Analysis # 1941

08/01/2014 14:34 pm

Table of Contents

Analysis Summary

Submitted File:	Remittance___Copy.exe
MD5:	b666e8eed6c4eae61d4cb9a9c8b09cdc
File Size:	24064
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-08-01 14:34:31
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Fri, 01 Aug 2014 23:38:02 +0000
Termination Time:	Fri, 01 Aug 2014 18:39:03 +0000
Analysis Time:	2014-08-01 14:34:31
Sandbox:	XP-SP2 - 00-0C-29-B2-D2-62
Total Processes:	10
Sample Notes:	

Digital Behavior Traits

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

Deleted Files
[process 2] C:\Remittance___Copy.exe
[process 4] C:\DOCUME~1\Charlie\LOCALS~1\Temp\etiav.exe
[process 5] C:\Documents and Settings\All Users\Application Data\Microsoft\OFFICE\DATA\OPA11.BAK.hq9
[process 5] C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.b ak.cu7
[process 5] C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.t xt.6nk
[process 5] C:\Documents and Settings\Charlie\Cookies\charlie@c1.microsoft[2].txt.49q
[process 5] C:\Documents and Settings\Charlie\Cookies\charlie@microsoft[1].txt.1z4
[process 5] C:\Documents and Settings\Charlie\Cookies\charlie@track.monitis[2].txt.rt2
[process 5] C:\Documents and Settings\Charlie\Cookies\charlie@www.microsoft[2].txt.u13
[process 5] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Exp lorer\brndlog.txt.h0u
[process 5] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Outlook\Outl ook.pst.t97
[process 5] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Windows Medi a\9.0\WMSDKNS.DTD.64s
[process 5] C:\Documents and Settings\Charlie\Templates\excel.xls.i22
[process 5] C:\Documents and Settings\Charlie\Templates\excel4.xls.1kv
[process 5] C:\Documents and Settings\Charlie\Templates\powerpnt.ppt.wq9
[process 5] C:\Documents and Settings\Charlie\Templates\quattro.wb2.r6d
[process 5] C:\Documents and Settings\Charlie\Templates\sndrec.wav.m2e
[process 5] C:\Documents and Settings\Charlie\Templates\winword.doc.p0o
[process 5] C:\Documents and Settings\Charlie\Templates\winword2.doc.c6q
[process 5] C:\Documents and Settings\Charlie\Templates\wordpfct.wpd.7tz
[process 5] C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brnd log.bak.s8q
[process 5] C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brnd log.txt.3ue
[process 5] C:\Documents and Settings\Default User\Local Settings\Application Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD.50k
[process 5] C:\Documents and Settings\Default User\Templates\excel.xls.1d2
[process 5] C:\Documents and Settings\Default User\Templates\excel4.xls.11f
[process 5] C:\Documents and Settings\Default User\Templates\powerpnt.ppt.8dm
[process 5] C:\Documents and Settings\Default User\Templates\quattro.wb2.7ig
[process 5] C:\Documents and Settings\Default User\Templates\sndrec.wav.61i
[process 5] C:\Documents and Settings\Default User\Templates\winword.doc.mg1
[process 5] C:\Documents and Settings\Default User\Templates\winword2.doc.07m
[process 5] C:\Documents and Settings\Default User\Templates\wordpfct.wpd.7jf
[process 5] C:\Documents and Settings\Charlie\Start Menu\Programs\Startup\0d50b3f.exe
[process 5] C:\Documents and Settings\Charlie\Application Data\0d50b3f.exe
[process 5] C:\0d50b3f\0d50b3f.exe
[process 5] C:\0d50b3f

