Analysis # 2532

09/10/2014 08:25 am

Table of Contents

Analysis Summary

Submitted File:	Invoice_copy_8829912.exe
MD5:	1e55c47600e486faf8b41c201e57e217
File Size:	250999
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-09-10 08:25:16
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Wed, 10 Sep 2014 12:29:51 +0000
Termination Time:	Wed, 10 Sep 2014 12:29:54 +0000
Analysis Time:	2014-09-10 08:25:16
Sandbox:	XP-SP2 - 00-0C-29-B2-D2-62
Total Processes:	6
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 6] C:\Invoice_copy_8829912.exe

Stored Modified Files
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temp\Zyoka\ivyk.exe
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\ZTYA413.bat
[process 5] C:\Documents and Settings\Charlie\Application Data\Microsoft\Address Book\Charlie.wab
[process 5] C:\Documents and Settings\Charlie\Application Data\Microsoft\Address Book\Charlie.wab
[process 5] C:\Documents and Settings\Charlie\Application Data\Microsoft\Address Book\Charlie.wab
[process 5] C:\Documents and Settings\Charlie\Application Data\Microsoft\Address Book\Charlie.wab
[process 5] C:\Documents and Settings\Charlie\Application Data\Microsoft\Address Book\Charlie.wab

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: Global\{52C73632-A29C-48D0-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Global\{C7A62370-B7DE-DDB1-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-E09D-7F4204EC7AB9}
	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\{EDDE1379-87D7-F7C9-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-389C-7F42DCED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-149F-7F42F0EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-A89F-7F424CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-909F-7F4274EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-E49F-7F4200EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-D89F-7F423CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-B898-7F425CE97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-E898-7F420CE97AB9}

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-7C99-7F4298E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-4C99-7F42A8E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-9499-7F4270E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-E09A-7F4204EB7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-B89B-7F425CEA7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-D89C-7F423CED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-009E-7F42E4EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-E49E-7F4200EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-C09E-7F4224EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-689D-7F428CEC7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-5898-7F42BCE97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{B5357B80-EF2E-AF22-F09C-7F4214ED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{A1721768-83C6-BB65-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{AD9EC05A-54F4-B789-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{AD9EC05D-54F3-B789-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\{CC787649-E2E7-D66F-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\{CC787648-E2E6-D66F-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{C7A62370-B7DE-DDB1-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{A1721768-83C6-BB65-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{AD9EC05A-54F4-B789-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{AD9EC05D-54F3-B789-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Local\{CC787649-E2E7-D66F-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Local\{CC787648-E2E6-D66F-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{C7A62370-B7DE-DDB1-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-389C-7F42DCED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 3]	Name: Global\{B5357B80-EF2E-AF22-149F-7F42F0EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-A89F-7F424CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-909F-7F4274EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-E49F-7F4200EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-D89F-7F423CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-B898-7F425CE97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-E898-7F420CE97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-7C99-7F4298E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-4C99-7F42A8E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-9499-7F4270E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-E09A-7F4204EB7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-D89C-7F423CED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-009E-7F42E4EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-E49E-7F4200EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-C09E-7F4224EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-689D-7F428CEC7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-5898-7F42BCE97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{B5357B80-EF2E-AF22-309D-7F42D4EC7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{52DDACB9-3817-48CA-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\{CC787649-E2E7-D66F-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\{CC787648-E2E6-D66F-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{C7A62370-B7DE-DDB1-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{C7A62370-B7DE-DDB1-6BF3-F5458F82F0BE}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: MPSWabDataAccessMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: MPSWABOlkStoreNotifyMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: MSIdent Logon

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 1]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Itquuxusow
[process 5]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager
[process 5]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts
[process 5]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
[process 5]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot
[process 5]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign
[process 5]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere
[process 5]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\WAB\WAB4\Wab File Name
[process 5]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\
[process 5]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\WAB\
[process 5]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\WAB\WAB4\

