Analysis # 1819

07/25/2014 03:53 am

Table of Contents

Analysis Summary

Submitted File:	Blended.exe
MD5:	036c7215d8fa37090b3aec9786a8e5b3
File Size:	321688
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-07-25 03:53:38
Start Reason:	AnalysisTarget
Termination Reason:	Timeout
Start Time:	Fri, 25 Jul 2014 07:56:51 +0000
Termination Time:	Fri, 25 Jul 2014 07:57:50 +0000
Analysis Time:	2014-07-25 03:53:38
Sandbox:	XP-SP2 - 00-0C-29-B2-D2-62
Total Processes:	10
Sample Notes:	

Digital Behavior Traits

Alters Windows Firewall	—	Hooks Keyboard	✓
Checks For Debugger	—	Injected Code	—
Copies to Windows	—	Makes Network Connection	✓
Could Not Load	✓	Modifies File in System	✓
Creates DLL in System	—	Modifies Local DNS	—
Creates EXE in System	—	More than 5 Processes	✓
Creates Hidden File	✓	Opens Physical Memory	—
Creates Mutex	✓	Starts EXE in Documents	✓
Creates Service	—	Starts EXE in Recycle	—
Deletes File in System	—	Starts EXE in System	✓
Deletes Original Sample	—	Windows/Run Registry Key Set	—

Deleted Files
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\3EE0E135.dat
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4 O5PO1W\r1_homebestmy_info[1]
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.1.ini.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.2_0.ini.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.general_logo.bmp.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.v_grey.jpg.part
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\FA R0XHUV\v_grey[1].jpg
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.v_grey.jpg.part
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4 O5PO1W\v_grey[1].jpg
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.v_grey.jpg.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.4.ini.part
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\8S 80F7UV\general_logo[1].bmp
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.general_logo.bmp.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.4_2.ini.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.4_3.ini.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.5.ini.part
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\MV 52VCF4\general_logo[1].bmp
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.general_logo.bmp.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.5_1.ini.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.6.ini.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.6_1.ini.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.setupespl.exe.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.6_1_0.ini.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.extIE_setup.exe.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.6_1_3.ini.part
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.setupytb.exe.part
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\dUG8Pp8.dat
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\dUG8Pp8.exe
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\jqzjj@qvvmt.net\content\bg.js
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\jqzjj@qvvmt.net\install.rdf
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\jqzjj@qvvmt.net\chrome.manifest
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\jqzjj@qvvmt.net\bootstrap.js
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki\lsdb.js
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki\content.js
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki\manifest.jso n
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki\background.h tml
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki\N5vsAjJp.js
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\jqzjj@qvvmt.net\content
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\jqzjj@qvvmt.net
[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c\my8.dat
[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c\my8.exe

[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c\8X.x64.dll
[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c\8X.tlb
[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c\8X.dll
[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c
[process 9] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Last Active\{EFE2BC8D-884E-11E3-B967-000C29B2D262}.dat
[process 9] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{EFE2BC8C-884E-11E3-B967-000C29B2D262}.dat

Stored Modified Files
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Tsu00438D06.dll
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\3EE0E135.dat
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\{A7D91CB0-562A-49D3-AB38-1E087C3A3E46}_Setup.dll
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\{A7D91CB0-562A-49D3-AB38-1E087C3A3E46}\Setup.ico
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\{A7D91CB0-562A-49D3-AB38-1E087C3A3E46}\Readme.txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\{A7D91CB0-562A-49D3-AB38-1E087C3A3E46}\Custom.dll
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\{A7D91CB0-562A-49D3-AB38-1E087C3A3E46}\Setup.exe
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4 O5PO1W\1[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.1.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\MV 52VCF4\2_0[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.2_0.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\8S 80F7UV\general_logo[1].bmp
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.general_logo.bmp
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\FA R0XHUV\v_grey[1].jpg
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.v_grey.jpg
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4 O5PO1W\v_grey[1].jpg
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4 O5PO1W\4[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.4.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\MV 52VCF4\general_logo[1].bmp
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\8S 80F7UV\4_2[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.4_2.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\8S 80F7UV\4_3[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.4_3.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\FA R0XHUV\5[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.5.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4 O5PO1W\general_logo[1].bmp
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\MV 52VCF4\5_1[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.5_1.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\MV 52VCF4\6[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.6.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\8S 80F7UV\6_1[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.6_1.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\FA R0XHUV\UXO3nD[1].exe
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.setupespl.exe
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4

O5PO1W\6_1_0[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.6_1_0.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\MV
52VCF4\Jd[1].exe
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.extIE_setup.exe
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\8S
80F7UV\6_1_3[1].txt
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.6_1_3.ini
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\FA
R0XHUV\ed[1].exe
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\down.1100.setupytb.exe
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\dUG8Pp8.dat
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\dUG8Pp8.exe
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\jqzjj@qvvmt.net\content\bg.js
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\jqzjj@qvvmt.net\install.rdf
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\jqzjj@qvvmt.net\chrome.manifest
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\jqzjj@qvvmt.net\bootstrap.js
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki\lsdb.js
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki\content.js
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki\manifest.jso
n
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki\background.h
tml
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\517708f4\nmpnnmnohmmkndkkcnnlhmgploiadkki\N5vsAjJp.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome\User Dat
a\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome\User Dat
a\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome\User Dat
a\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome\User Dat
a\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome\User Dat

a\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome\User Dat
a\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome\User Dat
a\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome\User Dat
a\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome\User Dat
a\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js