Stored Modified Files
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\jotyb.exe
[process 2] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4 O5PO1W\cw2800[1].rar
[process 2] C:\DOCUME~1\Charlie\LOCALS~1\Temp\etiav.exe
[process 5] C:\Documents and Settings\All Users\Application Data\Microsoft\OFFICE\DATA\OPA11.BAK.hq9
[process 5] C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.b ak.cu7
[process 5] C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.t xt.6nk
[process 5] C:\Documents and Settings\Charlie\Cookies\charlie@c1.microsoft[2].txt.49q
[process 5] C:\Documents and Settings\Charlie\Cookies\charlie@microsoft[1].txt.1z4
[process 5] C:\Documents and Settings\Charlie\Cookies\charlie@track.monitis[2].txt.rt2
[process 5] C:\Documents and Settings\Charlie\Cookies\charlie@www.microsoft[2].txt.u13
[process 5] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Exp lorer\brndlog.txt.h0u
[process 5] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Outlook\Outl ook.pst.t97
[process 5] C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Windows Medi a\9.0\WMSDKNS.DTD.64s
[process 5] C:\Documents and Settings\Charlie\Templates\excel.xls.i22
[process 5] C:\Documents and Settings\Charlie\Templates\excel4.xls.1kv
[process 5] C:\Documents and Settings\Charlie\Templates\powerpnt.ppt.wq9
[process 5] C:\Documents and Settings\Charlie\Templates\quattro.wb2.r6d
[process 5] C:\Documents and Settings\Charlie\Templates\sndrec.wav.m2e
[process 5] C:\Documents and Settings\Charlie\Templates\winword.doc.p0o
[process 5] C:\Documents and Settings\Charlie\Templates\winword2.doc.c6q
[process 5] C:\Documents and Settings\Charlie\Templates\wordpfct.wpd.7tz
[process 5] C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brnd log.bak.s8q
[process 5] C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brnd log.txt.3ue
[process 5] C:\Documents and Settings\Default User\Local Settings\Application Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD.50k
[process 5] C:\Documents and Settings\Default User\Templates\excel.xls.1d2
[process 5] C:\Documents and Settings\Default User\Templates\excel4.xls.11f
[process 5] C:\Documents and Settings\Default User\Templates\powerpnt.ppt.8dm
[process 5] C:\Documents and Settings\Default User\Templates\quattro.wb2.7ig
[process 5] C:\Documents and Settings\Default User\Templates\sndrec.wav.61i
[process 5] C:\Documents and Settings\Default User\Templates\winword.doc.mg1
[process 5] C:\Documents and Settings\Default User\Templates\winword2.doc.07m
[process 5] C:\Documents and Settings\Default User\Templates\wordpfct.wpd.7jf

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 3]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	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 3]	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 3]	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 3]	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 3]	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 4]	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 4]	Name: SHIMLIB_LOG_MUTEX
	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 5]	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 5]	Name: Local\c:!documents and settings!charlie!cookies!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	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 5]	Name: Local\WininetConnectionMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	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: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: CTF.TMD.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.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-6 02162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 7]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-6 02162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	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 8]	Name: Local\!BrowserEmulation!SharedMemory!Mutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: ConnHashTable<1188>_HashTable_Mutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\ZonesCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: oleacc-msaa-loaded
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\RSS Eventing Connection Database Mutex 000004a4
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\Feed Eventing Shared Memory Mutex S-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	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 9]	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 9]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 5]	\Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE
[process 5]	\Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF
[process 7]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Notepad
[process 8]	\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 8]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\
[process 8]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\
[process 8]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\
[process 8]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\0x00000000\

Deleted Keys	
	key
[process 8]	\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 8]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\0x00000000
[process 8]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile
[process 8]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}
[process 8]	\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 8]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile\0x00000000
[process 8]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}\LanguageProfile
[process 8]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\CTF\TIP\{1188450c-fdab-47ae-80d8-c9633f71be64}

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\jotyb.exe
[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\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: 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\etiav.exe
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[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 4]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: 0d50b3
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: 0d50b3f
[process 4]	Key Name: \Registry\Machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore Value: DisableSR
[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\Explorer\Shell Folders Value: Cache
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName

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

[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\brndlog.txt
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Cookies\charlie@c1.microsoft[2].txt
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Cookies\charlie@microsoft[1].txt
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Cookies\charlie@track.monitis[2].txt
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Cookies\charlie@www.microsoft[2].txt
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Explorer\brndlog.txt
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\excel.xls
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\excel4.xls
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\powerpnt.ppt
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\quattro.wb2
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\sndrec.wav
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\winword.doc
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\winword2.doc

