



Analysis # 2645

09/16/2014 06:16 am

Table of Contents

Analysis Summary	3
Analysis Summary	3
Digital Behavior Traits	3
File Activity	4
Deleted Files	4
Stored Modified Files	5
Created Mutexes	6
Created Mutexes	6
Registry Activity	8
Created Keys	8
Set Values	9
Deleted Values	15
Network Activity	16
Network Events	16
Network Traffic	17
DNS Requests	18
Virus Total Results	19

Analysis Summary	
Submitted File:	Message_2864_pdf___Copy.exe
MD5:	8ed0aa8a61552b4cbd7c997894d5b3d8
File Size:	20480
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-09-16 06:16:04
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Tue, 16 Sep 2014 15:20:48 +0000
Termination Time:	Tue, 16 Sep 2014 15:21:48 +0000
Analysis Time:	2014-09-16 06:16:04
Sandbox:	XP-SP2 - 00-0C-29-B2-D2-62
Total Processes:	5
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:\Message_2864_pdf___Copy.exe

[process 4] C:\DOCUME~1\Charlie\LOCALS~1\Temp\zfdhj.exe

[process 5] C:\WINDOWS\Temp\Cab1.tmp

[process 5] C:\WINDOWS\Temp\Tar2.tmp

Stored Modified Files

[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\vvhhh.exe
[process 2] C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4O5PO1W\1609uk4[1].lim
[process 2] C:\DOCUME~1\Charlie\LOCALS~1\Temp\zfdhj.exe
[process 3] C:\Documents and Settings\Charlie\Application Data\ILFVpjWmPTHNnyt.exe
[process 5] C:\WINDOWS\system32\config\systemprofile\Application Data\d6r5g4da.db
[process 5] C:\WINDOWS\system32\config\systemprofile\Application Data\d6r5g4da.db
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat
[process 5] C:\WINDOWS\system32\config\systemprofile\Application Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004
[process 5] C:\WINDOWS\system32\config\systemprofile\Application Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004
[process 5] C:\WINDOWS\system32\config\systemprofile\Application Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015
[process 5] C:\WINDOWS\system32\config\systemprofile\Application Data\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015
[process 5] C:\WINDOWS\Temp\Cab1.tmp
[process 5] C:\WINDOWS\Temp\Tar2.tmp

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-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: LocalZonesCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: LocalZoneAttributeCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: LocalZonesCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: LocalZonesLockedCacheCounterMutex 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-1-5-21-602162358-879983540-1177238915-1003 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: LocalZonesCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: LocalZoneAttributeCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: LocalZonesCacheCounterMutex

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: LocalZonesLockedCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Local\c:\!documents and settings!\charlie!\ietldcache! 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-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\553wwerdy7 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\c:\!windows!\system32!\config!\systemprofile!\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:\!windows!\system32!\config!\systemprofile!\cookies! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\c:\!windows!\system32!\config!\systemprofile!\local settings!\history!\history.ie5! 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: LocalZonesCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\c:\!windows!\system32!\config!\systemprofile!\ietldcache! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: LocalZoneAttributeCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: LocalZonesCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 5]	\REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietId
[process 5]	\REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId
[process 5]	\REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\BrowserEmulation

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: UNCAIntranet
[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\vwhhh.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\zfdhj.exe
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value:
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec
[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld Value: CachePath
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld Value: CachePrefix
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld Value: CacheLimit
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Ca

	che\Extensible Cache\ietId Value: CacheOptions
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Ca che\Extensible Cache\ietId Value: CachePath
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Ca che\Extensible Cache\ietId Value: CacheRepair
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId Value: IETIdDllVersionHigh
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId Value: IETIdDllVersionLow
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId Value: IETIdVersionHigh
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId Value: IETIdVersionLow
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId Value: StaleIETIdCache
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\BrowserEmulation Value: TLDUpdates
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: ProxyBypass
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: IntranetName
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: UNCAsIntranet
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: AutoDetect
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: ProxyBypass
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: IntranetName
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: UNCAsIntranet
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: AutoDetect
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connec tions Value: SavedLegacySettings
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec

[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\02FAF3E291435468607857694DF5E45B68851868 Value: Blob
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec

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\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates Value: 02FAF3E291435468607857694DF5E45B68851868

Network Events			
	Remote IP	Local IP	HTTP Command
[process 2]	188.165.204.210	10.20.25.250	GET /1609uk4/NODE01/0/51-SP3/0/
[process 2]	188.165.204.210	10.20.25.250	GET /1609uk4/NODE01/1/0/0/
[process 2]	198.143.152.226	10.20.25.250	GET /css/1609uk4.lim
[process 2]	188.165.204.210	10.20.25.250	GET /1609uk4/NODE01/41/5/4/
[process 5]	74.125.229.238	10.20.25.250	none
[process 5]	217.10.68.152	10.20.25.250	none
[process 5]	217.10.64.53	10.20.25.250	none
[process 5]	74.125.229.238	10.20.25.250	none
[process 5]	37.187.71.122	10.20.25.250	none
[process 5]	23.201.103.147	10.20.25.250	GET /msdownload/update/v3/static/trustedr/en/authroots eq.txt GET /msdownload/update/v3/static/trustedr/en/authroots tl.cab

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
Connection #3	217.10.68.152	10.20.25.250
Connection #4	217.10.64.53	10.20.25.250

DNS Requests	
Request	Result
brisamarcalcados.com.br	198.143.152.226
google.com	74.125.229.238
	74.125.229.229
	74.125.229.233
	74.125.229.230
	74.125.229.226
	74.125.229.225
	74.125.229.231
	74.125.229.227
	74.125.229.232
	74.125.229.224
74.125.229.228	
stun.sipgate.net	217.10.68.152
www.download.windowsupdate.com	23.201.103.147
	23.201.103.130

Virus Total Results	
Last Scanned:	2014-09-16 10:19:14
Bkav:	Not Detected
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Not Detected
Malwarebytes:	Not Detected
Zillya:	Not Detected
SUPERAntiSpyware:	Not Detected
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
NANO-Antivirus:	Not Detected
F-Prot:	Not Detected
Symantec:	Not Detected
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	TROJ_UPATRE.SM01
Avast:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Not Detected
Agnitum:	Not Detected
ViRobot:	Not Detected
Tencent:	Not Detected
Ad-Aware:	Not Detected
Emsisoft:	Not Detected
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
VIPRE:	Not Detected
TrendMicro:	TROJ_UPATRE.SM01
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
AegisLab:	Not Detected
AhnLab-V3:	Not Detected
GData:	Not Detected
ByteHero:	Not Detected
VBA32:	Not Detected
AVware:	Not Detected
Baidu-International:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	Not Detected
Rising:	Not Detected
Ikarus:	Not Detected
Fortinet:	Not Detected
AVG:	Not Detected
Panda:	Not Detected
Qihoo-360:	Malware.QVM20.Gen

ThreatTrack Security, Inc.

33 North Garden Avenue, Suite 1200, Clearwater, Florida, USA 33755

Telephone: (855) 443-4284 Intl: +1(813)367-9907

Email: Sales@ThreatTrack.com

Disclaimer © 2013. ThreatTrack Security, Inc. All rights reserved. All product and company names herein may be trademarks of their respective owners. The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. ThreatTrack Security, Inc. is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, ThreatTrack Security makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. ThreatTrack Security makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.