[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Comodo\Dragon\User Data\

Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Comodo\Dragon\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Comodo\Dragon\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Comodo\Dragon\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Comodo\Dragon\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Comodo\Dragon\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Comodo\Dragon\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Comodo\Dragon\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Comodo\Dragon\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Comodo\Dragon\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Comodo\Dragon\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Comodo\Dragon\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Comodo\Dragon\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Comodo\Dragon\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Comodo\Dragon\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Comodo\Dragon\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Comodo\Dragon\Us
er Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Comodo\Dragon
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Comodo\Dragon
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Comodo\Dragon
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Comodo\Dragon
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Comodo\Dragon
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Comodo\Dragon
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Comodo\Dragon
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Comodo\Dragon
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Comodo\Dragon
\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js

[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome SxS\User
Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome SxS\User
Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome SxS\User
Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome SxS\User
Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome SxS\User
Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome SxS\User
Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome SxS\User
Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome SxS\User
Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Google\Chrome SxS\User
Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome SxS\User D
ata\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome SxS\User D
ata\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome SxS\User D
ata\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome SxS\User D
ata\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome SxS\User D
ata\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome SxS\User D
ata\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome SxS\User D
ata\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome SxS\User D

ata\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Google\Chrome SxS\User D
ata\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Google\Chrome Sx
S\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
SxS\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
SxS\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
SxS\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
SxS\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
SxS\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
SxS\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
SxS\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
SxS\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Google\Chrome
SxS\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Torch\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Torch\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Torch\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Torch\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Torch\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Torch\User Data\
Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json

[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Torch\User Data\

Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Torch\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Administrator\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js

[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Charlie\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\Guest\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\HelpAssistant\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Chromatic Browser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\background.html
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Chromatic Bro

wser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Chromatic Bro
wser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\content.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Chromatic Bro
wser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Chromatic Bro
wser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\lsdb.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Chromatic Bro
wser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Chromatic Bro
wser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\manifest.json
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Chromatic Bro
wser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\Documents and Settings\SUPPORT_388945a0\Local Settings\Application Data\Chromatic Bro
wser\User Data\Default\Extensions\nmpnnmnohmmkndkkcnnlhmgploiadkki\3.9\N5vsAjJp.js
[process 4] C:\WINDOWS\system32\GroupPolicy\gpt.ini
[process 4] C:\WINDOWS\system32\GroupPolicy\gpt.ini
[process 4] C:\WINDOWS\system32\GroupPolicy\gpt.ini
[process 4] C:\WINDOWS\system32\GroupPolicy\Machine\Registry.pol
[process 4] C:\WINDOWS\system32\GroupPolicy\gpt.ini
[process 4] C:\WINDOWS\system32\GroupPolicy\gpt.ini
[process 4] C:\Documents and Settings\All Users\Application Data\e760b835e25f8c72\{FDB962F0-B5B8-946
0-D12F-7966E97BAA43}.20140725035722
[process 5] C:\Documents and Settings\All Users\ntuser.pol
[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c\my8.dat
[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c\my8.exe
[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c\8X.x64.dll
[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c\8X.tlb
[process 6] C:\DOCUME~1\Charlie\LOCALS~1\Temp\5260263c\8X.dll
[process 7] C:\Program Files\pricechop\8X.dll
[process 7] C:\Program Files\pricechop\8X.dll
[process 7] C:\Program Files\pricechop\8X.tlb
[process 7] C:\Program Files\pricechop\8X.tlb
[process 7] C:\Program Files\pricechop\8X.dat
[process 7] C:\Program Files\pricechop\8X.dat
[process 7] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763
}\pricechop.2.9.dat
[process 7] C:\Program Files\pricechop\8X.x64.dll
[process 7] C:\Program Files\pricechop\8X.x64.dll
[process 7] C:\Documents and Settings\All Users\Application Data\pricechop\my8.exe
[process 7] C:\Documents and Settings\All Users\Application Data\pricechop\my8.exe
[process 7] C:\Documents and Settings\All Users\Application Data\pricechop\my8.dat
[process 7] C:\Documents and Settings\All Users\Application Data\pricechop\my8.dat
[process 7] C:\Documents and Settings\All Users\Application Data\e760b835e25f8c72\{FDB962F0-B5B8-946
0-D12F-7966E97BAA43}.20140725035738
[process 9] C:\DOCUME~1\Charlie\LOCALS~1\Temp\~DFD48D.tmp
[process 9] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Exp
lorer\Recovery\Active\{590C3E45-13D1-11E4-B96C-000C29B2D262}.dat
[process 9] C:\DOCUME~1\Charlie\LOCALS~1\Temp\~DF110E.tmp
[process 9] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Exp
lorer\Recovery\Last Active\RecoveryStore.{EFE2BC8C-884E-11E3-B967-000C29B2D262}.dat

[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\FAR0XHUV\BODY[1]
[process 10] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4O5PO1W\sync[1]
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat
[process 10] C:\Documents and Settings\Charlie\AppData\LocalLow\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\pricechop.2.9.dat

Created Mutexes	
	mutex
[process 1]	Name: {63E09367-E50C-4567-A78C-AD2EB803B191}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-6
	02162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:!documents and settings!charlie!local settings!temporary internet files!content.ie5!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:!documents and settings!charlie!cookies!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:!documents and settings!charlie!local settings!history!history.ie5!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\WininetConnectionMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\ZonesCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-6
	02162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: Local\!BrowserEmulation!SharedMemory!Mutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: ConnHashTable<988>_HashTable_Mutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: Local\ZonesCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: oleacc-msaa-loaded