[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Charlie\Templates\wordpfct.wpd
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brndlog.bak
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brndlog.txt
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Local Settings\Application Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\excel.xls
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\excel4.xls
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\powerpnt.ppt
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\quattro.wb2
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\sndrec.wav
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\winword.doc
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\winword2.doc
[process 5]	Key Name: \Registry\User\S-1-5-21-602162358-879983540-1177238915-1003\software\0D50B3F768271E730FE21B82457869AE\01224567889ABEEF Value: C:\Documents and Settings\Default User\Templates\wordpfct.wpd
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Personal
[process 5]	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 5]	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 5]	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 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common Documents
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Desktop
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache Value: C:\WINDOWS\system32\notepad.exe
[process 5]	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 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	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\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 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

	Value: Cookies
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 8]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Rpc Value: UuidSequenceNumber
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Desktop
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: CompatibilityFlags
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Favorites
[process 8]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Recovery\Active Value: {04F7AD72-19AB-11E4-B96C-000C29B2D262}
[process 8]	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 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ex

	plorer\Main\WindowsSearch Value: Version
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones Value: SecuritySafe
[process 8]	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 8]	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 8]	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 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{1EA4DBF0-3C3B-11CF-810C-00AA00389B71}\1.1\0\wi

	n32 Value:
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{1EA4DBF0-3C3B-11CF-810C-00AA00389B71}\1.1\0\wi n32 Value:
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur rentVersion\Explorer\Shell Folders Value: AppData
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore Value: Type
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore Value: Count
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore Value: Time
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore Value: Type
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore Value: Count
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore Value: Time
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore Value: Type
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore Value: Count
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SOFTWARE\Microsoft\Windows\Cur rentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore Value: Time
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ex plorer\Main Value: FullScreen
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ex plorer\Main Value: Window_Placement
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ex plorer\Main\WindowsSearch Value: Version
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur rentVersion\Explorer\MenuOrder\Favorites\Links Value: Order
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\Cur rentVersion\Internet Settings Value: ProxyEnable
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\Cur

	rentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 8]	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 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: FullScreen
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: Window_Placement
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Favorites\Links Value: Order
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: IE8RunOnceLastShown
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\Main Value: IE8RunOnceLastShown_TIMESTAMP
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: Path
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: Handler
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: FeedUrl
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: DisplayName
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: ErrorState
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: DisplayMask
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: Path
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: Handler
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: FeedUrl
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: DisplayName

[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: ErrorState
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: DisplayMask
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: DisplayName
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: DisplayMask
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: ErrorState
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: Expiration
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: DisplayName
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: DisplayMask
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: ErrorState
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: Expiration
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

