200 OKContent-Type: application/octet-streamLast-Modified: Tue, 19 May 2020 19:12:48 GMTAccept-Ranges: bytesETag: "b8b7b7c112ed61:0"Server: Microsoft-IIS/7.5X-Powered-By: ASP.NETDate: Tue, 25 Aug 2020 03:22:11 GMTContent-Length: 465422Data Raw: 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 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 08 00 f0 55 07 00 00 1a 07 00 00 00 00 00 e0 00 0f 03 0b 01 02 18 00 9c 04 00 00 16 07 00 00 1e 00 00 70 15 00 00 00 10 00 00 00 b0 04 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 90 07 00 00 04 00 00 6b a3 07 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 50 07 00 6c 11 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 00 00 00 00 00 00 00 00 00 00 00 00 00 04 80 07 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 34 53 07 00 94 02 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 2e 74 65 78 74 00 00 00 40 9a 04 00 00 10 00 00 00 9c 04 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 2e 64 61 74 61 00 00 00 b8 02 00 00 00 b0 04 00 00 04 00 00 00 a0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 c0 2e 72 64 61 74 61 00 00 ec ab 01 00 00 c0 04 00 00 ac 01 00 00 a4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 40 2f 34 00 00 00 00 00 00 d0 b3 00 00 00 70 06 00 00 b4 00 00 00 50 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 62 73 73 00 00 00 00 a8 1d 00 00 00 30 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 60 c0 2e 69 64 61 74 61 00 00 6c 11 00 00 00 50 07 00 00 12 00 00 00 04 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 18 00 00 00 00 70 07 00 00 02 00 00 00 16 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00 00 00 20 00 00 00 00 80 07 00 00 02 00 00 00 18 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 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 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 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 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 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 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 0
Source: global traffic	HTTP traffic detected: HTTP/1.1 200 OKContent-Type: application/octet-streamLast-Modified: Tue, 19 May 2020 19:12:48 GMTAccept-Ranges: bytesETag: "e4794e7c112ed61:0"Server: Microsoft-IIS/7.5X-Powered-By: ASP.NETDate: Tue, 25 Aug 2020 03:22:12 GMTContent-Length: 62464Data Raw: 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 f8 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 0f f1 b4 58 4b 90 da 0b 4b 90 da 0b 4b 90 da 0b 0d c1 07 0b 49 90 da 0b 0d c1 05 0b 49 90 da 0b 0d c1 3a 0b 58 90 da 0b 0d c1 3b 0b 49 90 da 0b 96 6f 11 0b 49 90 da 0b 6c 56 a1 0b 48 90 da 0b 4b 90 db 0b 0f 90 da 0b 46 c2 3e 0b 43 90 da 0b 46 c2 01 0b 4a 90 da 0b 46 c2 04 0b 4a 90 da 0b 52 69 63 68 4b 90 da 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0f 89 54 59 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0c 00 00 7e 00 00 00 7e 00 00 00 00 00 00 69 88 00 00 00 10 00 00 00 90 00 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 20 01 00 00 04 00 00 00 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 94 d6 00 00 50 00 00 00 00 00 01 00 e0 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 d4 0e 00 00 40 91 00 00 38 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 60 d5 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 90 00 00 1c 01 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 2e 74 65 78 74 00 00 00 00 7d 00 00 00 10 00 00 00 7e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 2a 4c 00 00 00 90 00 00 00 4e 00 00 00 82 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 40 1c 00 00 00 e0 00 00 00 12 00 00 00 d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 e0 01 00 00 00 00 01 00 00 02 00 00 00 e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 d4 0e 00 00 00 10 01 00 00 10 00 00 00 e4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
	HTTP traffic detected: HTTP/1.1 200 OKContent-Type: application/octet-streamLast-Modified: Tue, 19 May 2020 19:12:41 GMTAccept-Ranges: bytesETag: "9a6cf777112ed61:0"Server: Microsoft-IIS/7.5X-Powered-By: ASP.NETDate: Tue, 25 Aug 2020 03:22:12 GMTContent-Length: 90112Data Raw: 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 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 03 00 39 a9 67 5e 00 00 00 00 00 00 00 00 e0 00 22 20 0b 01 30 00 00 30 01 00 00 20 00 00 00 00 00 00 ca 43 01 00 00 20 00 00 00 60 01 00 00 00 00 11 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 a0 01 00 00 10 00 00 40 3e 02 00 03 00 60 85 00 00