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: Local\RSS Eventing Connection Database Mutex 000003dc
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Local\Feed Eventing Shared Memory Mutex S-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-6 02162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Local\!PrivacIE!SharedMemory!Mutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Local\ZonesCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Local\c:!documents and settings!charlie!local settings!application data!microsoft!feeds cache!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Local\c:!documents and settings!charlie!ietldcache!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 4]	\REGISTRY\MACHINE\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
[process 4]	\REGISTRY\MACHINE\SOFTWARE\Google\Update
[process 4]	\REGISTRY\MACHINE\SOFTWARE\Google\Update\ClientState
[process 4]	\REGISTRY\MACHINE\SOFTWARE\Google\Update\ClientState\
[process 4]	\REGISTRY\MACHINE\SOFTWARE\Google\Update\ClientState\{4DC8B4CA-1BDA-483e-B5FA-D3C12E15B62D}
[process 4]	\REGISTRY\MACHINE\SOFTWARE\Policies\Google\Update
[process 4]	\REGISTRY\MACHINE\SOFTWARE\Policies\
[process 4]	\REGISTRY\MACHINE\SOFTWARE\Policies\Google\
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}User
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine\Software\Policies\Google\Chrome
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine\Software
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine\Software\Policies
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine\Software\Policies\Google
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine\Software\Policies\Google\Chrome
[process 4]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43}
[process 5]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List
[process 5]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0
[process 5]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPLink-List
[process 5]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPLink-List\0
[process 5]	\REGISTRY\MACHINE\Software\Policies\Google\Chrome
[process 5]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
[process 5]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\
[process 5]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History\
[process 5]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0
[process 5]	\REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
[process 7]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\RegisteredApplicationsEx
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
[process 7]	\Registry\Machine\Software\Classes\pRicechop.pRicechop.3.9
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\pRicechop.pRicechop.3.9\CLSID
[process 7]	\Registry\Machine\Software\Classes\pRicechop.pRicechop
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\pRicechop.pRicechop\CLSID
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\pRicechop.pRicechop\CurVer

[process 7]	\Registry\Machine\Software\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\ProgID
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\VersionIndependentProgID
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\Programmable
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\InprocServer32
[process 7]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\AppRovedExtensionsMigration
[process 7]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\AppRovedExtensionsMigration\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
[process 7]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Ext
[process 7]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Ext\CLSID
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\PreApproved\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\Implemented Categories
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\Implemented Categories\{59FB2056-D625-48D0-A944-1A85B5AB2640}
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{E2343056-CC08-46AC-B898-BFC7ACF4E755}
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{E2343056-CC08-46AC-B898-BFC7ACF4E755}\1.0
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{E2343056-CC08-46AC-B898-BFC7ACF4E755}\1.0\FLAGS
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{E2343056-CC08-46AC-B898-BFC7ACF4E755}\1.0\0
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{E2343056-CC08-46AC-B898-BFC7ACF4E755}\1.0\0\win32
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{E2343056-CC08-46AC-B898-BFC7ACF4E755}\1.0\HELPDIR
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{9B41579A-1996-42F9-8F84-7B7786818CEF}
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{9B41579A-1996-42F9-8F84-7B7786818CEF}\ProxyStubClsid
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{9B41579A-1996-42F9-8F84-7B7786818CEF}\ProxyStubClsid32
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{9B41579A-1996-42F9-8F84-7B7786818CEF}\TypeLib
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{7041156A-0D2B-4DCD-A8EE-D0608BFCB2D0}
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{7041156A-0D2B-4DCD-A8EE-D0608BFCB2D0}\ProxyStubClsid
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{7041156A-0D2B-4DCD-A8EE-D0608BFCB2D0}\ProxyStubClsid32
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{7041156A-0D2B-4DCD-A8EE-D0608BFCB2D0}\TypeLib
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{EAF749DC-CD87-4B04-B22A-D4AC3FBCB2BC}
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{EAF749DC-CD87-4B04-B22A-D4AC3FBCB2BC}\ProxyStubClsid
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{EAF749DC-CD87-4B04-B22A-D4AC3FBCB2BC}\ProxyStubClsid32
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{EAF749DC-CD87-4B04-B22A-D4AC3FBCB2BC}\TypeLib
[process 9]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Settings\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
[process 9]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}
[process 9]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\
[process 9]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\
[process 9]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\
[process 9]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\0x00000000\
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\iexplore
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\

[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37\CLSID

Deleted Keys	
	key
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}User
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine\Software
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine\Software\Policies
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine\Software\Policies\Google
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine\Software\Policies\Google\Chrome
[process 4]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects
[process 5]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List
[process 5]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0
[process 5]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPLink-List
[process 5]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPLink-List\0
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\InprocServer32
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\ProgID
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\Programmable
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\VersionIndependentProgID
[process 7]	\Registry\Machine\Software\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
[process 7]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\AppRovedExtensionsMigration\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
[process 7]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\AppRovedExtensionsMigration
[process 7]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\PreApproved\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
[process 9]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}
[process 9]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\0x00000000
[process 9]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile
[process 9]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-A

	BCDEFFEDCBB}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37\CLSID
[process 10]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37

Set Values	
	key
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur

	rentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Rpc Value: UuidSequenceNumber
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SessionInformation Value: ProgramCount
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SessionInformation Value: ProgramCount
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SessionInformation Value: ProgramCount
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SessionInformation Value: ProgramCount
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 4]	Key Name: \REGISTRY\MACHINE\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96} Value: ap
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Google\Update\ClientState\{4DC8B4CA-1BDA-483e-B5FA-D3C12E15B62D} Value: ap
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Policies\Google\Update Value: UpdateDefault
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG

	Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{23B27D25-22B3-4042-A1E7-9A8A69BAF748}Machine\Software\Policies\Google\Chrome Value: MetricsReportingEnabled
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 4]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: {FDB962F0-B5B8-9460-D12F-7966E97BAA43}
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine Value: Site-Name
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine Value: Distinguished-Name
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine Value: SlowLink
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0 Value: Version
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0 Value: WQLFilterPass
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0 Value: AccessDenied
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0 Value: GPO-Disabled
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0 Value: Options
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0 Value: GPOID
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0 Value: SOM
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0 Value: DisplayName
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO-List\0 Value: WQL-Id
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPLink-List\0 Value: Enabled

