Analysis # 2567

09/11/2014 16:36 pm

Table of Contents

Analysis Summary

Submitted File:	Documents___Copy.exe
MD5:	79b1f47c0dfd99f974d2920a381ad91f
File Size:	22528
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-09-11 16:36:44
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Fri, 12 Sep 2014 01:41:21 +0000
Termination Time:	Fri, 12 Sep 2014 01:42:22 +0000
Analysis Time:	2014-09-11 16:36:44
Sandbox:	XP-SP2 - 00-0C-29-B2-D2-62
Total Processes:	14
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 2] C:\Documents___Copy.exe
[process 5] C:\DOCUME~1\Charlie\LOCALS~1\Temp\kdbql.exe
[process 6] C:\Documents and Settings\All Users\Application Data\Microsoft\OFFICE\DATA\OPA11.BAK.70v
[process 6] C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.b ak.52n
[process 6] C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.t xt.kz9
[process 6] C:\Documents and Settings\Charlie\Cookies\charlie@c1.microsoft[2].txt.mj9
[process 6] C:\Documents and Settings\Charlie\Cookies\charlie@microsoft[1].txt.945
[process 6] C:\Documents and Settings\Charlie\Cookies\charlie@track.monitis[2].txt.5bn
[process 6] C:\Documents and Settings\Charlie\Cookies\charlie@www.microsoft[2].txt.9yc
[process 6] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Exp lorer\brndlog.txt.5r9
[process 6] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Outlook\Outl ook.pst.l34
[process 6] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Windows Medi a\9.0\WMSDKNS.DTD.w4u
[process 6] C:\Documents and Settings\Charlie\Templates\excel.xls.fd1
[process 6] C:\Documents and Settings\Charlie\Templates\excel4.xls.jx2
[process 6] C:\Documents and Settings\Charlie\Templates\powerpnt.ppt.31m
[process 6] C:\Documents and Settings\Charlie\Templates\quattro.wb2.q3b
[process 6] C:\Documents and Settings\Charlie\Templates\sndrec.wav.wq5
[process 6] C:\Documents and Settings\Charlie\Templates\winword.doc.i69
[process 6] C:\Documents and Settings\Charlie\Templates\winword2.doc.h3z
[process 6] C:\Documents and Settings\Charlie\Templates\wordpfct.wpd.kn0
[process 6] C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brnd log.bak.7ss
[process 6] C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brnd log.txt.xe7
[process 6] C:\Documents and Settings\Default User\Local Settings\Application Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD.b9w
[process 6] C:\Documents and Settings\Default User\Templates\excel.xls.8ic
[process 6] C:\Documents and Settings\Default User\Templates\excel4.xls.99j
[process 6] C:\Documents and Settings\Default User\Templates\powerpnt.ppt.n18
[process 6] C:\Documents and Settings\Default User\Templates\quattro.wb2.ek4
[process 6] C:\Documents and Settings\Default User\Templates\sndrec.wav.4j3
[process 6] C:\Documents and Settings\Default User\Templates\winword.doc.k21
[process 6] C:\Documents and Settings\Default User\Templates\winword2.doc.m1a
[process 6] C:\Documents and Settings\Default User\Templates\wordpfct.wpd.9qt
[process 6] C:\Documents and Settings\Charlie\Start Menu\Programs\Startup\0d50b3f.exe
[process 6] C:\Documents and Settings\Charlie\Application Data\0d50b3f.exe
[process 6] C:\0d50b3f\0d50b3f.exe
[process 6] C:\0d50b3f
[process 15] C:\Documents and Settings\Charlie\Local Settings\History\History.IE5\MSHist012014012820 140129\index.dat
[process 15] C:\Documents and Settings\Charlie\Local Settings\History\History.IE5\MSHist012014012820 140129
[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Cab1.tmp
[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Tar2.tmp
[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Cab3.tmp

[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Tar4.tmp
[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Cab5.tmp
[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Tar6.tmp