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

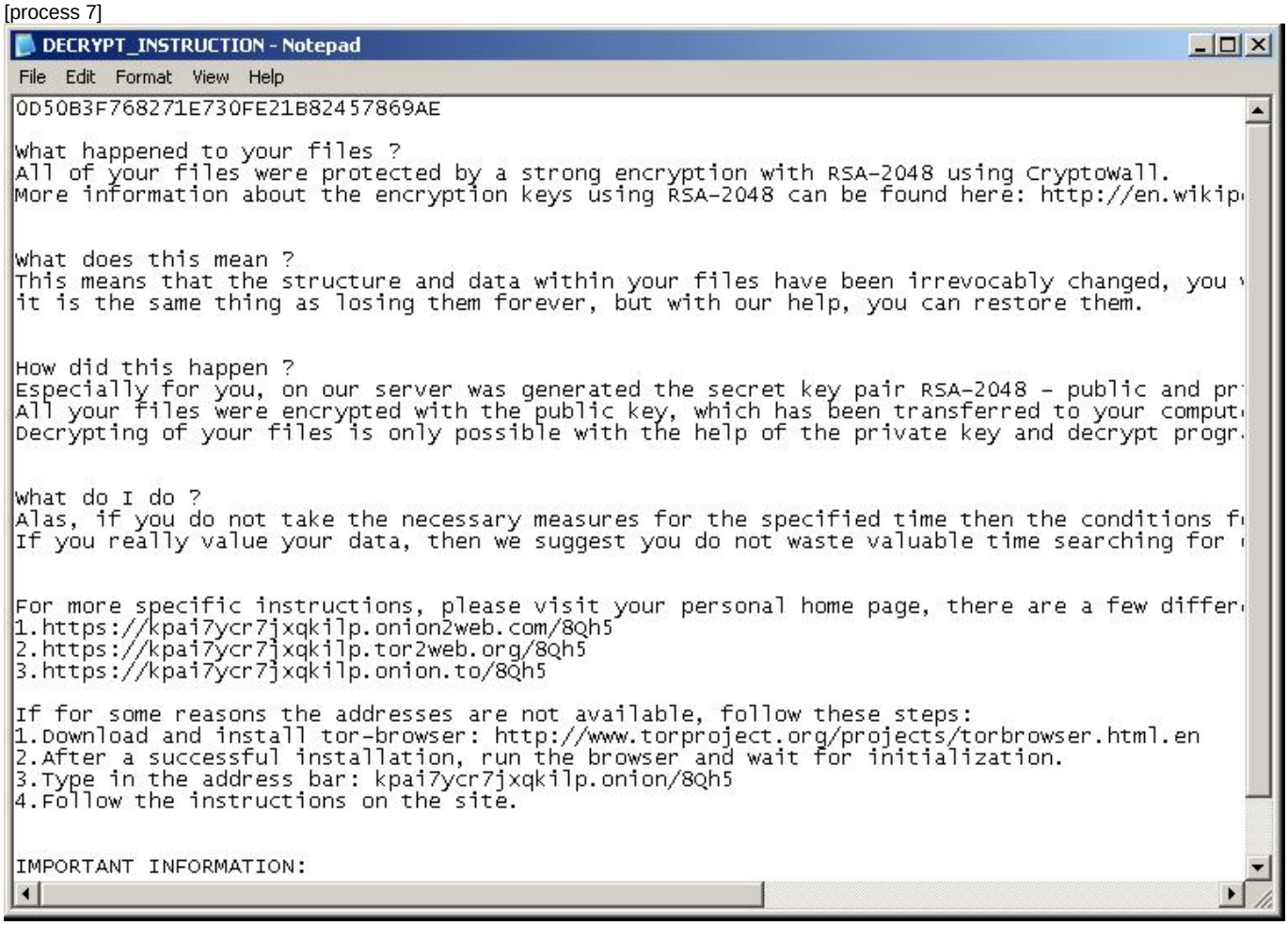
	rentVersion\Run Value: 0d50b3f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: 0d50b3
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\0 Value: Expiration
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Explorer\LinksBar\ItemCache\1 Value: Expiration

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process 2]	94.23.247.202	10.20.25.250	GET /18w/NODE01/0/51-SP3/0/
[process 2]	94.23.247.202	10.20.25.250	GET /18w/NODE01/1/0/0/ POST /private/sandbox_status.php
[process 2]	94.141.27.237	10.20.25.250	GET /dmdocuments/cw2800.rar
[process 2]	94.23.247.202	10.20.25.250	GET /18w/NODE01/41/5/4/
[process 3]	178.132.204.120	10.20.25.250	none
[process 3]	178.132.204.120	10.20.25.250	none
[process 5]	194.58.101.111	10.20.25.250	POST /i6hgqc67wj55
[process 5]	194.58.101.111	10.20.25.250	POST /1m82ia1i61wd8
[process 5]	194.58.101.111	10.20.25.250	POST /qlnthh63xy
[process 5]	194.58.101.111	10.20.25.250	POST /inbx78j6ykc
[process 5]	194.58.101.111	10.20.25.250	POST /qvforlzxzd45m
[process 5]	194.58.101.111	10.20.25.250	POST /jlaazl1xojwa
[process 5]	194.58.101.111	10.20.25.250	POST /1g1jroqiv14fb
[process 10]	127.0.0.1	0.0.0.0	none
[process 10]	127.0.0.1	0.0.0.0	none
[process 10]	127.0.0.1	127.0.0.1	none
[process 10]	23.13.165.163	10.20.25.250	GET /crls/secureca.crl GET /crls/gtglobal.crl
[process 10]	23.13.165.163	10.20.25.250	GET /crls/rapidssl.crl
[process 10]	178.132.204.120	10.20.25.250	none
[process 10]	178.132.204.120	10.20.25.250	none
[process 10]	178.132.204.120	10.20.25.250	none
[process 10]	178.132.204.120	10.20.25.250	none