[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPLink-List\0 Value: NoOverride
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPLink-List\0 Value: DsPath
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPLink-List\0 Value: SOM
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Policies\Google\Chrome Value: MetricsReportingEnabled
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0 Value: Options
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0 Value: Version
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0 Value: DsPath
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0 Value: FileSysPath
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0 Value: DisplayName
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0 Value: Extensions
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0 Value: Link
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0 Value: GPOName
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0 Value: GPOLink
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\0 Value: lParam
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{35378EAC-683F-11D2-A89A-00C04FBBCFA2} Value: Status
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{35378EAC-683F-11D2-A89A-00C04FBBCFA2} Value: RsopStatus
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{35378EAC-683F-11D2-A89A-00C04FBBCFA2} Value: LastPolicyTime
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{3537

	8EAC-683F-11D2-A89A-00C04FBBCFA2} Value: PrevSlowLink
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{3537 8EAC-683F-11D2-A89A-00C04FBBCFA2} Value: PrevRsopLogging
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{3537 8EAC-683F-11D2-A89A-00C04FBBCFA2} Value: ForceRefreshFG
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Ext ension-List\{00000000-0000-0000-0000-000000000000} Value: StartTimeLo
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Ext ension-List\{00000000-0000-0000-0000-000000000000} Value: StartTimeHi
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Ext ension-List\{00000000-0000-0000-0000-000000000000} Value: EndTimeLo
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Ext ension-List\{00000000-0000-0000-0000-000000000000} Value: EndTimeHi
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Ext ension-List\{00000000-0000-0000-0000-000000000000} Value: Status
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Ext ension-List\{00000000-0000-0000-0000-000000000000} Value: LoggingStatus
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\RegisteredApplication sEx Value: 3dff8875531eb1d743dafe2cd3616c77
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur rentVersion\Explorer\Shell Folders Value: Local AppData
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur rentVersion\Explorer\Shell Folders Value: AppData
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
	Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
	Value: NoExplorer
[process 7]	Key Name: \Registry\Machine\Software\Classes\pRicechop.pRicechop.3.9
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\pRicechop.pRicechop.3.9\CLSID
	Value:
[process 7]	Key Name: \Registry\Machine\Software\Classes\pRicechop.pRicechop
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\pRicechop.pRicechop\CLSID
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\pRicechop.pRicechop\CurVer
	Value:
[process 7]	Key Name: \Registry\Machine\Software\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\ProgID
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\VersionIndependentProgID
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\InprocServer32
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\InprocServer32
	Value: ThreadingModel
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Ext\CLSID
	Value: {273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
[process 7]	Key Name: \Registry\Machine\Software\Classes\pRicechop.pRicechop.3.9
	Value:
[process 7]	Key Name: \Registry\Machine\Software\Classes\pRicechop.pRicechop
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\pRicechop.pRicechop\CLSID
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\pRicechop.pRicechop\CurVer
	Value:
[process 7]	Key Name: \Registry\Machine\Software\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\ProgID
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\InprocServer32
	Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\InprocServer32
	Value: ThreadingModel

[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{E2343056-CC08-46AC-B898-BFC7ACF4E755}\1.0 Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{E2343056-CC08-46AC-B898-BFC7ACF4E755}\1.0\FLAGS Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{E2343056-CC08-46AC-B898-BFC7ACF4E755}\1.0\0\win32 Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{E2343056-CC08-46AC-B898-BFC7ACF4E755}\1.0\HELPDIR Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{9B41579A-1996-42F9-8F84-7B7786818CEF} Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{9B41579A-1996-42F9-8F84-7B7786818CEF}\ProxyStubClsid Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{9B41579A-1996-42F9-8F84-7B7786818CEF}\ProxyStubClsid32 Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{9B41579A-1996-42F9-8F84-7B7786818CEF}\TypeLib Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{9B41579A-1996-42F9-8F84-7B7786818CEF}\TypeLib Value: Version
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{7041156A-0D2B-4DCD-A8EE-D0608BFCB2D0} Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{7041156A-0D2B-4DCD-A8EE-D0608BFCB2D0}\ProxyStubClsid Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{7041156A-0D2B-4DCD-A8EE-D0608BFCB2D0}\ProxyStubClsid32 Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{7041156A-0D2B-4DCD-A8EE-D0608BFCB2D0}\TypeLib Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{7041156A-0D2B-4DCD-A8EE-D0608BFCB2D0}\TypeLib Value: Version
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{EAF749DC-CD87-4B04-B22A-D4AC3FBCB2BC} Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{EAF749DC-CD87-4B04-B22A-D4AC3FBCB2BC}\ProxyStubClsid Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{EAF749DC-CD87-4B04-B22A-D4AC3FBCB2BC}\ProxyStubClsid32 Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{EAF749DC-CD87-4B04-B22A-D4AC3FBCB2BC}\TypeLib Value:
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\Interface\{EAF749DC-CD87-4B04-B22A-D4AC3FBCB2BC}\TypeLi

	b Value: Version
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: UninstallString
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: SilentUninstall
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: DisplayName
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: URLInfoAbout
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: URLUpdateInfo
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: Publisher
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: DisplayVersion
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: NoRepair
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: NoModify
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: CategoryName
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: InstallDate
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: DisplayIcon
[process 7]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FDB962F0-B5B8-9460-D12F-7966E97BAA43} Value: _In
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Desktop
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Settings\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763} Value: VerCache
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: CompatibilityFlags
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Favorites
[process 9]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