Source: global traffic	10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 78 43 01 00 4f 00 00 00 00 60 01 00 1c 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 01 00 0c 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 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d0 23 01 00 00 20 00 00 00 30 01 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 1c 04 00 00 00 60 01 00 00 10 00 00 00 40 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 01 00 00 10 00 00 00 50 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
Source: global traffic	HTTP traffic detected: HTTP/1.1 200 OKContent-Type: application/octet-streamLast-Modified: Tue, 19 May 2020 19:12:44 GMTAccept-Ranges: bytesETag: "fb43f379112ed61:0"Server: Microsoft-IIS/7.5X-Powered-By: ASP.NETDate: Tue, 25 Aug 2020 03:22:13 GMTContent-Length: 16896Data Raw: 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 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 03 00 76 b8 a2 94 00 00 00 00 00 00 00 00 e0 00 22 20 0b 01 30 00 00 3a 00 00 00 06 00 00 00 00 00 00 da 56 00 00 00 20 00 00 00 60 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 a0 00 00 00 02 00 00 00 00 00 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 85 56 00 00 4f 00 00 00 00 60 00 00 9c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 0c 00 00 00 80 55 00 00 54 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 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 a0 39 00 00 00 20 00 00 00 3a 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 9c 03 00 00 00 60 00 00 00 04 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 00 00 00 02 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b9 56 00 00 00 00 00 00 48 00 00 00 02 00 05 00 78 36 00 00 08 1f 00 00 01 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 00 00 00 00 00 00 00 00 1e 02 28 10 00 00 0a 2a 1e 02 28 10 00 00 0a 2a 1e 02 28 10 00 00 0a 2a 1e 02 28 15 00 00 06 2a 22 02 03 28 16 00 00 06 2a 22 02 03 28 17 00 00 06 2a 00 00 13 30 05 00 ca 00 00 00 01 00 00 11 02 7c 0a 00 00 04 25 28 23 00 00 06 20 ff ff ff 00 5f 28 24 00 00 06 02 7c 0a 00 00 04 28 23 00 00 06 0c 02 7c 0a 00 00 04 02 7c 0a 00 00 04 28 25 00 00 06 28 24 00 00 06 02 7c 0a 00 00 04 08 28 26 00 00 06 02 7c 0a 00 00 04 28 25 00 00 06 17 5f 0a 06 20 04 08 87 00 02 7c 0a 00 00 04 25 28 25 00 00 06 17 64 25 0d 28 26 00 00 06 09 5f 61 0a 06 20 5c ce 29 00 02 7c 0a 00 00 04 28 23 00 00 06 5f 61 0a 06 03 2d 03 16 2b 01 17 61 0a 06 02 7c 0a 00 00 04 28 23 00 00 06 28 1d 00 00 06 25 0b 04 2d 03 16 2b 01 17 5f 61 0a 02 7c 0a 00 00 04 25 28 25 00 00 06 06 28 20 00 00 06 1f 17 62 60 28 26 00 00 06 07 2a 00 00 13 30 04 00 28 00 00 00 02 00 00 11 16 0a 1d 0b 2b 1c 06 02 03 07 28 3e 00 00 06 04 28 07 00 00 06 07 1f 1f 5f 62 d2 60 d2 0a 07 17 59 0b 07 16 2f e
Source: global traffic	HTTP traffic detected: HTTP/1.1 200 OKContent-Type: application/octet-streamLast-Modified: Tue, 19 May 2020 19:12:45 GMTAccept-Ranges: bytesETag: "276367a112ed61:0"Server: Microsoft-IIS/7.5X-Powered-By: ASP.NETDate: Tue, 25 Aug 2020 03:22:13 GMTContent-Length: 61952Data Raw: 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 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 03 00 68 b8 f9 a0 00 00 00 00 00 00 00 00 e0 00 22 20 0b 01 30 00 00 e8 00 00 00 08 00 00 00 00 00 00 d6 06 01 00 00 20 00 00 00 20 01 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 01 00 00 02 00 00 00 00 00 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 82 06 01 00 4f 00 00 00 00 20 01 00 04 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 01 00 0c 00 00 00 e4 05 01 00 38 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 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 dc e6 00 00 00 20 00 00 00 e8 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 04 04 00 00 00 20 01 00 00 06 00 00 00 ea 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 01 00 00 02 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b6 06 01 00 00 00 00 00 48 00 00 00 02 00 05 00 f8 68 00 00 0c 8f 00 00 01 00 00 00 00 00 00 00 04 f8 00 00 e0 0d 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 00 00 00 1e 02 7b 1f 00 00 0a 2a 1e 02 7b 20 00 00 0a 2a 56 02 28 21 00 00 0a 02 03 7d 1f 00 00 0a 02 04 7d 20 00 00 0a 2a 00 00 13 30 03 00 3b 00 00 00 01 00 00 11 03 75 03 00 00 1b 0a 06 2c 2f 28 22 00 00 0a 02 7b 1f 00 00 0a 06 7b 1f 00 00 0a 6f 23 00 00 0a 2c 17 28 24 00 00 0a 02 7b 20 00 00 0a 06 7b 20 00 00 0a 6f 25 00 00 0a 2a 16 2a d2 20 91 31 ad 45 20 29 55 55 a5 5a 28 22 00 00 0a 02 7b 1f 00 00 0a 6f 26 00 00 0a 58 20 29 55 55 a5 5a 28 24 00 00 0a 02 7b 20 00 00 0a 6f 27 00 00 0a 58 2a 13 30 07 00 88 00 00 00 02 00 00 11 14 72 01 00 00 70 18 8d 0f 00 00 01 25 16 02 7b 1f 00 00 0a 0a 12 00 12 01 fe 15 06 00 00 1b 07 8c 06 00 00 1b 2d 14 71 06 00 00 1b 0b 12 01 07 8c 06 00 00 1b 2d 04 26 14 2b 0b fe 16 06 00 00 1b 6f 28 00 00 0a a2 25 17 02 7b 20 00 00 0a 0c 12 02 12 03 fe 15 07 00 00 1b 09 8c 07 00 00 1b 2d 14 71 07 00 00 1b 0d 12 03 09 8c 07 00 00 1b 2d 04 26 14 2b 0b fe 16 07 00 00 1b 6f 28 00 00 0a a2 28 29 00 00 0a 2a 3a 02 28 21 00 00
Source: global traffic	HTTP traffic detected: HTTP/1.1 200 OKContent-Type: application/octet-streamLast-Modified: Tue, 19 May 2020 19:12:44 GMTAccept-Ranges: bytesETag: "74ab7979112ed61:0"Server: Microsoft-IIS/7.5X-Powered-By: ASP.NETDate: Tue, 25 Aug 2020 03:22:13 GMTContent-Length: 1361920Data Raw: 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 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 03 00 4a 2f c4 5e 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 60 14 00 00 66 00 00 00 00 00 00 e2 7e 14 00 00 20 00 00 00 80 14 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 15 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 90 7e 14 00 4f 00 00 00 00 80 14 00 c4 63 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 15 00 0c 00 00 00 58 7d 14 00 1c 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 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 e8 5e 14 00 00 20 00 00 00 60 14 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 c4 63 00 00 00 80 14 00 00 64 00 00 00 62 14 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 15 00 00 02 00 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c4 7e 14 00 00 00 00 00 48 00 00 00 02 00 05 00 2c 94 01 00 f4 4a 01 00 03 00 00 00 dc 00 00 06 20 df 02 00 38 9e 11 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 00 00 1e 02 7b 1e 00 00 0a 2a 1e 02 7b 1f 00 00 0a 2a 1e 02 7b 20 00 00 0a 2a 1e 02 7b 21 00 00 0a 2a 92 02 28 22 00 00 0a 02 03 7d 1e 00 00 0a 02 04 7d 1f 00 00 0a 02 05 7d 20 00 00 0a 02 0e 04 7d 21 00 00 0a 2a 00 00 00 13 30 03 00 6b 00 00 00 01 00 00 11 03 75 02 00 00 1b 0a 06 2c 5f 28 23 00 00 0a 02 7b 1e 00 00 0a 06 7b 1e 00 00 0a 6f 24 00 00 0a 2c 47 28 25 00 00 0a 02 7b 1f 00 00 0a 06 7b 1f 00 00 0a 6f 26 00 00 0a 2c 2f 28 27 00 00 0a 02 7b 20 00 00 0a 06 7b 20 00 00 0a 6f 28 00 00 0a 2c 17 28 29 00 00 0a 02 7b 21 00 00 0a 06 7b 21 00 00 0a 6f 2a 00 00 0a 2a 16 2a 00 13 30 03 00 62 00 00 00 00 00 00 00 20 ec ce 3c e0 20 29 55 55 a5 5a 28 23 00 00 0a 02 7b 1e 00 00 0a 6f 2b 00 00 0a 58 20 29 55 55 a5 5a 28 25 00 00 0a 02 7b 1f 00 00 0a 6f 2c 00 00 0a 58 20 29 55 55 a5 5a 28 27 00 00 0a 02 7b 20 00 00 0a 6f 2d 00 00 0a 58 20 29 55 55 a5 5a 28 29 00 00 0a 02 7b 21 00 00 0a 6f 2e 00 00 0a 58 2a 00 00 13 30 07 00 06 01 00 00 02 00 00 11 14
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/ChameleonMiniGUI.application HTTP/1.1Host: www.icesql.seAccept-Encoding: gzipConnection: Keep-Alive
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/ChameleonMiniGUI.exe.manifest HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip

Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/chameleon.ico.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Resources/chameleon.png.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/Chameleon-RevG.hex.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/Chameleon-RevG.eep.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/Ultralight-EV1-164B-Black.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/English.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/MIfare-S20-320b.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Fran%C3%A7ais.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/myfile.bin.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/German.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Spanish.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/myfilee.bin.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Dutch.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/iClass-Black.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/avrdude.exe.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Chinese.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/ChameleonMiniGUI.exe.config.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/MIfare-S50-1k.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Greek.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Resources/warning.png.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/avrdude.conf.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/BOOT_LOADER_EXE.exe.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/MIfare-S20-320b-Black.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/MIfare-S50-1k-Black.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Svenska.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/Ultralight-EV1-164B.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Italiano.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Be.Windows.Forms.HexBox.dll.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Crapto1Sharp.dll.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/DynamicExpresso.Core.dll.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/ChameleonMiniGUI.exe.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip	
Source: Joe Sandbox View	ASN Name: TELENOR-NEXTELTelenorNorgeASNO TELENOR-NEXTELTelenorNorgeASNO	
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/ChameleonMiniGUI.application HTTP/1.1Accept: */*Accept-Encoding: gzip, deflateUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)Host: www.icesql.seConnection: Keep-Alive	
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BB0899 __EH_prolog3_GS,URLDownloadToCacheFileW,	0_2_00BB0899

Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/ChameleonMiniGUI.application HTTP/1.1Accept: */*Accept-Encoding: gzip, deflateUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)Host: www.icesql.seConnection: Keep-Alive
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/ChameleonMiniGUI.application HTTP/1.1Host: www.icesql.seAccept-Encoding: gzipConnection: Keep-Alive
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/ChameleonMiniGUI.exe.manifest HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/chameleon.ico.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Resources/chameleon.png.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/Chameleon-RevG.hex.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/Chameleon-RevG.eep.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/Ultralight-EV1-164B-Black.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/English.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/MIfare-S20-320b.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Fran%C3%A7ais.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/myfile.bin.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/German.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Spanish.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/myfilee.bin.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Dutch.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/iClass-Black.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/avrdude.exe.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Chinese.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/ChameleonMiniGUI.exe.config.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/MIfare-S50-1k.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Greek.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Resources/warning.png.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/avrdude.conf.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/BOOT_LOADER_EXE.exe.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/MIfare-S20-320b-Black.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/MIfare-S50-1k-Black.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Svenska.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Templates/Ultralight-EV1-164B.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Languages/Italiano.txt.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Be.Windows.Forms.HexBox.dll.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Crapto1Sharp.dll.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/DynamicExpresso.Core.dll.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip

Source: global traffic	HTTP traffic detected: GET /download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/ChameleonMiniGUI.exe.deploy HTTP/1.1Host: www.icesql.seAccept-Encoding: gzip
Source: unknown	DNS traffic detected: queries for: www.icesql.se
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://akizukidenshi.com/catalog/g/gP-07487/
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://akizukidenshi.com/download/ds/akizuki/k6096_manual_20130816.pdf
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://armwerks.com/catalog/o-link-debugger-copy/
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://dangerousprototypes.com/docs/FT2232_breakout_board
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://electropol.free.fr/spip/spip.php?article27)
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://elk.informatik.fh-augsburg.de/hhweb/doc/openocd/usbjtag/usbjtag.html
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://flashrom.org/FT2232SPI_Programmer
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://fontfabrik.com
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://forum.mikrokopter.de/topic-post48317.html
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://item.taobao.com/item.htm?id=1559277013
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://micro-research.co.th/
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://nightshade.homeip.net/
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://real.kiev.ua/old/avreal/en/adapters
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.exe0.1.dr	String found in binary or memory: http://savannah.nongnu.org/projects/avrdude/
Source: dfsvc.exe, 00000001.00000002.1028398749.00000218128D8000.00000004.00000001.sdmp	String found in binary or memory: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Source: avrdude.exe0.1.dr	String found in binary or memory: http://sourceware.org/pthreads-win32/.
Source: dfsvc.exe, 00000001.00000003.243087684.000002182E4B7000.00000004.00000001.sdmp	String found in binary or memory: http://wJ3.org/2000/0Kldsig#sha256P
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://wiki.openmoko.org/wiki/Debug_Board_v3
Source: avrdude.exe0.1.dr, avrdude.conf.1.dr	String found in binary or memory: http://wiring.org.co/
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.100ask.net/shop/english.html
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.amontec.com/jtagkey.shtml
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.andahammer.com/olink/
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.apache.org/licenses/LICENSE-2.0
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.000	String found in binary or memory: http://www.atmel.com/dyn/products/tools_card.asp?tool_id=2877

00004.00000001.sdmp, avrdude.conf.1.dr	
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.atmel.com/dyn/resources/prod_documents/doc1280.pdf
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.atmel.com/dyn/resources/prod_documents/doc2525.pdf
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.atmel.com/images/doc2562.pdf
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.exe0.1.dr	String found in binary or memory: http://www.bdmicro.com/
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.bitwizard.nl/wiki/index.php/FTDI_ATmega
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.bsdhome.com/avrdude/
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.carterandcone.coml
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.cs.put.poznan.pl/wswitala/download/pdf/811EVBK.pdf
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.developmentboard.net/31-o-link-debugger.html
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.ere.co.th/download/sch050713.pdf
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.ethernut.de/en/hardware/turtelizer/index.html
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.exe0.1.dr, avrdude.conf.1.dr	String found in binary or memory: http://www.fischl.de/usbasp/
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.fontbureau.com
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.fontbureau.com/designers
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.fontbureau.com/designers/?
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.fontbureau.com/designers/cabarga.htmlN
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.fontbureau.com/designers/frere-user.html
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.fontbureau.com/designers8
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.fontbureau.com/designers?
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.fontbureau.com/designersG
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.fonts.com
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.founder.com.cn/cn
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.founder.com.cn/cn/bThe

Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.founder.com.cn/cn/cThe
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.ftdichip.com/Products/Cables/USBTTLSerial.htm
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.ftdichip.com/Products/Modules/DLPModules.htm
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.ftdichip.com/Support/Documents/DataSheets/Cables/DS_TTL-232R_CABLES.pdf
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.galapagosdesign.com/DPlease
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.galapagosdesign.com/staff/dennis.htm
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.geocities.jp/arduino_diecimila/bootloader/index_en.html
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.goodfont.co.kr
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se
Source: dfsvc.exe, 00000001.00000002.1037350923.000002182B190000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Be.Windo
Source: dfsvc.exe, 00000001.00000002.1030977541.0000021812A1F000.00000004.00000001.sdmp, SD6J871E.log.1.dr	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Chameleo
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Crapto1S
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/DynamicE
Source: dfsvc.exe, 00000001.00000003.268431882.000002182E50B000.00000004.00000001.sdmp, dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/B
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/C
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, dfsvc.exe, 00000001.00000002.1037350923.000002182B190000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/a
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Extras/m
Source: dfsvc.exe, 00000001.00000002.1037350923.000002182B190000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Language
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, dfsvc.exe, 00000001.00000002.1037350923.000002182B190000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Resource
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/Template
Source: dfsvc.exe, 00000001.00000003.268431882.000002182E50B000.0000	

0004.00000001.sdmp, dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/Application%20Files/ChameleonMiniGUI_1_3_0_3/chameleo
Source: SD6J871E.log.1.dr, cham..tion_0000000000000000_0001.0003_none_d5701622488d1f04.cdf-ms.1.dr	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application
Source: ChameleonMiniGUI.exe, 00000005.00000002.1028693427.0000000001310000.00000004.00000040.sdmp, ChameleonMiniGUI.exe, 00000005.00000002.1025668721.0000000000F80000.00000004.00000020.sdmp, ChameleonMiniGUI.exe, 00000005.00000002.1032168511.0000000002EE1000.00000004.00000001.sdmp, ChameleonMiniGUI.exe, 00000005.00000002.1031187239.0000000001570000.00000004.00000040.sdmp, Chameleon Mini Rebooted GUI.appref-ms.1.dr, SD6J871E.log.1.dr	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application#ChameleonMiniGUI.applica
Source: ChameleonMiniGUI.exe, 00000005.00000002.1027571659.0000000001165000.00000004.00000020.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application%
Source: dfsvc.exe, 00000001.00000003.265856105.000002182B1E6000.00000004.00000001.sdmp, ChameleonMiniGUI.exe, 00000005.00000003.281899189.0000000001165000.00000004.00000001.sdmp, cham..tion_0000000000000000_0001.0003_none_d5701622488d1f04.cdf-ms.1.dr	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application%1.2.1.0%
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application)
Source: dfsvc.exe, 00000001.00000003.268694040.000002182E56B000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application.0
Source: ChameleonMiniGUI.exe, 00000005.00000002.1027571659.0000000001165000.00000004.00000020.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application02
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application089
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application0897
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application089MSILg
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application089R
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application089z
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application1
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application89
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application899
Source: dfsvc.exe, 00000001.00000002.1037350923.000002182B190000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.application;z
Source: dfsvc.exe, 00000001.00000002.1030977541.0000021812A1F000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationDefa
Source: dfsvc.exe, 00000001.00000003.270135663.000002182B1DD000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationE
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.0000	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationH

0004.00000001.sdmp	
Source: dfsvc.exe, 00000001.00000002.1037350923.000002182B190000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationM
Source: dfsvc.exe, 00000001.00000003.270135663.000002182B1DD000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationX
Source: dfsvc.exe, 00000001.00000002.1035940141.00000218130AE000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationp
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationre=MSILV
Source: dfsvc.exe, 00000001.00000003.270135663.000002182B1DD000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationsK
Source: ChameleonMiniGUI.exe, 00000005.00000002.1027571659.0000000001165000.00000004.00000020.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationt
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationts
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationts9
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationtsas
Source: dfsvc.exe, 00000001.00000003.270324353.000002182E4F4000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationtsl
Source: dfsvc.exe, 00000001.00000002.1037350923.000002182B190000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationwz
Source: ChameleonMiniGUI.exe, 00000005.00000002.1027420345.000000000112F000.00000004.00000020.sdmp	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/ChameleonMiniGUI.applicationy
Source: GUIControlSoftware-setup.exe	String found in binary or memory: http://www.icesql.se/download/ChameleonMiniGUI/TruePAhttps://github.com/iceman1001/ChameleonMini-reb
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp	String found in binary or memory: http://www.icesql.se8
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.jiyu-kobo.co.jp/
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.ladyada.net/make/usbtinyisp/
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.lancos.com/siprogsch.html
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.micro4you.com/store/openjtag-arm-jtag-usb.html
Source: dfsvc.exe, 00000001.00000003.234661363.000002182B31F000.00000004.00000001.sdmp	String found in binary or memory: http://www.monotype.
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.olimex.com/dev/arm-usb-ocd.html
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.openjtag.org
Source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, avrdude.conf.1.dr	String found in binary or memory: http://www.picoweb.net/
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.sajatypeworks.com
Source: dfsvc.exe, 00000001.00000003.228441705.000002182B313000.0000	String found in binary or memory: http://www.sajatypeworks.com/

0004.00000001.sdmp		
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.sakkal.com	
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.sandoll.co.kr	
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.tiro.com	
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.typography.netD	
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.urwpp.deDPlease	
Source: dfsvc.exe, 00000001.00000003.242776161.000002182E4CB000.00000004.00000001.sdmp	String found in binary or memory: http://www.w3.or	
Source: ChameleonMiniGUI.exe, 00000005.00000003.307628889.000000000614B000.00000004.00000001.sdmp	String found in binary or memory: http://www.w3.orfZm	
Source: dfsvc.exe, 00000001.00000002.1028707947.0000021812926000.00000004.00000001.sdmp	String found in binary or memory: http://www.xrml.org/schema/2001/11/xrml2core	
Source: dfsvc.exe, 00000001.00000002.1028707947.0000021812926000.00000004.00000001.sdmp	String found in binary or memory: http://www.xrml.org/schema/2001/11/xrml2core2	
Source: ChameleonMiniGUI.exe, 00000005.00000002.1040841321.0000000006710000.00000002.00000001.sdmp	String found in binary or memory: http://www.zhongyicts.com.cn	
Source: dfsvc.exe, 00000001.00000002.1035513981.0000021812F64000.00000004.00000001.sdmp, ChameleonMiniGUI.exe, ChameleonMiniGUI.exe0.1.dr	String found in binary or memory: https://github.com/iceman1001/ChameleonMini-rebooted/wiki/Terminal-Commands	
Source: Chameleon Mini Rebooted GUI online support.url.1.dr	String found in binary or memory: https://github.com/iceman1001/ChameleonMini-rebootedGUI/issues	
Source: cham..tion_0000000000000000_0001.0003_none_d5701622488d1f04.cdf-ms.1.dr	String found in binary or memory: https://github.com/iceman1001/ChameleonMini-rebootedGUI/issues%%The	
Source: dfsvc.exe, 00000001.00000002.1030977541.0000021812A1F000.00000004.00000001.sdmp	String found in binary or memory: https://github.com/iceman1001/ChameleonMini-rebootedGUI/issues0y=1	
Source: dfsvc.exe, 00000001.00000002.1035513981.0000021812F64000.00000004.00000001.sdmp, ChameleonMiniGUI.exe, ChameleonMiniGUI.exe0.1.dr	String found in binary or memory: https://rawgit.com/emsec/ChameleonMini/master/Doc/Doxygen/html/_page__command_line.html	
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BCB86D	0_2_00BCB86D
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BD3866	0_2_00BD3866
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BD9840	0_2_00BD9840
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BD9CF0	0_2_00BD9CF0
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BC5C16	0_2_00BC5C16
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BCB63E	0_2_00BCB63E
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Code function: 5_2_00978AD5	5_2_00978AD5
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Code function: 5_2_00976748	5_2_00976748
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.D		

KT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Code function: 5_2_0130CBF4	5_2_0130CBF4
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Code function: 5_2_0130EBD0	5_2_0130EBD0
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Code function: 5_2_0130EBC0	5_2_0130EBC0
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Code function: 5_2_00977871	5_2_00977871
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: String function: 00BA07B1 appears 31 times	
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: String function: 00BC3180 appears 58 times	
Source: GUIControlSoftware-setup.exe	Static PE information: Resource name: RT_ICON type: GLS_BINARY_LSB_FIRST	
Source: GUIControlSoftware-setup.exe	Static PE information: Resource name: RT_ICON type: GLS_BINARY_LSB_FIRST	
Source: GUIControlSoftware-setup.exe	Static PE information: Resource name: RT_ICON type: GLS_BINARY_LSB_FIRST	
Source: GUIControlSoftware-setup.exe	Static PE information: Resource name: RT_ICON type: GLS_BINARY_LSB_FIRST	
Source: GUIControlSoftware-setup.exe	Binary or memory string: OriginalFilename vs GUIControlSoftware-setup.exe	
Source: GUIControlSoftware-setup.exe, 00000000.00000000.219112328.0000000000BEE000.00000002.00020000.sdmp	Binary or memory string: OriginalFilenamesetup.exe vs GUIControlSoftware-setup.exe	
Source: GUIControlSoftware-setup.exe, 00000000.00000002.224078260.00000000049C0000.00000002.00000001.sdmp	Binary or memory string: OriginalFilenamemswsock.dll.muij% vs GUIControlSoftware-setup.exe	
Source: GUIControlSoftware-setup.exe	Binary or memory string: OriginalFilenamesetup.exe vs GUIControlSoftware-setup.exe	
Source: classification engine	Classification label: sus28.evad.winEXE@5/88@3/1	
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BC0150 FindResourceW,LoadResource,SizeofResource,LockResource,	0_2_00BC0150
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	File created: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ChameleonMiniGUI[1].application	Jump to behavior
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	File created: C:\Users\user\AppData\Local\Temp\VSD97F8.tmp	Jump to behavior
Source: GUIControlSoftware-setup.exe	Static PE information: Section: .text IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ	
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Section loaded: C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Section loaded: C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	File read: C:\Users\user\Desktop\desktop.ini	Jump to behavior
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Key opened: HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	Jump to behavior
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	File read: C:\Windows\System32\drivers\etc\hosts	Jump to behavior
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	File read: C:\Windows\System32\drivers\etc\hosts	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	File read: C:\Windows\System32\drivers\etc\hosts	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	File read: C:\Windows\System32\drivers\etc\hosts	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	File read: C:\Windows\System32\drivers\etc\hosts	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	File read: C:\Windows\System32\drivers\etc\hosts	Jump to behavior
Source: GUIControlSoftware-setup.exe	String found in binary or memory: sage:\r\n -? or -h or -help : Show this dialog.\r\n -url or -componentsurl : Show the stored url and componentsurl for this	