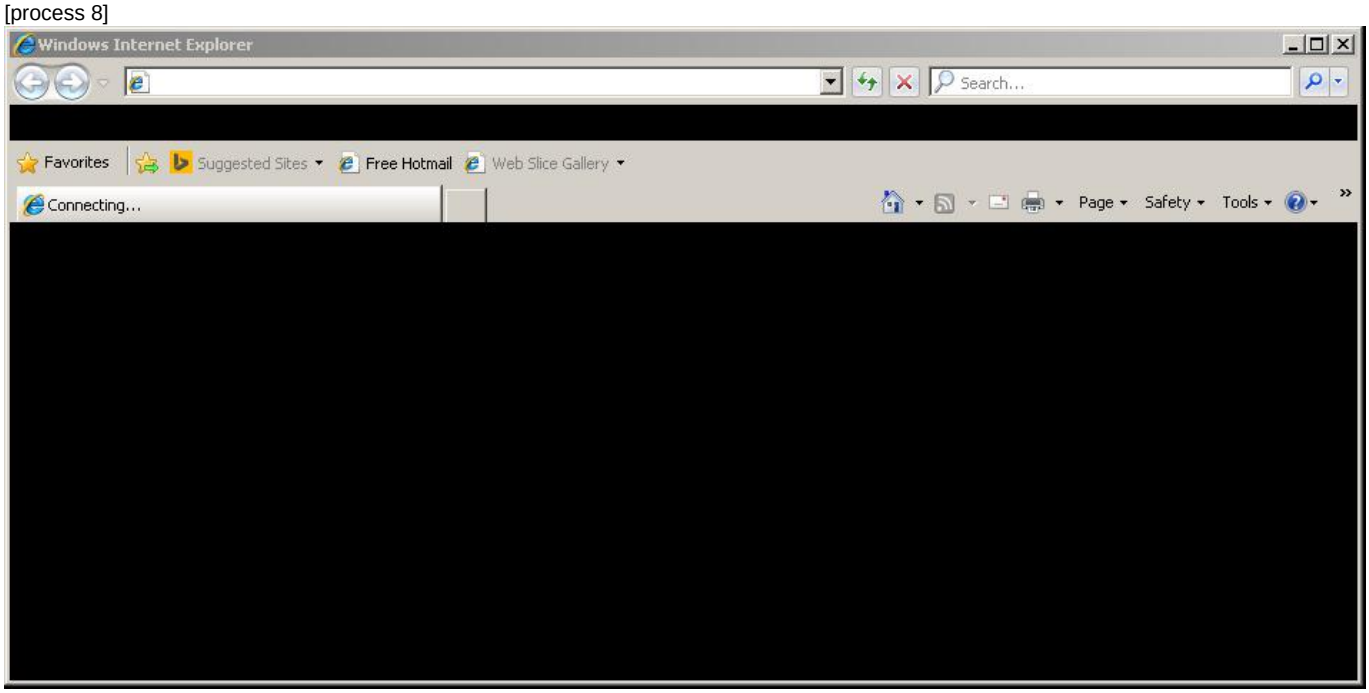
Network Traffic		
	Remote IP	**Local IP**
Connection #1	10.20.25.255	10.20.25.250
Connection #2	239.255.255.250	10.20.25.250

DNS Requests	
Request	**Result**
theothersmag.com	94.141.27.237
poroshenkogitler.com	194.58.101.111
kpai7ycr7jxqkilp.onion2web.com	178.132.204.120
crl.geotrust.com	23.13.165.163
rapidssl-crl.geotrust.com	23.13.165.163