	Value: Local AppData
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Recovery\Active Value: {590C3E44-13D1-11E4-B96C-000C29B2D262}
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d} Value: Enable
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main\WindowsSearch Value: Version
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones Value: SecuritySafe
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur

	rentVersion\Explorer\MountPoints2\{874cd3ea-87a3-11e3-96b7-806d6172696f} Value: BaseClass
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur rentVersion\Explorer\MountPoints2\{874cd3e9-87a3-11e3-96b7-806d6172696f} Value: BaseClass
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur rentVersion\Explorer\MountPoints2\{874cd3e8-87a3-11e3-96b7-806d6172696f} Value: BaseClass
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{1EA4DBF0-3C3B-11CF-810C-00AA00389B71}\1.1\0\wi n32 Value:
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{1EA4DBF0-3C3B-11CF-810C-00AA00389B71}\1.1\0\wi n32 Value:
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur rentVersion\Explorer\Shell Folders Value: AppData
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore Value: Type
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore Value: Count
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore Value: Time
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore Value: Type
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore Value: Count
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore Value: Time
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore Value: Type
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore Value: Count
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore Value: Time
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ex plorer\Main Value: FullScreen
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ex plorer\Main Value: Window_Placement
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ex

	plorer\Main\WindowsSearch Value: Version
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Favorites\Links Value: Order
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: IE8RunOnceLastShown
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: IE8RunOnceLastShown_TIMESTAMP
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: FullScreen
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: Window_Placement
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Favorites
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{874cd3ea-87a3-11e3-96b7-806d6172696f} Value: BaseClass
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{874cd3e9-87a3-11e3-96b7-806d6172696f} Value: BaseClass
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{874cd3e8-87a3-11e3-96b7-806d6172696f} Value: BaseClass
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies

[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore Value: Type
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore Value: Count
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore Value: Time
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore Value: LoadTime
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore Value: LoadTimeCount
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\iexplore Value: Type
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\iexplore Value: Flags
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\iexplore Value: Count
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\iexplore Value: Time
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet

[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\iexplore Value: LoadTime
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{273025D6-61CB-CC3F-DEEC-8E3CEDAC7763}\iexplore Value: LoadTimeCount
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore Value: Type
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore Value: Count
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore Value: Time
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore Value: LoadTime
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore Value: LoadTimeCount
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore Value: Type
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore Value: Count
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore Value: Time
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA} Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32 Value:

[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32 Value: ThreadingModel
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB} Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32 Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32 Value: ThreadingModel
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC} Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32 Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32 Value: ThreadingModel
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA} Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32 Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32 Value: ThreadingModel
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93} Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32 Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32 Value: ThreadingModel
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37\CLSID Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{E7E6F031-17CE-4C07-BC86-EABFE594F69C}\iexplore Value: Type
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{E7E6F031-17CE-4C07-BC86-EABFE594F69C}\iexplore Value: Count
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{E7E6F031-17CE-4C07-BC86-EABFE594F69C}\iexplore Value: Time

[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{E7E6F031-17CE-4C07-BC86-EABFE594F69C}\iexplore Value: LoadTime
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{E7E6F031-17CE-4C07-BC86-EABFE594F69C}\iexplore Value: LoadTimeCount
[process 10]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings

Deleted Values	
	key
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LowRegistry Value: AddToFavoritesInitialSelection
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ex

plorer\LowRegistry
Value: AddToFeedsInitialSelection

Network Events

	Remote IP	Local IP	HTTP Command
[process 1]	54.191.92.23	10.20.25.250	POST /?report_version=5&
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=1&installer_id=375548921664154926 3&publisher_id=3252&source_id=0&page_id=0&affiliate_id=0&country_code=GB&locale=EN&browser_id=2&download_id=2444794351920115825&external_id=0&session_id=1572398332807219066 2&hardware_id=11366129688198888681&installer_file_name=Blended&filesize=&product_name=Your+File&uuid=%252A
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=2_0&installer_id=375548921664154926 3&publisher_id=3252&source_id=0&page_id=0&affiliate_id=0&country_code=GB&locale=EN&browser_id=2&download_id=2444794351920115825&external_id=0&session_id=1572398332807219066 2&hardware_id=11366129688198888681&installer_file_name=Blended&filesize=&product_name=Your+File&uuid=%252A
[process 1]	198.7.61.118	10.20.25.250	GET /images/general_logo.bmp
[process 1]	198.7.61.118	10.20.25.250	GET /images/v_grey.jpg
[process 1]	198.7.61.118	10.20.25.250	GET /images/v_grey.jpg
[process 1]	198.7.61.118	10.20.25.250	GET /images/v_grey.jpg POST /private/sandbox_status.php
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=4&installer_id=375548921664154926 3&publisher_id=3252&source_id=0&page_id=0&affiliate_id=0&country_code=GB&locale=EN&browser_id=2&download_id=2444794351920115825&external_id=0&session_id=1572398332807219066 2&hardware_id=11366129688198888681&installer_file_name=Blended&filesize=&product_name=Your+File&uuid=%252A
[process 1]	198.7.61.118	10.20.25.250	GET /images/general_logo.bmp
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=4_2&installer_id=375548921664154926 3&publisher_id=3252&source_id=0&page_id=0&affiliate_id=0&country_code=GB&locale=EN&browser_id=2&download_id=2444794351920115825&external_id=0&session_id=1572398332807219066 2&hardware_id=11366129688198888681&installer_file_name=Blended&filesize=&product_name=Your+File&uuid=%252A
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=4_3&installer_id=375548921664154926 3&publisher_id=3252&source_id=0&page_id=0&affiliate_id=