Stored Modified Files
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\zcrjc.exe
[process 2] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4 O5PO1W\install2[1].tar
[process 2] C:\DOCUME~1\Charlie\LOCALS~1\Temp\kdbql.exe
[process 6] C:\Documents and Settings\All Users\Application Data\Microsoft\OFFICE\DATA\OPA11.BAK.70v
[process 6] C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.b ak.52n
[process 6] C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.t xt.kz9
[process 6] C:\Documents and Settings\Charlie\Cookies\charlie@c1.microsoft[2].txt.mj9
[process 6] C:\Documents and Settings\Charlie\Cookies\charlie@microsoft[1].txt.945
[process 6] C:\Documents and Settings\Charlie\Cookies\charlie@track.monitis[2].txt.5bn
[process 6] C:\Documents and Settings\Charlie\Cookies\charlie@www.microsoft[2].txt.9yc
[process 6] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Exp lorer\brndlog.txt.5r9
[process 6] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Outlook\Outl ook.pst.l34
[process 6] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Windows Medi a\9.0\WMSDKNS.DTD.w4u
[process 6] C:\Documents and Settings\Charlie\Templates\excel.xls.fd1
[process 6] C:\Documents and Settings\Charlie\Templates\excel4.xls.jx2
[process 6] C:\Documents and Settings\Charlie\Templates\powerpnt.ppt.31m
[process 6] C:\Documents and Settings\Charlie\Templates\quattro.wb2.q3b
[process 6] C:\Documents and Settings\Charlie\Templates\sndrec.wav.wq5
[process 6] C:\Documents and Settings\Charlie\Templates\winword.doc.i69
[process 6] C:\Documents and Settings\Charlie\Templates\winword2.doc.h3z
[process 6] C:\Documents and Settings\Charlie\Templates\wordpfct.wpd.kn0
[process 6] C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brnd log.bak.7ss
[process 6] C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brnd log.txt.xe7
[process 6] C:\Documents and Settings\Default User\Local Settings\Application Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD.b9w
[process 6] C:\Documents and Settings\Default User\Templates\excel.xls.8ic
[process 6] C:\Documents and Settings\Default User\Templates\excel4.xls.99j
[process 6] C:\Documents and Settings\Default User\Templates\powerpnt.ppt.n18
[process 6] C:\Documents and Settings\Default User\Templates\quattro.wb2.ek4
[process 6] C:\Documents and Settings\Default User\Templates\sndrec.wav.4j3
[process 6] C:\Documents and Settings\Default User\Templates\winword.doc.k21
[process 6] C:\Documents and Settings\Default User\Templates\winword2.doc.m1a
[process 6] C:\Documents and Settings\Default User\Templates\wordpfct.wpd.9qt
[process 9] C:\WINDOWS\system32\stubyoyn.exe
[process 9] C:\Documents and Settings\Charlie\stubyoyn.exe
[process 15] C:\Documents and Settings\Charlie\Local Settings\History\History.IE5\MSHist012014091120 140912\index.dat
[process 15] C:\Documents and Settings\Charlie\Application Data\Microsoft\CryptnetUrlCache\Content\0 A873D20E943287602D5D327C5CA3D2F
[process 15] C:\Documents and Settings\Charlie\Application Data\Microsoft\CryptnetUrlCache\MetaData\ 0A873D20E943287602D5D327C5CA3D2F
[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Cab1.tmp

[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Tar2.tmp
[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Cab3.tmp
[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Tar4.tmp
[process 15] C:\Documents and Settings\Charlie\Application Data\Microsoft\CryptnetUrlCache\Content\2 BF68F4714092295550497DD56F57004
[process 15] C:\Documents and Settings\Charlie\Application Data\Microsoft\CryptnetUrlCache\MetaData\ 2BF68F4714092295550497DD56F57004
[process 15] C:\Documents and Settings\Charlie\Application Data\Microsoft\CryptnetUrlCache\Content\9 4308059B57B3142E455B38A6EB92015
[process 15] C:\Documents and Settings\Charlie\Application Data\Microsoft\CryptnetUrlCache\MetaData\ 94308059B57B3142E455B38A6EB92015
[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Cab5.tmp
[process 15] C:\DOCUME~1\Charlie\LOCALS~1\Temp\Tar6.tmp
[process 15] C:\Documents and Settings\Charlie\Application Data\Microsoft\CryptnetUrlCache\Content\C 8E7EC0C85688F4738F3BE49B104BA67
[process 15] C:\Documents and Settings\Charlie\Application Data\Microsoft\CryptnetUrlCache\MetaData\ C8E7EC0C85688F4738F3BE49B104BA67
[process 15] C:\Documents and Settings\Charlie\Application Data\Microsoft\CryptnetUrlCache\Content\D 88A43F72E2F70CB75791302DD65CDE7
[process 15] C:\Documents and Settings\Charlie\Application Data\Microsoft\CryptnetUrlCache\MetaData\ D88A43F72E2F70CB75791302DD65CDE7
[process 15] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Ex plorer\MSIMGSIZ.DAT

Created Mutexes	
	mutex
[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\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 2]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	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 2]	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 2]	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 2]	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 2]	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 2]	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 2]	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 2]	Name: Local\c:!documents and settings!charlie!cookies!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	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 2]	Name: Local\WininetConnectionMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZonesCacheCounterMutex

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	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 6]	Name: Local\c:!documents and settings!charlie!cookies!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	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 6]	Name: Local\WininetConnectionMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Local\ZonesCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	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 6]	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 6]	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 6]	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 6]	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 7]	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: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: CTR.F981AEF7D8944523
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	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 11]	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 11]	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 11]	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 11]	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 12]	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 12]	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 12]	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 12]	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 12]	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 12]	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 12]	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 12]	Name: Local\!BrowserEmulation!SharedMemory!Mutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: ConnHashTable<524>_HashTable_Mutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Local\ZonesCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: oleacc-msaa-loaded
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Local\RSS Eventing Connection Database Mutex 0000020c
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Local\Feed Arbitration Shared Memory Mutex [User : S-1-5-21-602162358-879983540-1177238915-10 03]
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 13]	Name: Local\Feeds Store Mutex S-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 13]	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 13]	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 13]	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 13]	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 13]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 15]	Name: Local\ZonesCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 15]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 15]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 15]	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 15]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 15]	Name: Local\!PrivacIE!SharedMemory!Mutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 15]	Name: _!SHMSFTHISTORY!_
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 15]	Name: Local\c:!documents and settings!charlie!local settings!history!history.ie5!mshist0120140911201
	40912!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 6]	\Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE
[process 6]	\Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF
[process 11]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Notepad
[process 12]	\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 12]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\
[process 12]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\
[process 12]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\
[process 12]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\0x00000000\
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37\CLSID
[process 15]	\REGISTRY\MACHINE\SOFTWARE\Classes\.mhtml\OpenWithList\WINWORD.EXE
[process 15]	\REGISTRY\MACHINE\SOFTWARE\Classes\.mhtml\
[process 15]	\REGISTRY\MACHINE\SOFTWARE\Classes\.mhtml\OpenWithList\
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012014091120140912
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\SystemCertificates\CA\Certificates\5824CF32C3CC2A47443DB10A33BBE3AC8DE524E1

Deleted Keys	
	key
[process 12]	\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 12]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\0x00000000
[process 12]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile
[process 12]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37\CLSID
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-0

	0805F499D93}
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37\CLSID
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37
[process 15]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012014012820140129

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: Personal
[process 1]	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 1]	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 1]	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 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common Documents
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Desktop
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common Desktop
[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\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\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\ShellNoRoam\MUICache Value: C:\DOCUME~1\Charlie\LOCALS~1\Temp\zcrjc.exe
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 2]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings

	Value: ProxyEnable
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections
	Value: SavedLegacySettings
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: ProxyBypass
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: IntranetName
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: UNCAsIntranet
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: AutoDetect
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: ProxyBypass
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: IntranetName
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: UNCAsIntranet
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: AutoDetect
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings
	Value: ProxyEnable
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections
	Value: SavedLegacySettings
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
	Value: Personal
[process 2]	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 2]	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 2]	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 2]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
	Value: Common Documents
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
	Value: Desktop

[process 2]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common Desktop
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache Value: C:\DOCUME~1\Charlie\LOCALS~1\Temp\kdbql.exe
[process 3]	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\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: 0d50b3
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: 0d50b3f
[process 5]	Key Name: \Registry\Machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore Value: DisableSR
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 6]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur

	rentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE Value: da
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE Value: 5b
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE Value: 0c
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE Value: bd
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\All Users\Application Data\Microsoft\OFFICE\DATA\OPA11.BAK
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21

	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.bak
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.txt
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur
	rentVersion\Explorer\Shell Folders
	Value: AppData
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Cookies\charlie@c1.microsoft[2].txt
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Cookies\charlie@microsoft[1].txt
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Cookies\charlie@track.monitis[2].txt
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Cookies\charlie@www.microsoft[2].txt
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Explorer
	\brndlog.txt
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur
	rentVersion\Explorer\Shell Folders
	Value: AppData
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Outlook\Outlook.p
	st
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Windows Media\9.0
	\WMSDKNS.DTD
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Templates\excel.xls
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Templates\excel4.xls
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Templates\powerpnt.ppt
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Templates\quattro.wb2
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21
	B82457869AE\01224567889ABEEF
	Value: C:\Documents and Settings\Charlie\Templates\sndrec.wav
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21

	B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\winword.doc
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\winword2.doc
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\wordpfct.wpd
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brndlog.b ak
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brndlog.t xt
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Local Settings\Application Data\Microsoft\Windows Medi a\9.0\WMSDKNS.DTD
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\excel.xls
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\excel4.xls
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\powerpnt.ppt
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\quattro.wb2
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\sndrec.wav
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\winword.doc
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\winword2.doc
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21 B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\wordpfct.wpd
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur rentVersion\Explorer\Shell Folders Value: Personal
[process 6]	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 6]	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 6]	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 6]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common Documents
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Desktop
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache Value: C:\WINDOWS\system32\notepad.exe
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached Value: {FBF23B40-E3F0-101B-8488-00AA003E56F8} {000214E8-0000-0000-C000-000000000046} 0x401
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\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\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG

	Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Value: stubyoyn
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: stubyoyn
[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 11]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

	Value: Desktop
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: CompatibilityFlags
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Favorites
[process 12]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Recovery\Active Value: {F9BBBB13-3A1D-11E4-B96B-000C29B2D262}
[process 12]	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 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main\WindowsSearch Value: Version
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

	Value: UNCAsIntranet
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: AutoDetect
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: ProxyBypass
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: IntranetName
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: UNCAsIntranet
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
	Value: AutoDetect
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
	Value: SecuritySafe
[process 12]	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 12]	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 12]	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 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{1EA4DBF0-3C3B-11CF-810C-00AA00389B71}\1.1\0\win32
	Value:
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{1EA4DBF0-3C3B-11CF-810C-00AA00389B71}\1.1\0\win32
	Value:
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
	Value: AppData
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore
	Value: Type
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore
	Value: Count
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore
	Value: Time
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore
	Value: Type
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore

	Value: Count
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore
	Value: Time
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore
	Value: Type
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore
	Value: Count
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore
	Value: Time
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main
	Value: FullScreen
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main
	Value: Window_Placement
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Favorites\Links
	Value: Order
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main
	Value: IE8RunOnceLastShown
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main
	Value: IE8RunOnceLastShown_TIMESTAMP
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0
	Value: Path
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0
	Value: Handler
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0
	Value: FeedUrl
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0
	Value: DisplayName
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0
	Value: ErrorState
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0
	Value: DisplayMask
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1
	Value: Path
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1

	Value: Handler
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: FeedUrl
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: DisplayName
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: ErrorState
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: DisplayMask
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: DisplayName
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: DisplayMask
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: ErrorState
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: Expiration
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: DisplayName
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: DisplayMask
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: ErrorState
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: Expiration
[process 13]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 13]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 13]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 13]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 13]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 13]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 13]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

[process 13]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Favorites
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 15]	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 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	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 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}
	Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32
	Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32
	Value: ThreadingModel
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}
	Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32
	Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32
	Value: ThreadingModel
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}
	Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32
	Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32
	Value: ThreadingModel
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}
	Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32
	Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32
	Value: ThreadingModel
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}
	Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32
	Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32
	Value: ThreadingModel
[process 15]	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 15]	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 15]	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 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37\CLSID Value:
[process 15]	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 15]	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 15]	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 15]	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 15]	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 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA} Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32 Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBA}\InprocServer32 Value: ThreadingModel
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB} Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32 Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBB}\InprocServer32 Value: ThreadingModel
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC} Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32 Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-0037-ABCDEFFEDCBC}\InprocServer32 Value: ThreadingModel

[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA} Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32 Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{CAFEEFAC-0016-0000-FFFF-ABCDEFFEDCBA}\InprocServer32 Value: ThreadingModel
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93} Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32 Value:
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32 Value: ThreadingModel
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003_CLASSES\JavaPlugin.160_37\CLSID Value:
[process 15]	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 15]	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 15]	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 15]	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 15]	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 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass

[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 15]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 15]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Internet Explorer\Default MHTML Editor Value: Last
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012014091120140912 Value: CachePath
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012014091120140912 Value: CachePrefix
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012014091120140912 Value: CacheLimit
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012014091120140912 Value: CacheOptions
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012014091120140912 Value: CachePath
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012014091120140912

	Value: CacheRepair
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main\WindowsSearch
	Value: Version
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\Certificates\E5215D3460C2C20BBE2D9FE5FB665DAA2C0E225C
	Value: Blob
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\02FAF3E291435468607857694DF5E45B68851868
	Value: Blob
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\SystemCertificates\CA\Certificates\5824CF32C3CC2A47443DB10A33BBE3AC8DE524E1
	Value: Blob
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
	Value: Local AppData
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\B1BC968BD4F49D622AA89A81F2150152A41D829C
	Value: Blob
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\B1BC968BD4F49D622AA89A81F2150152A41D829C
	Value: Blob

Deleted Values	
	key
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE Value: da
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE Value: 5b
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE Value: 0c
[process 6]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE Value: bd
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur

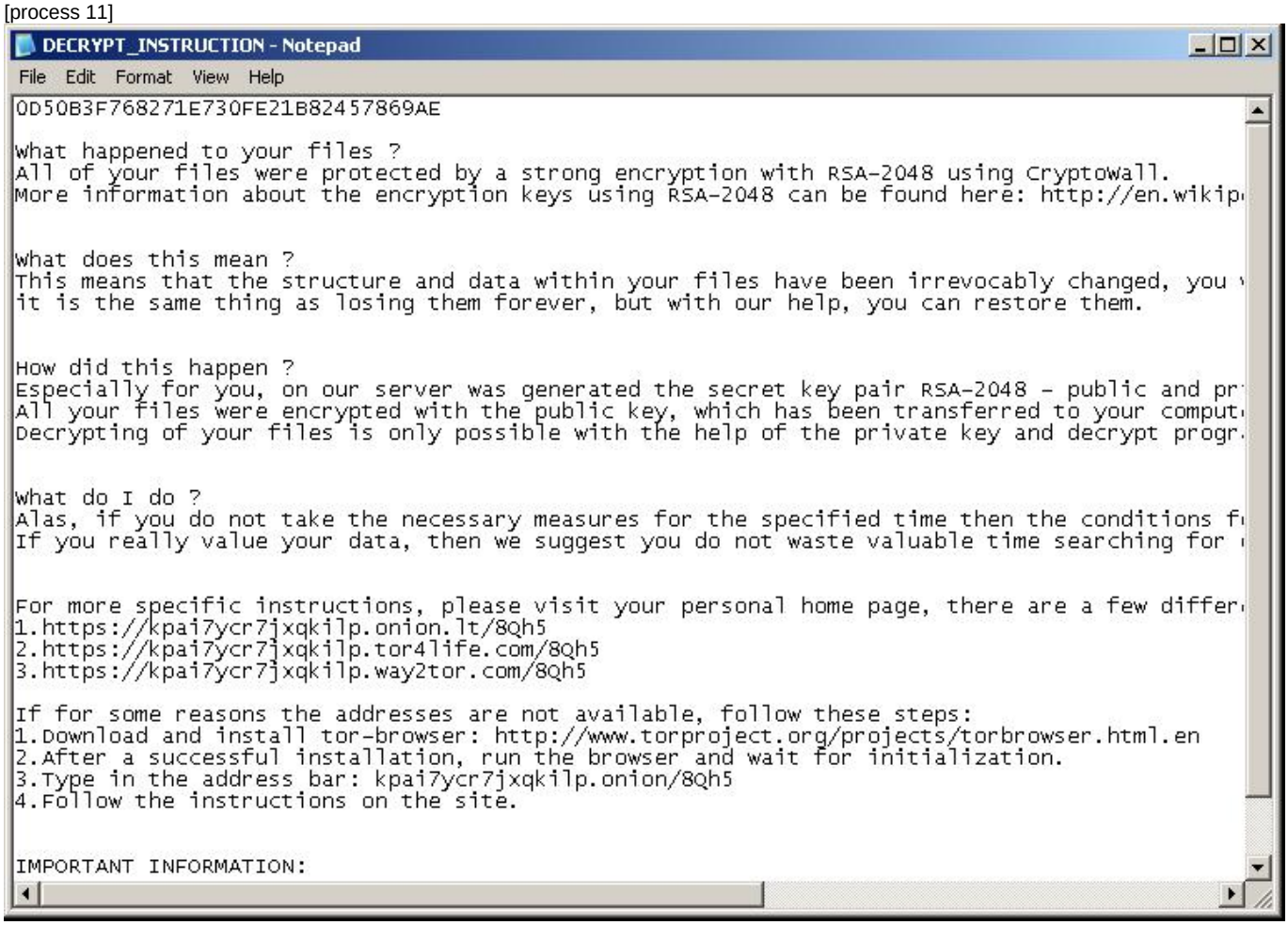
	rentVersion\Run Value: 0d50b3f
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: 0d50b3
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: Expiration
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: Expiration
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\Certificates Value: E5215D3460C2C20BBE2D9FE5FB665DAA2C0E225C
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates Value: 02FAF3E291435468607857694DF5E45B68851868
[process 15]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\SystemCertificates\CA\Certificates Value: 5824CF32C3CC2A47443DB10A33BBE3AC8DE524E1
[process 15]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates Value: B1BC968BD4F49D622AA89A81F2150152A41D829C