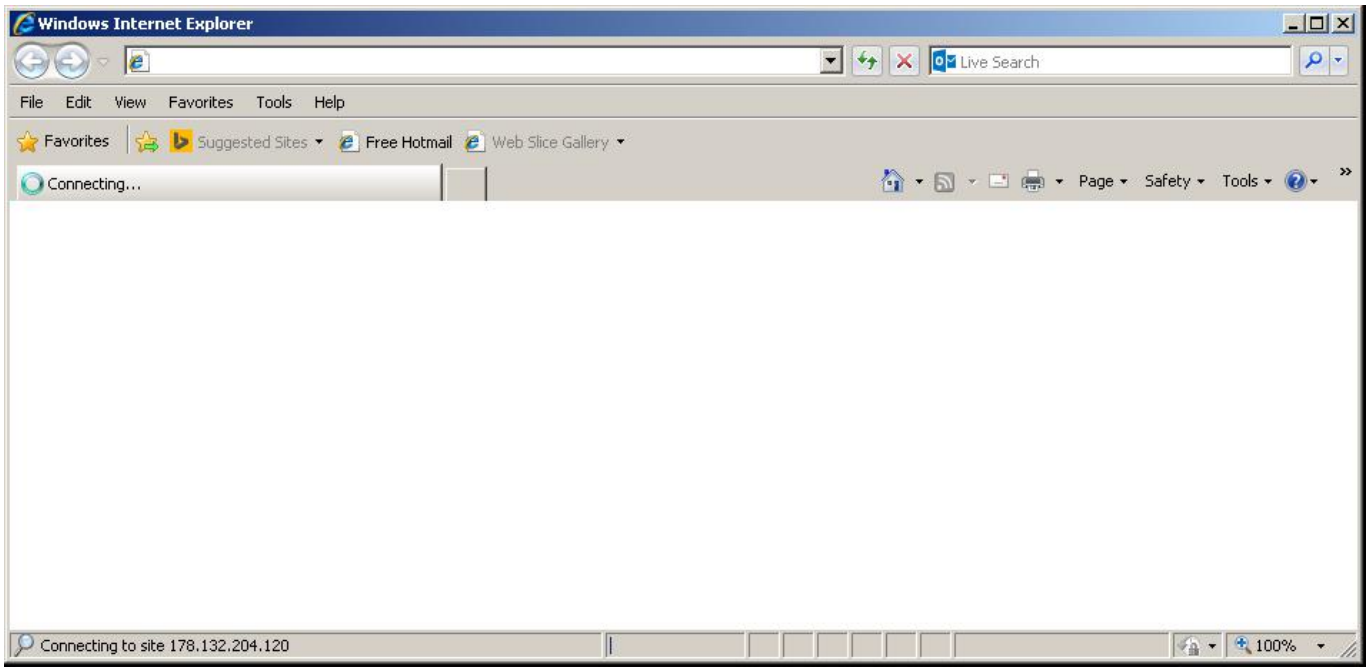
[process 7]



[process 8]



[process 8]



[process 8]

Virus Total Results	
Last Scanned:	**2014-08-01 18:35:15**
Bkav:	Not Detected
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Downloader-FSH!B666E8EED6C4
Malwarebytes:	Trojan.Upatre
AegisLab:	Not Detected
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
NANO-Antivirus:	Not Detected
F-Prot:	W32/Trojan3.JSS
Symantec:	Not Detected
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	Not Detected
Avast:	Win32:Crypt-REV [Trj]
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Not Detected
Agnitum:	Not Detected
SUPERAntiSpyware:	Not Detected
ByteHero:	Not Detected
Ad-Aware:	Not Detected
Sophos:	Troj/Upatre-DS
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
VIPRE:	Not Detected
AntiVir:	Not Detected
TrendMicro:	Not Detected
McAfee-GW-Edition:	Artemis!B666E8EED6C4
Emsisoft:	Not Detected
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
ViRobot:	Not Detected
GData:	Not Detected
Commtouch:	W32/Trojan.LXFN-8686
AhnLab-V3:	Not Detected
VBA32:	Not Detected
AVware:	Not Detected
Panda:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	a variant of Win32/Kryptik.CHZB
Rising:	Not Detected
Ikarus:	Not Detected
Fortinet:	Not Detected
AVG:	Not Detected
Baidu-International:	Not Detected
Qihoo-360:	Win32/Trojan.Multi.daf

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