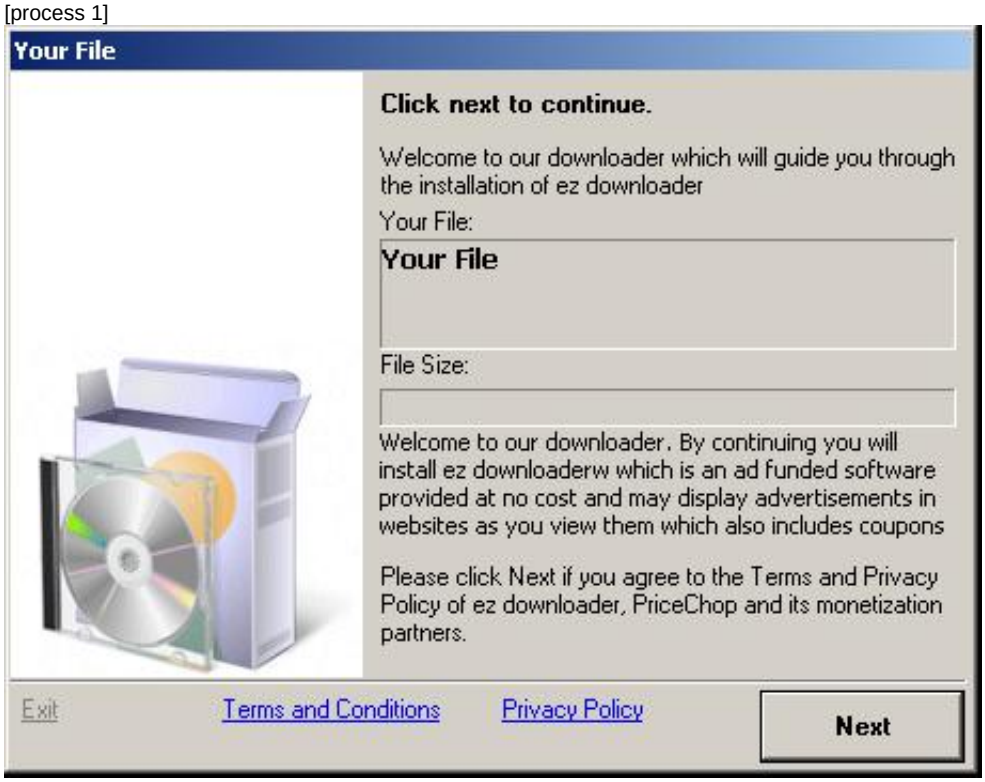
			0&country_code=GB&locale=EN&browser_id=2&download_ id=2444794351920115825&external_id=0&session_id=15 723983328072190662&hardware_id=1136612968819888868 1&installer_file_name=Blended&filesize=&product_na me=Your+File&uuid=%252A
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=5&installer_id=3755489216641549263&publi sher_id=3252&source_id=0&page_id=0&affiliate_id=0& country_code=GB&locale=EN&browser_id=2&download_id =2444794351920115825&external_id=0&session_id=1572 3983328072190662&hardware_id=11366129688198888681& installer_file_name=Blended&filesize=&product_name =Your+File&uuid=%252A
[process 1]	198.7.61.118	10.20.25.250	GET /images/general_logo.bmp
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=5_1&installer_id=3755489216641549263&pub lisher_id=3252&source_id=0&page_id=0&affiliate_id= 0&country_code=GB&locale=EN&browser_id=2&download_ id=2444794351920115825&external_id=0&session_id=15 723983328072190662&hardware_id=1136612968819888868 1&installer_file_name=Blended&filesize=&product_na me=Your+File&uuid=%252A
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=6&installer_id=3755489216641549263&publi sher_id=3252&source_id=0&page_id=0&affiliate_id=0& country_code=GB&locale=EN&browser_id=2&download_id =2444794351920115825&external_id=0&session_id=1572 3983328072190662&hardware_id=11366129688198888681& installer_file_name=Blended&filesize=&product_name =Your+File&uuid=%252A
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=6_1&installer_id=3755489216641549263&pub lisher_id=3252&source_id=0&page_id=0&affiliate_id= 0&country_code=GB&locale=EN&browser_id=2&download_ id=2444794351920115825&external_id=0&session_id=15 723983328072190662&hardware_id=1136612968819888868 1&installer_file_name=Blended&filesize=&product_na me=Your+File&uuid=%252A
[process 1]	54.187.243.98	10.20.25.250	GET /?e=pcho&cht=2&dcu=1&cpatch=2&dcs=1&pf=1&unp=Azm9C dOLv7DVDyxECyFPg7x9Ae0KBfUKAe4MBG0VWznLDe4PBNq9geF I&publisher=3252&dd=4&country=GB&ind=3755489216641 549263&exid=0&ssd=1572398332807219066 2&hid=1136612 9688198888681&osid=501&channel=0&sfx=1&jc=1&catego ry_name=PriceChop2&install_date=20130725 GET /?e=pcho&unp=Azm9CdOLv7DVDyxECyFPg7x9Ae0KBfUKAe4MB G0VWznLDe4PBNq9geFI&publisher=3252&dd=3&country=GB &ind=3755489216641549263&exid=0&ssd=15723983328072 190662&hid=11366129688198888681&osid=501&channel=0

			&sfx=1&jc=1&utid=3&category_name=PriceChopIE&insta ll_date=20130725
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=6_1_0&installer_id=3755489216641549263&p ublisher_id=3252&source_id=0&page_id=0&affiliate_i d=0&country_code=GB&locale=EN&browser_id=2&downloa d_id=2444794351920115825&external_id=0&session_id= 1572398332807219066 2&hardware_id=11366129688198888 681&installer_file_name=Blended&filesize=&product_ name=Your+File&uuid=%252A
[process 1]	54.191.92.197	10.20.25.250	GET /?step_id=6_1_3&installer_id=3755489216641549263&p ublisher_id=3252&source_id=0&page_id=0&affiliate_i d=0&country_code=GB&locale=EN&browser_id=2&downloa d_id=2444794351920115825&external_id=0&session_id= 1572398332807219066 2&hardware_id=11366129688198888 681&installer_file_name=Blended&filesize=&product_ name=Your+File&uuid=%252A
[process 10]	127.0.0.1	0.0.0.0	none
[process 10]	95.211.187.165	10.20.25.250	GET /sync/?q=hfZ9ofbTAy1MCyVUojrGqjsMg708BNmGWj8lkGhGh eDUojw9rdCGqja6qjCGrGhPBMn0rHC8qjn5pjsFqTg9rjk9pjs 7rGhHC7n0rjk6rTr4pdrHrTYEqHsFpja7qTsMDMlGojUMAe4HD d9HtM0HAen0qjaFtMZPhd9Frjr7qTwGpjg5pdw4pdY5pdg5rih SCH9FtNZKge8VofbGAeqVg7ZLCa%3D%3D&rmbs=1&jsoncallb ack=getjson
[process 10]	127.0.0.1	127.0.0.1	none