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process 2]	188.165.204.210	10.20.25.250	GET /1109inst2/NODE01/0/51-SP3/0/
[process 2]	188.165.204.210	10.20.25.250	GET /1109inst2/NODE01/1/0/0/
[process 2]	46.151.145.11	10.20.25.250	GET /files/3/install2.tar
[process 2]	188.165.204.210	10.20.25.250	GET /1109inst2/NODE01/41/5/4/
[process 6]	76.74.170.149	10.20.25.250	POST /87n3hdh5wi04gy
[process 6]	76.74.170.149	10.20.25.250	POST /i12c4y0w5394m9
[process 6]	76.74.170.149	10.20.25.250	POST /ttfvku8z7jn
[process 6]	50.63.85.76	10.20.25.250	GET /wp-content/themes/twentyeleven/111.exe
[process 6]	76.74.170.149	10.20.25.250	POST /zg27ug498b3
[process 6]	76.74.170.149	10.20.25.250	POST /gwfqwaratrpl2c
[process 6]	76.74.170.149	10.20.25.250	POST /h0nxfsskh0xu
[process 6]	76.74.170.149	10.20.25.250	POST /kvlfhc0hjgo6sgo
[process 10]	193.169.86.151	10.20.25.250	none
[process 10]	193.19.184.20	10.20.25.250	none
[process 15]	127.0.0.1	0.0.0.0	none
[process 15]	127.0.0.1	0.0.0.0	none
[process 15]	82.94.251.220	10.20.25.250	none
[process 15]	127.0.0.1	127.0.0.1	none
[process 15]	141.101.115.22	10.20.25.250	GET /cacert/gsalphag2.crt
[process 15]	198.172.136.43	10.20.25.250	GET /msdownload/update/v3/static/trustedr/en/authrootseq.txt GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab GET /msdownload/update/v3/static/trustedr/en/B1BC968BD4F49D622AA89A81F2150152A41D829C.crt
[process 15]	108.162.232.196	10.20.25.250	GET /root.crl
[process 15]	190.93.247.21	10.20.25.250	GET /gs/gsalphag2.crl
[process 15]	82.94.251.220	10.20.25.250	none

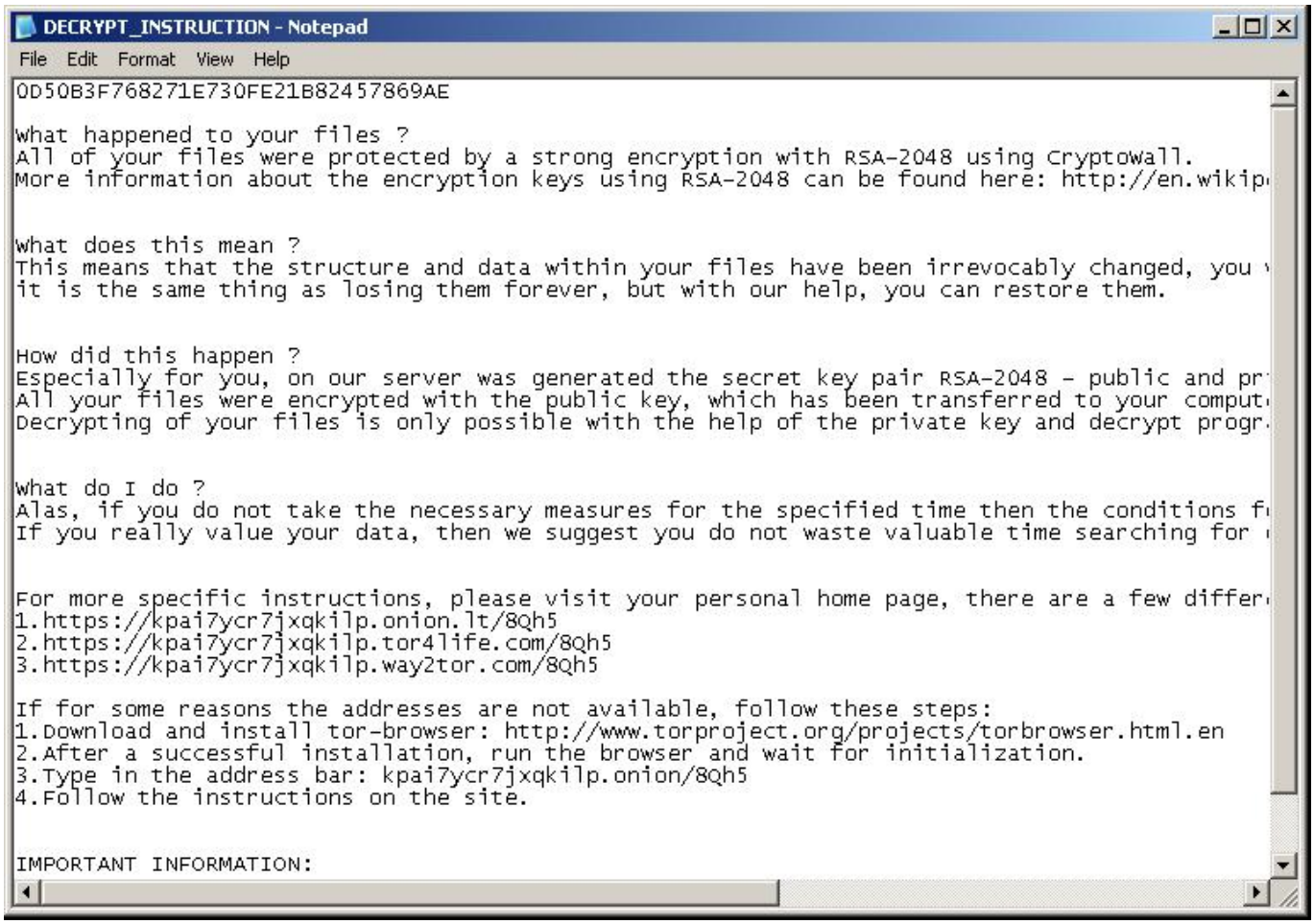
Network Traffic		
	Remote IP	**Local IP**
Connection #1	10.20.25.255	10.20.25.250

