



## **Analysis # 2518**

**09/09/2014 11:39 am**

## Table of Contents

<b>Analysis Summary</b>	<b>3</b>
<b>Analysis Summary</b>	<b>3</b>
<b>Digital Behavior Traits</b>	<b>3</b>
<b>File Activity</b>	<b>4</b>
<b>Deleted Files</b>	<b>4</b>
<b>Stored Modified Files</b>	<b>5</b>
<b>Created Mutexes</b>	<b>6</b>
<b>Created Mutexes</b>	<b>6</b>
<b>Registry Activity</b>	<b>8</b>
<b>Created Keys</b>	<b>8</b>
<b>Set Values</b>	<b>9</b>
<b>Deleted Values</b>	<b>14</b>
<b>Network Activity</b>	<b>15</b>
<b>Network Events</b>	<b>15</b>
<b>Network Traffic</b>	<b>16</b>
<b>DNS Requests</b>	<b>17</b>
<b>Virus Total Results</b>	<b>18</b>

Analysis Summary	
Submitted File:	invoice_090914___Copy.exe
MD5:	a75ca176f4a8ab869e53db06c53dae30
File Size:	33792
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-09-09 11:39:24
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Tue, 09 Sep 2014 20:43:57 +0000
Termination Time:	Tue, 09 Sep 2014 20:44:57 +0000
Analysis Time:	2014-09-09 11:39:24
Sandbox:	XP-SP2 - 00-0C-29-B2-D2-62
Total Processes:	5
Sample Notes:	

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

**Deleted Files**

[process 2] C:\invoice\_090914\_\_\_Copy.exe

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

Stored Modified Files	
[process 1]	C:\DOCUME~1\Charlie\LOCALS~1\Temp\qqfic.exe
[process 2]	C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\C4O5PO1W\9k1[1].dll
[process 2]	C:\DOCUME~1\Charlie\LOCALS~1\Temp\cpfww.exe
[process 3]	C:\Documents and Settings\Charlie\Application Data\alba.exe
[process 5]	C:\WINDOWS\system32\config\systemprofile\Application Data\whr458da.db
[process 5]	C:\WINDOWS\system32\config\systemprofile\Application Data\whr458da.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\IETldCache\index.dat
[process 5]	C:\WINDOWS\system32\config\systemprofile\IETldCache\index.dat

Created Mutexes	
	mutex
[process 1]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-602162358-879983540-1177238915-1003 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: 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 2]	Name: Local\ZonesLockedCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\c:\documents and settings\charlie\ietldcache! 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 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\cdv5b74f5y7 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: Local\ZonesCounterMutex 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: 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

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: 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\qqfic.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\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\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:\DOCUMENT~1\Charlie\LOCALS~1\Temp\cpfvw.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

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

Network Events			
	Remote IP	Local IP	HTTP Command
[process 2]	95.141.37.158	10.20.25.250	GET /0909uk1/NODE01/0/51-SP3/0/
[process 2]	95.141.37.158	10.20.25.250	GET /0909uk1/NODE01/1/0/0/
[process 2]	46.30.212.72	10.20.25.250	GET /js/9k1.cll
[process 2]	95.141.37.158	10.20.25.250	GET /0909uk1/NODE01/41/5/4/
[process 5]	173.194.37.4	10.20.25.250	none
[process 5]	74.125.131.127	10.20.25.250	none
[process 5]	173.194.37.4	10.20.25.250	none
[process 5]	188.165.204.210	10.20.25.250	none
[process 5]	188.165.204.210	10.20.25.250	none
[process 5]	188.165.204.210	10.20.25.250	none
[process 5]	188.165.204.210	10.20.25.250	none
[process 5]	188.165.204.210	10.20.25.250	none
[process 5]	188.165.204.210	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
Connection #3	10.20.25.255	10.20.25.250
Connection #4	74.125.131.127	10.20.25.250



DNS Requests	
Request	Result
vaderhopland.be	46.30.212.72
google.com	173.194.37.4
	173.194.37.3
	173.194.37.8
	173.194.37.6
	173.194.37.0
	173.194.37.9
	173.194.37.5
	173.194.37.2
	173.194.37.14
	173.194.37.1
173.194.37.7	
stun1.l.google.com	74.125.131.127

Virus Total Results	
<b>Last Scanned:</b>	<b>2014-09-09 15:42:44</b>
Bkav:	HW32.Inectrj.xmes
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Packed-CA!A75CA176F4A8
Malwarebytes:	Not Detected
VIPRE:	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:	Not Detected
Avast:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Not Detected
Agnitum:	Not Detected
AegisLab:	Not Detected
ByteHero:	Not Detected
Tencent:	Not Detected
Ad-Aware:	Not Detected
Sophos:	Mal/Generic-S
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
Zillya:	Not Detected
TrendMicro:	Not Detected
McAfee-GW-Edition:	BehavesLike.Win32.BadFile.nm
Emsisoft:	Not Detected
Cyren:	Not Detected
Jiangmin:	Not Detected
Avira:	TR/Crypt.Xpack.90493
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	VirTool:Win32/Obfuscator.WT
ViRobot:	Not Detected
GData:	Not Detected
AhnLab-V3:	Not Detected
VBA32:	Not Detected
AVware:	Not Detected
Panda:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	a variant of Win32/Kryptik.CKTV
Rising:	Not Detected
Ikarus:	Not Detected
Fortinet:	Not Detected
AVG:	Not Detected
Baidu-International:	Not Detected
Qihoo-360:	HEUR/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](mailto: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.