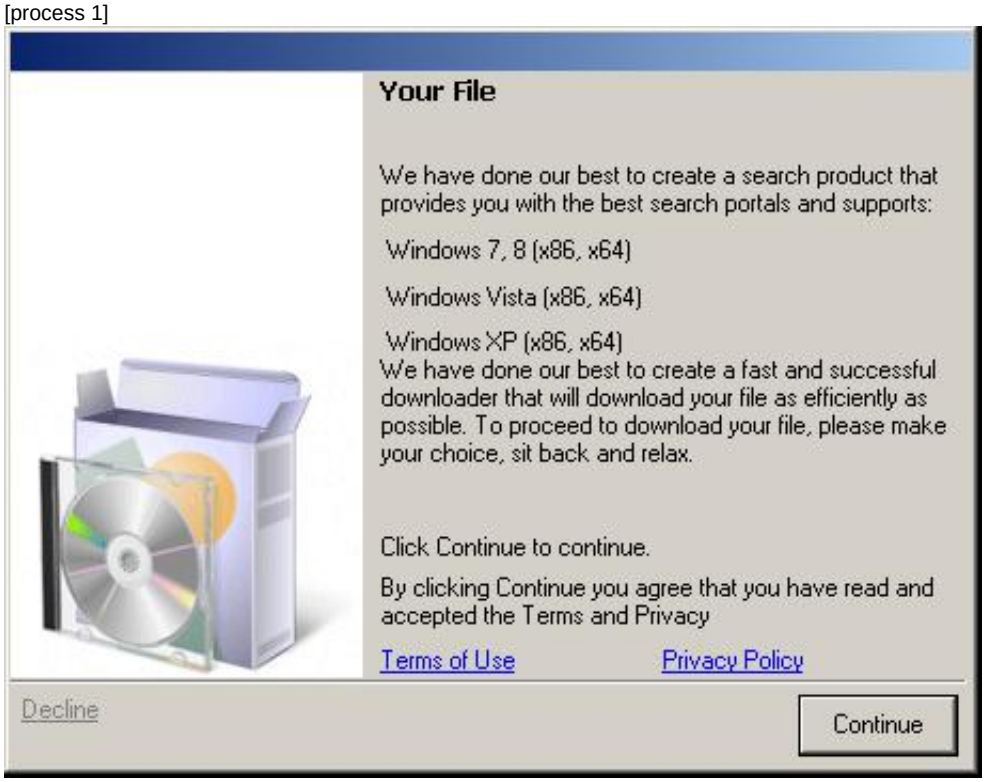
Network Traffic		
	Remote IP	**Local IP**
Connection #1	10.20.25.255	10.20.25.250

DNS Requests	
Request	**Result**
r1.homebestmy.info	54.191.92.23
	54.191.92.197
c1.setepicnew.info	54.191.92.197
	54.191.92.23
i1.superstoragemy.com	198.7.61.118
getdottamy.info	54.187.243.98
getyouraddon.co.il	95.211.187.165
	91.109.18.39

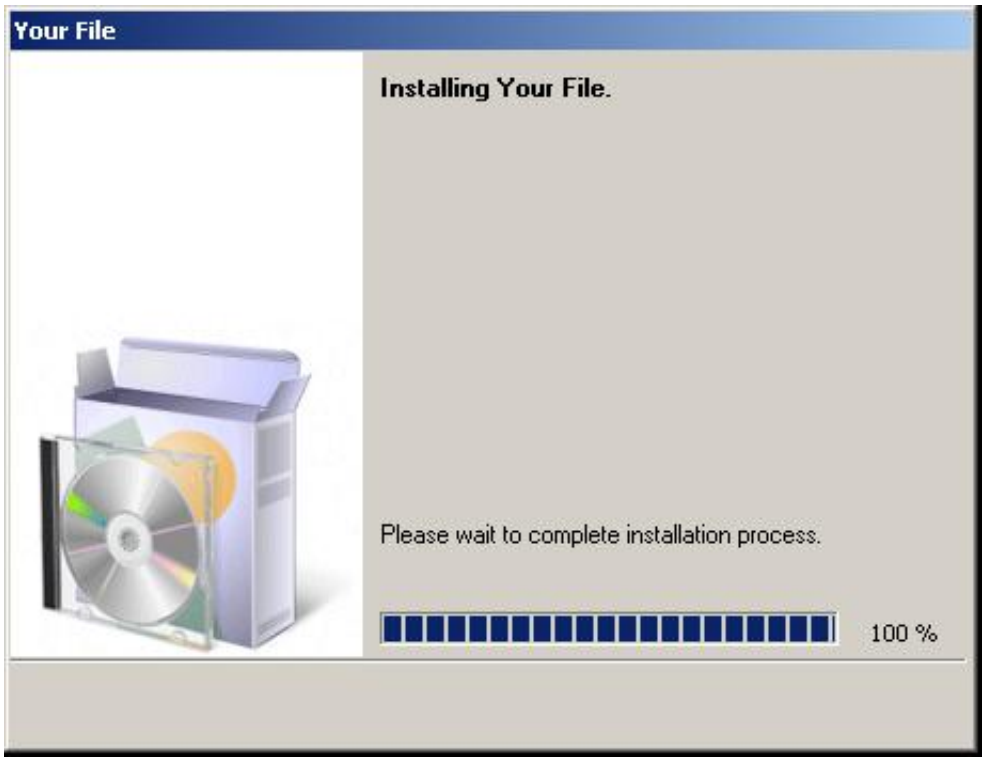
[process 1]