DNS Requests	
Request	**Result**
mtsvp.com	46.151.145.11
suspendedwar.com	76.74.170.149
goodbookideas.com	50.63.85.76
kpai7ycr7jxqkilp.onion.lt	82.94.251.220
secure2.alphassl.com	141.101.115.22
	141.101.114.22
	190.93.247.21
	190.93.244.22
	190.93.246.21
www.download.windowsupdate.com	198.172.136.43
	198.172.136.11
crl.globalsign.net	108.162.232.196
	108.162.232.200
	108.162.232.204
	108.162.232.202
	108.162.232.203
	108.162.232.198
	108.162.232.207
	108.162.232.201
	108.162.232.199
	108.162.232.197
	108.162.232.205
crl2.alphassl.com	190.93.247.21
	190.93.246.21
	141.101.114.22
	190.93.244.22
	141.101.115.22

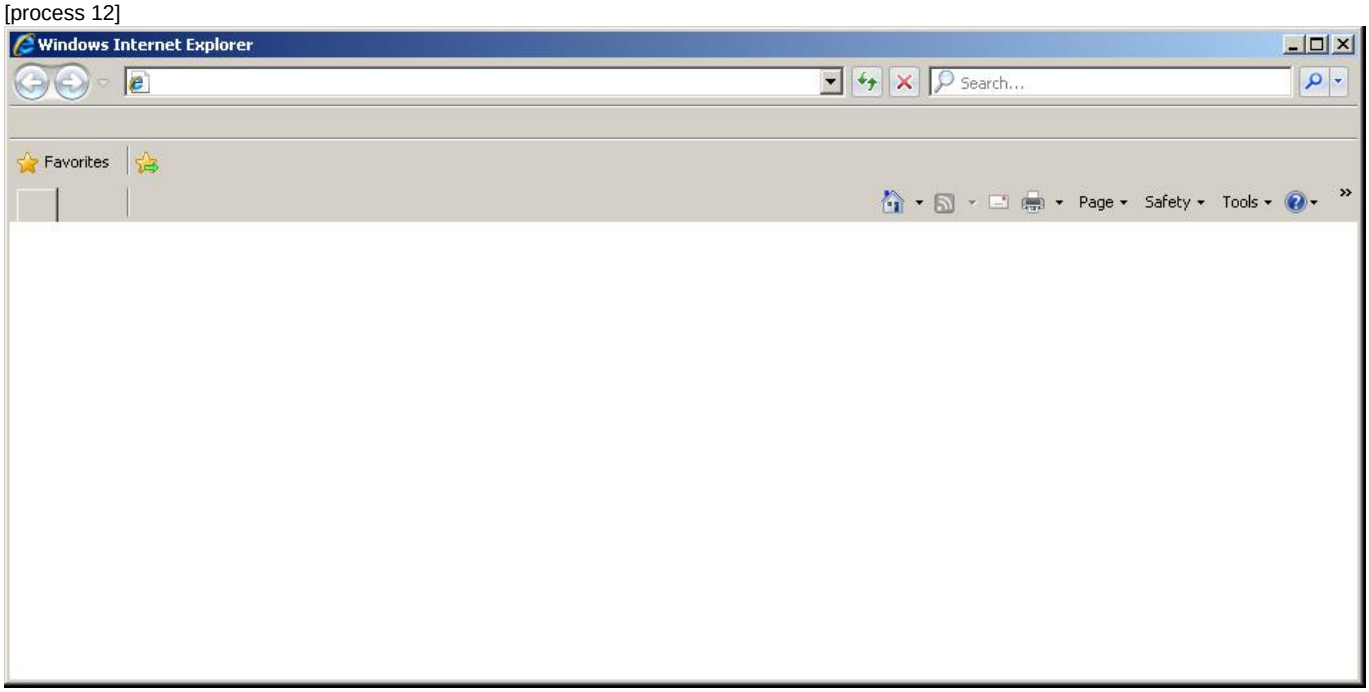
[process 11]