Source: unknown	Process created: C:\Users\user\Desktop\GUIControlSoftware-setup.exe 'C:\Users\user\Desktop\GUIControlSoftware-setup.exe'	
Source: unknown	Process created: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	
Source: unknown	Process created: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe 'C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe'	
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Process created: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Process created: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe 'C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe'	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Key value queried: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00020420-0000-0000-C000-000000000046}\InprocServer32	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Key opened: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Settings	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Automated click: Install	
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Automated click: Run	
Source: Window Recorder	Window detected: More than 3 window changes detected	
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	File opened: C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorrc.dll	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Registry value created: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\336808998ffdc525	Jump to behavior
Source: GUIControlSoftware-setup.exe	Static PE information: data directory type: IMAGE_DIRECTORY_ENTRY_IMPORT	
Source: GUIControlSoftware-setup.exe	Static PE information: data directory type: IMAGE_DIRECTORY_ENTRY_RESOURCE	
Source: GUIControlSoftware-setup.exe	Static PE information: data directory type: IMAGE_DIRECTORY_ENTRY_BASERELOC	
Source: GUIControlSoftware-setup.exe	Static PE information: data directory type: IMAGE_DIRECTORY_ENTRY_DEBUG	
Source: GUIControlSoftware-setup.exe	Static PE information: data directory type: IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	
Source: GUIControlSoftware-setup.exe	Static PE information: data directory type: IMAGE_DIRECTORY_ENTRY_IAT	
Source: GUIControlSoftware-setup.exe	Static PE information: TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT	
Source: GUIControlSoftware-setup.exe	Static PE information: data directory type: IMAGE_DIRECTORY_ENTRY_DEBUG	
Source:	Binary string: C:\Users\Koisi\documents\visual studio 2017\Projects\Crapto1Sharp\Crapto1Sharp\obj\Release\net45\Crapto1Sharp.pdb source: dfsvc.exe, 00000001.00000002.1035513981.0000021812F64000.00000004.00000001.sdmp, Crapto1Sharp.dll0.1.dr	
Source:	Binary string: E:\stm32 UCOS\STM32_USB\BOOT_LOADER_EXE(lib)\Release\BOOT_LOADER_EXE.pdb source: dfsvc.exe, 00000001.00000002.1032725485.0000021812B7E000.00000004.00000001.sdmp, BOOT_LOADER_EXE.exe0.1.dr	
Source:	Binary string: C:\Projects\ChameleonMini\ChameleonMini-rebootedGUI_2\ChameleonMiniGUI\obj\Release\ChameleonMiniGUI.pdb source: dfsvc.exe, 00000001.00000002.1035940141.00000218130AE000.00000004.00000001.sdmp, ChameleonMiniGUI.exe, ChameleonMiniGUI.exe0.1.dr	
Source:	Binary string: d:\a\1\s\src\DynamicExpresso.Core\obj\Release\net461\DynamicExpresso.Core.pdb source: dfsvc.exe, 00000001.00000002.1035513981.0000021812F64000.00000004.00000001.sdmp, DynamicExpresso.Core.dll0.1.dr	
Source:	Binary string: setup.pdbS source: GUIControlSoftware-setup.exe	
Source:	Binary string: setup.pdb source: GUIControlSoftware-setup.exe	
Source:	Binary string: C:\Users\Koisi\documents\visual studio 2017\Projects\Crapto1Sharp\Crapto1Sharp\obj\Release\net45\Crapto1Sharp.pdbSHA256P)iz source: dfsvc.exe, 00000001.00000002.1035513981.0000021812F64000.00000004.00000001.sdmp, Crapto1Sharp.dll0.1.dr	
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BAFBE1 LoadLibraryW,GetProcAddress,GetProcAddress,	0_2_00BAFBE1
Source: GUIControlSoftware-setup.exe	Static PE information: real checksum: 0x7a7c8 should be: 0x89e33	
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BC3876 push ecx; ret	0_2_00BC3889
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BC3115 push ecx; ret	0_2_00BC3128
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Code function: 5_2_00976748 push 00000028h; iretd	5_2_009770DA
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Code function: 5_2_054E8C59 push 680601E7h; iretd	5_2_054E8C65
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Jump to dropped file

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\Crapto1Sharp.dll	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\DynamicExpresso.Core.dll	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Crapto1Sharp.dll	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Be.Windows.Forms.HexBox.dll	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\ChameleonMiniGUI.exe	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\avrdude.exe	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\be.w..xbox_e0e5adf0ebc99863_0001.0006_none_3d4df2ccf20aaec3\Be.Windows.Forms.HexBox.dll	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\avrdude.exe	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\BOOT_LOADER_EXE.exe	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\DynamicExpresso.Core.dll	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\BOOT_LOADER_EXE.exe	Jump to dropped file
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	File created: C:\Users\user\AppData\Local\Temp\VSD97F8.tmp\install.log	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Christian Herrmann	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Christian Herrmann\The rebooted suite	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Christian Herrmann\The rebooted suite\Chameleon Mini Rebooted GUI.appref-ms	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Christian Herrmann\The rebooted suite\Chameleon Mini Rebooted GUI online support.url	Jump to behavior

Hooking and other Techniques for Hiding and Protection:

Creates files in alternative data streams (ADS)

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File created: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\ChameleonMiniGUI.exe:Zone.Identifier	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Key value created or modified: HKEY_CURRENT_USER_Classes\Software\Microsoft\Windows\CurrentVersion\Deployment\SideBySide\2.0\PackageMetadata\{2ec93463-b0c3-45e1-8364-327e96aea856}_{60051b8f-4f12-400a-8e50-dd05ebd438d1}\cham..tion_0000000000000000_0001.0003_ebe3bf2e417b6dcf {c989bb7a-8385-4715-98cf-a741a8edb823}!ApplicationTrust	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft		

.NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft		

.NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior

Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000	Process information set: NOOPENFILEERRORBOX	Jump to behavior

_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe		
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior

Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Process information set: NOOPENFILEERRORBOX	Jump to behavior

Malware Analysis System Evasion:

Queries sensitive port information (via WMI, Win32_SerialPort, often done to detect virtual machines)

Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Ap	

ps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Ap	

ps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;

Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;

_dd81ee9d302ebe52\ChameleonMiniGUI.exe	
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.D	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID

KT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.D	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID

KT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.D	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID

KT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.D	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID

KT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Ap	

ps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort

Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort where PNPDeviceID like &apos;%VID_03EB&amp;PID_2044%&apos; or PNPDeviceID like &apos;%VID_16D0&amp;PID_04B2%&apos;	
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	WMI Queries: IWbemServices::ExecQuery - root\cimv2 : select Name, DeviceID, PNPDeviceID from Win32_SerialPort	
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	File opened / queried: SCSI#CdRom&Ven_NECVMWar&Prod_VMware_SATA_CD00#5&280b647&0&000000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 922337203685477	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 600000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 599860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 599750	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 599657	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 599547	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 599453	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 599360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 599203	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 599110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 598953	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 598860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 598563	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 598453	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 598250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 598110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 598000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 597860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 597703	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 597610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 597500	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 597360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 597250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 597110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 597000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 596907	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 596797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 596703	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 596610	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 596453	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 596360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 596250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 596157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 596000	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 595907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 595797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 595703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 595610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 595453	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 595360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 595250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 595157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 595047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 594907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 594797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 594703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 594610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 594500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 594360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 594250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 594157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 594047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 593907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 593797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 593703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 593610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 593453	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 593360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 593250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 593157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 593047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 592907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 592797	Jump to behavior

Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 592703	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 592610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 592500	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 592360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 592250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 592110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 592000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 591860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 591750	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 591610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 591500	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 591407	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 591297	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 591203	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 591110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 590953	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 590860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 590750	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 590610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 590500	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 590407	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 590297	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 590157	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 590047	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 589953	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 589797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 589657	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 589547	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 589453	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 589360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 589250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 589110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 589000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 588907	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 588813	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 588703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 588563	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 588453	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 588360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 588250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 588157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 588063	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 587907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 587797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 587657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 587500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 587407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 587297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 587157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 587047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 586953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 586860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 586500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 586360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 586250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 586157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 586000	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 585407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 584953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 584860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 584703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 584610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 584500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 584407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 584250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 584157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 584047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 583953	Jump to behavior

Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 583860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 583703	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 583610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 583500	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 583407	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 583297	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 583157	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 583047	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 582953	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 582860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 582657	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 582547	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 582453	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 582360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 582250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 582110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 582000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 581907	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 581797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 581703	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 581563	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 581453	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 581360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 581250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 581157	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 581047	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 580907	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 580797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 580703	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 580610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 580500	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 580360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 580250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 580157	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 580047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 579953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 579797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 579657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 579547	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 579453	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 579360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 579203	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 579110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 579000	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 578860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 578703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 578610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 578500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 578407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 578297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 578157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 578000	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 577907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 577750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 577610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 577500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 577407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 577297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 577203	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 577110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 576953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 576860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 576750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 576657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 576547	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 576407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 576297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 576203	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 576047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 575907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 575797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 575703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 575610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 575500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 575360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 575250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 575157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 575047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 574953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 574860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 574703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 574610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 574500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 574407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 574297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 574157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 574047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 573953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 573860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 573750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 573610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 573500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 573407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 573297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 573203	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 573110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 572953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 572860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 572750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 572610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 572500	Jump to behavior
Source: C:\Windows\Microsoft	Thread delayed: delay time: 572360	Jump to behavior

.NET\Framework64\v4.0.30319\dfsvc.exe		
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 572250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 572157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 572047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 571953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 571860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 571703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 571610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 571500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 571407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 571297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 571157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 571047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 570953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 570860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 570750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 570610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 570500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 570407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 570297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 570203	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 570110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 569953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 569860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 569750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 569657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 569547	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 569297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 569203	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 569110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 569000	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 568860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 568750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 568657	Jump to behavior

Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 568203	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 568110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 568000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 567907	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 567797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 567360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 567203	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 566797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 566657	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 566547	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 566407	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 566297	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 566203	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 566110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 566000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 565860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 565750	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 565657	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 565547	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 565453	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 565360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 565203	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 565110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 565000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 564907	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 564797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 564657	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 564547	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 564453	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 564360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 564250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 564110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 564000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 563907	Jump to behavior

Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 563797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 563703	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 563610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 563453	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 563360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 563250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 563157	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 563047	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 562907	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 562797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 562703	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 562610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 562500	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 562360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 562250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 562157	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 562047	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 561953	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 561860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 561703	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 561610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 561500	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 561407	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 561297	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 561157	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 561047	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 560953	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 560860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 560750	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 560610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 560500	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 560407	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 560297	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 560203	Jump to behavior

Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 560110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 559953	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 559860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 559750	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 559657	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 559547	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 559407	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 559297	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 559203	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 559110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 559000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 558860	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 558750	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 558657	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 558547	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 558453	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 558360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 558203	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 558110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 558000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 557907	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 557797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 557657	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 557547	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 557453	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 557360	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 557250	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 557110	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 557000	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 556907	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 556797	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 556703	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 556610	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 556453	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 556360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 556250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 556157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 556047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 555907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 555797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 555703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 555610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 555500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 555360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 555250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 555157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 555047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 554953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 554860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 554703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 554610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 554500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 554407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 554297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 554157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 554047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 553953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 553860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 553750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 553610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 553500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 553407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 553297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 553203	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 553110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 552953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 552860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 552750	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 552657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 552547	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 552407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 552297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 552203	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 552110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 552000	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 551860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 551750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 551657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 551547	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 551453	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 551360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 551157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 551047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 550953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 550860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 550703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 550610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 550500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 550110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 550000	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 549907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 549797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 549657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 549203	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 549110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 548657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 548453	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 548360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 548250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 548157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 548047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 547907	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 547797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 547703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 547610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 547500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 547360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 547250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 547157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 547047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 546953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 546860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 546703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 546610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 546500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 546407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 546297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 546157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 546047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 545953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 545860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 545750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 545610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 545500	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 545407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 545297	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 545203	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 545110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 544953	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 544860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 544750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 544657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 544547	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 544407	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 544297	Jump to behavior
Source: C:\Windows\Microsoft	Thread delayed: delay time: 544203	Jump to behavior

.NET\Framework64\v4.0.30319\dfsvc.exe		
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 544110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 544000	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 543860	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 543750	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 543657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 543547	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 543453	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 543360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 543203	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 543110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 543000	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 542907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 542797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 542657	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 542547	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 542453	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 542360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 542250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 542110	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 542000	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 541907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 541797	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 541703	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 541610	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 541453	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 541360	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 541250	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 541157	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 541047	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread delayed: delay time: 540907	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Window / User API: threadDelayed 412	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Window / User API: threadDelayed 2409	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Dropped PE file which has not been started: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\Crapto1Sharp.dll	Jump to dropped file

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Dropped PE file which has not been started: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\DynamicExpresso.Core.dll	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Dropped PE file which has not been started: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Crapto1Sharp.dll	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Dropped PE file which has not been started: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\avrdude.exe	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Dropped PE file which has not been started: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\avrdude.exe	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Dropped PE file which has not been started: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Extras\BOOT_LOADER_EXE.exe	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Dropped PE file which has not been started: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\DynamicExpresso.Core.dll	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Dropped PE file which has not been started: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham...exe_0000000000000000_0001.0003_none_20a63939d72fdbc5\Extras\BOOT_LOADER_EXE.exe	Jump to dropped file
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -922337203685477s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -600000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -599860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -599750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -599657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -599547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -599453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -599360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -599203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -599110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -598953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -598860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -598563s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -598453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -598250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -598110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -598000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -597860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread sleep time: -597703s >= -30000s	Jump to behavior

TID: 4940		
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -597610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -597500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -597360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -597250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -597110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -597000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -596907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -596797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -596703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -596610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -596453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -596360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -596250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -596157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -596000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -595907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -595797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -595703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -595610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -595453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -595360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -595250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -595157s >= -30000s	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -595047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -594907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -594797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -594703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -594610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -594500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -594360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -594250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -594157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -594047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -593907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -593797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -593703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -593610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -593453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -593360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -593250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -593157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -593047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -592907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -592797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -592703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 5364	Thread sleep time: -120450s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft		

.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -592610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -592500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -592360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -592250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -592110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -592000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -591860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -591750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -591610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -591500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -591407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -591297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -591203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -591110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -590953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -590860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -590750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -590610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -590500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -590407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -590297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -590157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -590047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread sleep time: -589953s >= -30000s	Jump to behavior

TID: 4940		
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -589797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -589657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -589547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -589453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -589360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -589250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -589110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -589000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -588907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -588813s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -588703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -588563s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -588453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -588360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -588250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -588157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -588063s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -587907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -587797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -587657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -587500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -587407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -587297s >= -30000s	Jump to behavior

Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -587157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -587047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -586953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -586860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -586500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -586360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -586250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -586157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -586000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -585407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -584953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -584860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -584703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -584610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -584500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -584407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -584250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -584157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -584047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -583953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -583860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -583703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -583610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft		

.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -583500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -583407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -583297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -583157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -583047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -582953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -582860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -582657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -582547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -582453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -582360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -582250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -582110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -582000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -581907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -581797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -581703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -581563s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -581453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -581360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -581250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -581157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -581047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread sleep time: -580907s >= -30000s	Jump to behavior