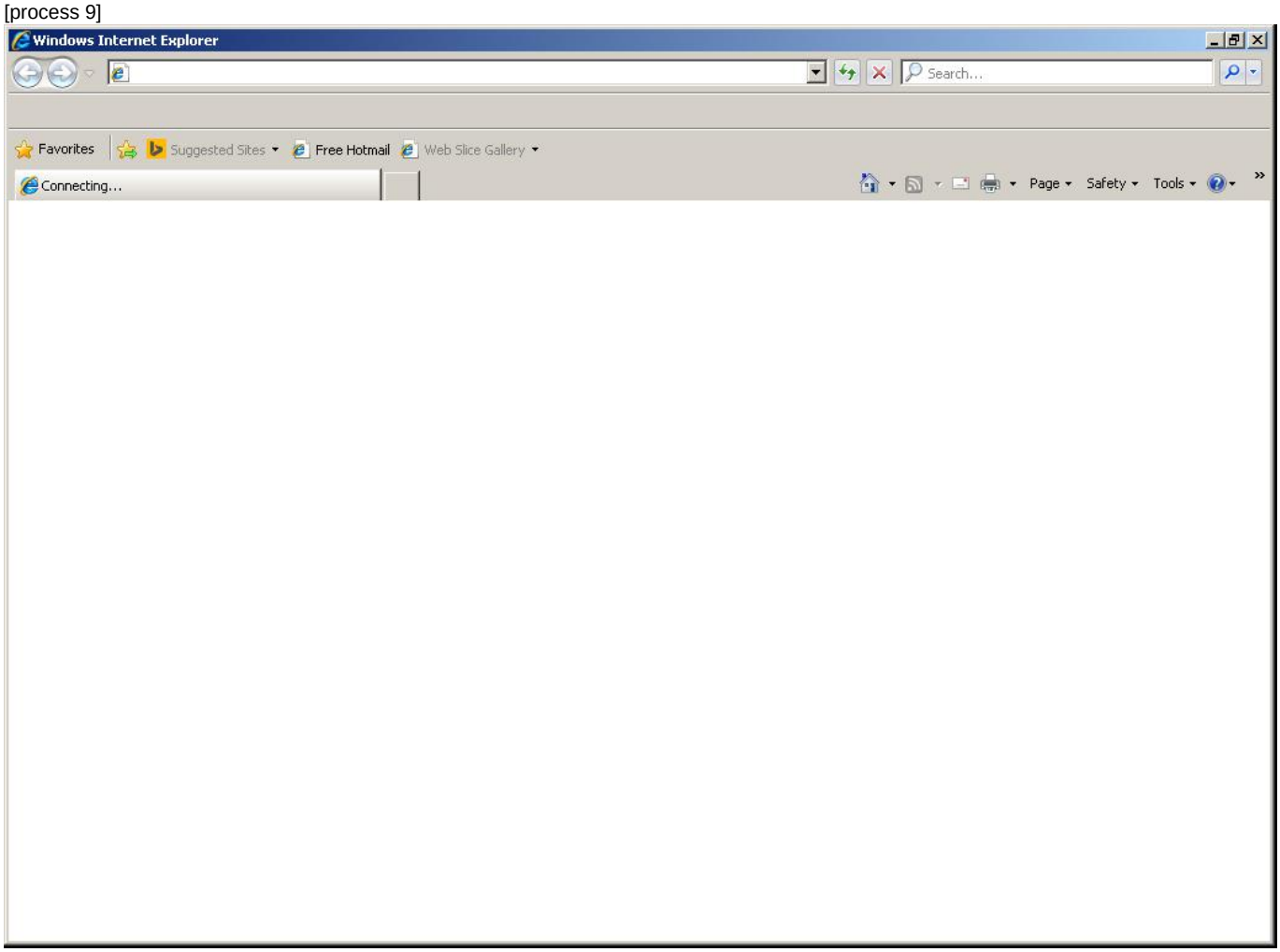
[process 1]



[process 1]



[process 9]



[process 9]

Virus Total Results	
Last Scanned:	**2014-07-25 07:43:55**
Bkav:	W32.FamVT.AntiFWK.Trojan
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Trojan.AntiFW.A5
McAfee:	Not Detected
Malwarebytes:	Not Detected
TheHacker:	Not Detected
K7GW:	Not Detected
K7AntiVirus:	Not Detected
NANO-Antivirus:	Riskware.Win32.InfoLeak.cvgqot
F-Prot:	Not Detected
Symantec:	Not Detected
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Trojan.Win32.AntiFW.b
BitDefender:	Not Detected
Agnitum:	Not Detected
ViRobot:	Not Detected
SUPERAntiSpyware:	Not Detected
ByteHero:	Not Detected
Tencent:	Not Detected
Ad-Aware:	Not Detected
Emsisoft:	Not Detected
Comodo:	Application.Win32.InstalleRex.KG
F-Secure:	Not Detected
VIPRE:	Trojan.Win32.Generic!BT
AntiVir:	Adware/MultiPlug.aob
TrendMicro:	Not Detected
McAfee-GW-Edition:	Not Detected
Sophos:	MultiPlug
Jiangmin:	Not Detected
Antiy-AVL:	Trojan/Win32.AntiFW.b
Kingsoft:	Win32.Troj.AntiFW.b.(kcloud)
Microsoft:	Not Detected
AegisLab:	Not Detected
GData:	Win32.Application.InstalleRex.E
Commtouch:	Not Detected
AhnLab-V3:	Not Detected
VBA32:	Downware.TSU
Baidu-International:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	Win32/InstalleRex.M
Rising:	Not Detected
Ikarus:	AdWare.SaveNet
Fortinet:	Not Detected
AVG:	Generic.8FD
Panda:	PUP/TSUploader
Qihoo-360:	Malware.QVM20.Gen

ThreatTrack Security, Inc.
33 North Garden Avenue, Suite 1200, Clearwater, Florida, USA 33755
Telephone: (855) 443-4284 Intl: +1(813)367-9907
Email: Sales@ThreatTrack.com