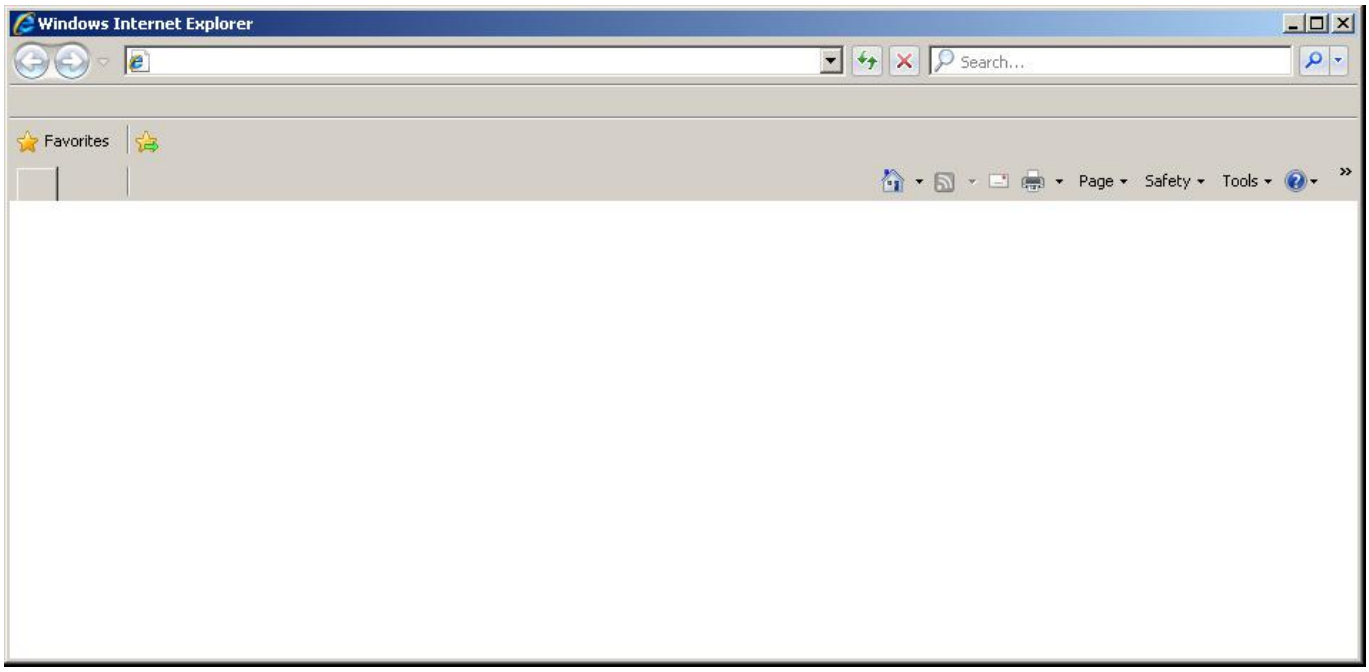
[process 11]



[process 12]



[process 12]



[process 12]

Virus Total Results	
Last Scanned:	**2014-09-11 20:39:20**
Bkav:	Not Detected
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Not Detected
Malwarebytes:	Not Detected
VIPRE:	Not Detected
SUPERAntiSpyware:	Not Detected
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
Agnitum:	Not Detected
F-Prot:	Not Detected
Symantec:	Not Detected
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	Not Detected
Avast:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Not Detected
NANO-Antivirus:	Not Detected
AegisLab:	Not Detected
ByteHero:	Not Detected
Rising:	Not Detected
Ad-Aware:	Not Detected
Emsisoft:	Not Detected
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Trojan.Dyre.25
Zillya:	Not Detected
TrendMicro:	Not Detected
McAfee-GW-Edition:	Not Detected
Sophos:	Not Detected
Cyren:	Not Detected
Jiangmin:	Not Detected
Avira:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
ViRobot:	Not Detected
GData:	Not Detected
AhnLab-V3:	Not Detected
VBA32:	Not Detected
AVware:	Trojan.Win32.Generic.pak!cobra
Panda:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	Not Detected
Tencent:	Not Detected
Ikarus:	Not Detected
Fortinet:	Not Detected
AVG:	Not Detected
Baidu-International:	Not Detected
Qihoo-360:	Not Detected

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