TID: 4940		
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -580797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -580703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -580610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -580500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -580360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -580250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -580157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -580047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -579953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -579797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -579657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -579547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -579453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -579360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -579203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -579110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -579000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -578860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -578703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -578610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -578500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -578407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -578297s >= -30000s	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -578157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -578000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -577907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -577750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -577610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -577500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -577407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -577297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -577203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -577110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -576953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -576860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -576750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -576657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -576547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -576407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -576297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -576203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -576047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -575907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -575797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -575703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -575610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft		

.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -575500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -575360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -575250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -575157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -575047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -574953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -574860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -574703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -574610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -574500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -574407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -574297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -574157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -574047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -573953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -573860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -573750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -573610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -573500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -573407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -573297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -573203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -573110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Thread sleep time: -572953s >= -30000s	Jump to behavior

TID: 4940		
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -572860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -572750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -572610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -572500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -572360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -572250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -572157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -572047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -571953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -571860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -571703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -571610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -571500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -571407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -571297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -571157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -571047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -570953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -570860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -570750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -570610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -570500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -570407s >= -30000s	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -570297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -570203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -570110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -569953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -569860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -569750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -569657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -569547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -569297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -569203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -569110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -569000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -568860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -568750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -568657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -568203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -568110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -568000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -567907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -567797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -567360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -567203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -566797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread sleep time: -566657s >= -30000s	Jump to behavior

TID: 4940		
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -566547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -566407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -566297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -566203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -566110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -566000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -565860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -565750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -565657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -565547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -565453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -565360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -565203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -565110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -565000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -564907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -564797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -564657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -564547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -564453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -564360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -564250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -564110s >= -30000s	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -564000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -563907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -563797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -563703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -563610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -563453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -563360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -563250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -563157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -563047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -562907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -562797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -562703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -562610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -562500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -562360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -562250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -562157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -562047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -561953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -561860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -561703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -561610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft		

.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -561500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -561407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -561297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -561157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -561047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -560953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -560860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -560750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -560610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -560500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -560407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -560297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -560203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -560110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -559953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -559860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -559750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -559657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -559547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -559407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -559297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -559203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -559110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -559000s >= -30000s	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -558860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -558750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -558657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -558547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -558453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -558360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -558203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -558110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -558000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -557907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -557797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -557657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -557547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -557453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -557360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -557250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -557110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -557000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -556907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -556797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -556703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -556610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -556453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft		

.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -556360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -556250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -556157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -556047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -555907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -555797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -555703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -555610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -555500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -555360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -555250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -555157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -555047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -554953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -554860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -554703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -554610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -554500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -554407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -554297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -554157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -554047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -553953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Thread sleep time: -553860s >= -30000s	Jump to behavior

TID: 4940		
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -553750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -553610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -553500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -553407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -553297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -553203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -553110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -552953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -552860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -552750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -552657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -552547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -552407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -552297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -552203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -552110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -552000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -551860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -551750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -551657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -551547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -551453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -551360s >= -30000s	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -551157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -551047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -550953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -550860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -550703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -550610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -550500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -550110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -550000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -549907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -549797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -549657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -549203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -549110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -548657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -548453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -548360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -548250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -548157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -548047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -547907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -547797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -547703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft		

.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -547610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -547500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -547360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -547250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -547157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -547047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -546953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -546860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -546703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -546610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -546500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -546407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -546297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -546157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -546047s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -545953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -545860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -545750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -545610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -545500s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -545407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -545297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -545203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -545110s >= -30000s	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -544953s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -544860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -544750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -544657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -544547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -544407s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -544297s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -544203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -544110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -544000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -543860s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -543750s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -543657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -543547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -543453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -543360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -543203s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -543110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -543000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -542907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -542797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -542657s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -542547s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft		

.NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -542453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -542360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -542250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -542110s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -542000s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -541907s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -541797s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -541703s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -541610s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -541453s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -541360s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -541250s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -541157s >= -30000s	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe TID: 4940	Thread sleep time: -541047s >= -30000s	Jump to behavior
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BA3DDD __EH_prolog3_GS,char_traits,char_traits,FindFirstFileW,char_traits,FindNextFileW,FindClose,FindClose,	0_2_00BA3DDD
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\AppData\Local\Apps\2.0\	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\AppData\Local\	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\AppData\Local\Apps\	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\AppData\	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	File opened: C:\Users\user\	Jump to behavior
Source: dfsvc.exe, 00000001.00000002.1037258734.000002182B169000.00000004.00000001.sdmp	Binary or memory string: Hyper-V RAW	
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BC7F97 IsDebuggerPresent,SetUnhandledExceptionFilter,UnhandledExceptionFilter,	0_2_00BC7F97
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BAFBE1 LoadLibraryW,GetProcAddress,GetProcAddress,	0_2_00BAFBE1
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Process token adjusted: Debug	Jump to behavior
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Process created: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Jump to behavior
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BC390E SetUnhandledExceptionFilter,UnhandledExceptionFilter,GetCurrentProcess,TerminateProcess,	0_2_00BC390E

Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BC7F97 IsDebuggerPresent,SetUnhandledExceptionFilter,UnhandledExceptionFilter,	0_2_00BC7F97
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Memory allocated: page read and write | page guard	Jump to behavior
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BA1178 ShellExecuteExW,GetLastError,WaitForSingleObject,CloseHandle,	0_2_00BA1178
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Process created: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe 'C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe'	Jump to behavior
Source: dfsvc.exe, 00000001.00000002.1027475591.00000218114B0000.00000002.00000001.sdmp, ChameleonMiniGUI.exe, 00000005.00000002.1031261174.0000000001910000.00000002.00000001.sdmp	Binary or memory string: Shell_TrayWnd	
Source: dfsvc.exe, 00000001.00000002.1027475591.00000218114B0000.00000002.00000001.sdmp, ChameleonMiniGUI.exe, 00000005.00000002.1031261174.0000000001910000.00000002.00000001.sdmp	Binary or memory string: Progman	
Source: dfsvc.exe, 00000001.00000002.1027475591.00000218114B0000.00000002.00000001.sdmp, ChameleonMiniGUI.exe, 00000005.00000002.1031261174.0000000001910000.00000002.00000001.sdmp	Binary or memory string: Progmanlock	
Source: dfsvc.exe, 00000001.00000002.1027475591.00000218114B0000.00000002.00000001.sdmp, ChameleonMiniGUI.exe, 00000005.00000002.1031261174.0000000001910000.00000002.00000001.sdmp	Binary or memory string: Program Manager[	
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: EnumSystemLocalesW,	0_2_00BD0931
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: GetLocaleInfoW,GetLocaleInfoW,GetACP,	0_2_00BD7BC7
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: GetLocaleInfoW,	0_2_00BD0C3A
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: IsValidCodePage,GetLocaleInfoW,	0_2_00BD746A
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: GetUserDefaultLCID,IsValidCodePage,IsValidLocale,GetLocaleInfoW,GetLocaleInfoW,	0_2_00BD7D9B
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: EnumSystemLocalesW,	0_2_00BD76E2
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: EnumSystemLocalesW,	0_2_00BD77C1
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: EnumSystemLocalesW,	0_2_00BD772D
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Deployment\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Deployment.dll VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\arial.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ariali.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\arialbd.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\arialbi.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ARIALN.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ariblk.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ARIALNI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ARIALNB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ARIALNBI.TTF VolumeInformation	Jump to behavior

Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\bahnschrift.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\calibri.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\calibril.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\calibrii.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\calibrili.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\calibrib.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\calibriz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\cambria.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\cambriai.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\cambriab.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\cambriaz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\Candara.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\Candarai.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\Candarab.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\Candaraz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\comic.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\comici.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\comicbd.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\comicz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\consola.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\consolai.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\consolab.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\consolaz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\constan.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\constani.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\constanb.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\constanz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\corbel.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\corbeli.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\corbelb.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\corbelz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\cour.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\couri.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\courbd.ttf VolumeInformation	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\courbi.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ebrima.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ebrimabd.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\framd.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FRADM.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\framdit.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FRADMIT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FRAMDCN.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FRADMCN.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FRAHV.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FRAHVIT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\Gabriola.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\gadugi.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\gadugib.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\georgia.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\georgiai.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\georgiab.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\georgiaz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\impact.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\Inkfree.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\javatext.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LeelawUI.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LeelUIsl.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LeelaUIb.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\lucon.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\l_10646.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\malgun.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\malgunsl.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\malgunbd.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\himalaya.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\msjh.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\msjhl.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\msjhbd.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ntailu.ttf VolumeInformation	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ntailub.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\phagspa.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\phagspab.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\micross.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\taile.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\taileb.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\msyh.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\msyhl.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\msyhbd.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\msyi.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\mingliub.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\monbaiti.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\msgothic.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\mvboli.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\mmrtext.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\mmrtextb.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\Nirmala.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\NirmalaS.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\NirmalaB.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\pala.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\palai.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\palab.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\palabi.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\segoepr.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\segoeprb.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\segoesc.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\segoescb.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\segoeuii.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\seguisli.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\seguili.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\seguisbi.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\segoeuiz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\seguibl.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\seguibli.ttf VolumeInformation	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\seguiemj.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\seguihis.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\seguisym.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\simsun.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\simsunb.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\Sitka.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\SitkaI.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\SitkaB.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\SitkaZ.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\sylfaen.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\symbol.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\tahoma.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\tahomabd.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\timesi.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\timesbd.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\timesbi.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\trebuc.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\trebucit.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\trebucbd.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\trebucbi.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\verdana.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\verdanai.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\verdanab.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\verdanaz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\webdings.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\wingding.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\YuGothR.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\YuGothM.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\YuGothL.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\YuGothB.ttc VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\holomdl2.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CENTURY.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LEELAWAD.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LEELAWDB.TTF VolumeInformation	Jump to behavior

Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\MSUIGHUR.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\MSUIGHUB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\WINGDNG2.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\WINGDNG3.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\TEMPSITC.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PRISTINA.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PAPYRUS.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\MISTRAL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LHANDW.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ITCKRIST.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\JUICE___.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FRSCRIPT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FREESCPT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BRADHITC.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\OUTLOOK.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BKANT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ANTQUAI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ANTQUAB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ANTQUABI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GARA.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GARAIT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GARABD.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\MTCORSVA.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GOTHIC.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GOTHICI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GOTHICB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GOTHICBI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ALGER.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BASKVILL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BAUHS93.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BELL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BELLI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BELLB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BRLNSR.TTF VolumeInformation	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BRLNSDB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BRLNSB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BERNHC.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_PSTC.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BRITANIC.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BROADW.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BRUSHSCI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CALIFR.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CALIFI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CALIFB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CENTAUR.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CHILLER.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\COLONNA.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\COOPBL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FTLTLT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\HARLOWSI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\HARNGTON.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\HTOWERT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\HTOWERTI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\JOKERMAN.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\KUNSTLER.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LBRITE.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LBRITED.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LBRITEI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LBRITEDI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LCALLIG.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LFAX.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LFAXD.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LFAXI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LFAXDI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\MAGNETOB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\MATURASC.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\MOD20.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\NIAGENG.TTF VolumeInformation	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\NIAGSOL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\OLDENGL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ONYX.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PARCHM.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PLAYBILL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\POORICH.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\RAVIE.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\INFROMAN.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\SHOWG.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\SNAP____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\STENCIL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\VINERITC.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\VIVALDII.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\VLADIMIR.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LATINWD.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\TCM_____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\TCMI____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\TCB_____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\TCBI____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\TCCM____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\TCCB____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\TCCEB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\SCRIPTBL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ROCK.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ROCKI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ROCKB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ROCKEB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ROCKBI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ROCC____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ROCCB___.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\RAGE.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PERTILI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PERTIBD.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PER_____.TTF VolumeInformation	Jump to behavior

Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PERI____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PERB____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PERBI___.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\PALSCRI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\OCRAEXT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\MAIAN.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LTYPE.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LTYPEO.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LTYPEB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LTYPEBO.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LSANS.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LSANSD.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LSANSI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\LSANSDI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\IMPRISHA.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\HATTEN.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GOUDYSTO.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GOUDOS.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GOUDOSI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GOUDOSB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GLECB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GIL_____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GILI____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GILB____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GILBI___.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GILC____.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GLSNECB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\GIGI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FRABK.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FRABKIT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FORTE.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\FELIXTI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ERASMD.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ERASLGHT.TTF VolumeInformation	Jump to behavior

Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ERASDEMI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ERASBD.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ENGR.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ELEPHNT.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ELEPHNTI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ITCEDSCR.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CURLZ___.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\COPRGTL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\COPRGTB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CENSCBK.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\SCHLBKI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\SCHLBKB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\SCHLBKBI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CASTELAR.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CALIST.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CALISTI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CALISTB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\CALISTBI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOOKOS.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOOKOSB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOOKOSI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOOKOSBI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_R.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_I.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_B.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_BI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_CR.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_BLAR.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_CI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_CB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_BLAI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BOD_CBI.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ITCBLKAD.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft .NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\ARLRDBD.TTF VolumeInformation	Jump to behavior

Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\AGENCYR.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\AGENCYB.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\BSSYM7.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\REFSAN.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\REFSPCL.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\MTEXTRA.TTF VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\marlett.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\segoeuii.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\segoeuiz.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\micross.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Security\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Security.dll VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Windows\Fonts\segoeui.ttf VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Be.Windows.Forms.HexBox.dll VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Crapto1Sharp.dll VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\DynamicExpresso.Core.dll VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\ChameleonMiniGUI.exe VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\ChameleonMiniGUI.exe VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Be.Windows.Forms.HexBox.dll VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\Crapto1Sharp.dll VolumeInformation	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Queries volume information: C:\Users\user\AppData\Local\Temp\Deployment\RHJ1RP4N.RRL\8NARJKRT.HWH\DynamicExpresso.Core.dll VolumeInformation	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Queries volume information: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe VolumeInformation	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Queries volume information: C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll VolumeInformation	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Queries volume information: C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Drawing.dll VolumeInformation	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Queries volume information: C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Accessibility\v4.0_4.0.0.0__b03f5f7f11d50a3a\Accessibility.dll VolumeInformation	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Queries volume information: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\Be.Windows.Forms.HexBox.dll VolumeInformation	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Queries volume information: C:\Windows\Fonts\cour.ttf VolumeInformation	Jump to behavior

Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Queries volume information: C:\Windows\Fonts\couri.ttf VolumeInformation	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Queries volume information: C:\Windows\Fonts\courbd.ttf VolumeInformation	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Queries volume information: C:\Windows\Fonts\courbi.ttf VolumeInformation	Jump to behavior
Source: C:\Users\user\AppData\Local\Apps\2.0\98Q6K1PM.A98\T3ZWOO1X.DKT\cham..tion_0000000000000000_0001.0003_dd81ee9d302ebe52\ChameleonMiniGUI.exe	Queries volume information: C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Management.dll VolumeInformation	Jump to behavior
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BC351D GetSystemTimeAsFileTime,GetCurrentThreadId,GetCurrentProcessId,QueryPerformanceCounter,	0_2_00BC351D
Source: C:\Users\user\Desktop\GUIControlSoftware-setup.exe	Code function: 0_2_00BC0D9F GetVersionExW,	0_2_00BC0D9F
Source: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe	Key value queried: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography MachineGuid	Jump to behavior

Close