Set Values	
	key
[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: AppData
[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 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\Itquuxusow Value: f082ee56
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache Value: C:\Documents and Settings\Charlie\Local Settings\Temp\Zyoka\ivyk.exe
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\SessionInformation Value: ProgramCount
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Itquuxusow Value: e23741b8
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: ivyk
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Itquuxusow Value: e23741b8
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC Value: LDAP Server ID
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot Value: LDAP Server ID
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign Value: LDAP Server ID
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere

	Value: LDAP Server ID
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager
	Value: Server ID
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts
	Value: PreConfigVer
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts
	Value: PreConfigVerNTDS
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: Account Name
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP Server
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP Search Return
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP Timeout
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP Authentication
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP Simple Search
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP Bind DN
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP Port
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP Resolve Flag
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP Secure Connection
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP User Name
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC
	Value: LDAP Search Base
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot
	Value: Account Name
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot

	Value: LDAP Server
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot
	Value: LDAP URL
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot
	Value: LDAP Search Return
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot
	Value: LDAP Timeout
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot
	Value: LDAP Authentication
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot
	Value: LDAP Simple Search
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot
	Value: LDAP Logo
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign
	Value: Account Name
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign
	Value: LDAP Server
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign
	Value: LDAP URL
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign
	Value: LDAP Search Return
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign
	Value: LDAP Timeout
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign
	Value: LDAP Authentication
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign
	Value: LDAP Search Base
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign
	Value: LDAP Simple Search
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\VeriSign
	Value: LDAP Logo
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere
	Value: Account Name
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere

	Value: LDAP Server
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere
	Value: LDAP URL
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere
	Value: LDAP Search Return
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere
	Value: LDAP Timeout
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere
	Value: LDAP Authentication
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere
	Value: LDAP Simple Search
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere
	Value: LDAP Logo
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager
	Value: Default LDAP Account
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Account Manager
	Value: Server ID
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\WAB\WAB4\Wab File Name
	Value:
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\WAB\WAB4
	Value: OlkContactRefresh
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\WAB\WAB4
	Value: OlkFolderRefresh
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Identities
	Value: Identity Ordinal
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Itquuxusow
	Value: e23741b8
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
	Value: Seed

Deleted Values	
	key
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Identities
	Value: Changing
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Identities
	Value: IncomingID
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Identities
	Value: OutgoingID

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process 3]	127.0.0.1	0.0.0.0	none

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

DNS Requests	
Request	**Result**
1ut5c3u1gkdnzna2omap10t7vyq.net	NONE
1l0tqu8xm18wik3yqf51ji165s.org	NONE
lv0nhm1o8v4x8azx0o91tcgphx.net	NONE
cfd5th1qrgpr01nbuy5y1yvdxn1.com	NONE
1gdfa2ccub43f16f0ru119j0rd3.org	NONE
1hhhw1y1k7l3fdl55hw81mqfmm1.biz	NONE
ustxcq7f8v6fcgxkw6my9xy3.net	NONE
1ek2bl0oqae8t17flfc41geafhv.com	NONE
1rkaw2p15t6r4s7sdpvs14h53vg.net	NONE
yz8kjira178e1s7j6wnmyx0ko.biz	NONE
1jmidqo1107g251y15ahp1b18m01.org	NONE
18zvel51r9gzpt1k5v4mj129j7bi.com	NONE
uisl72jkabp15cl8p320reiu.net	NONE
16vpsga962lru1x4rl3h1lqad7v.org	NONE
1npwu6g3bl3sl1b1ok5y1tqk0ot.net	NONE
n4udsi13twso0owts6br549mb.com	NONE
1ty9xxe1kkts0c5e73kj1j0fe7x.org	NONE
1prq17b1d67cejzbh7d01f5oefe.biz	NONE
1ixciai2wl7fr60phhc1r43ut2.net	NONE
s22x39bpa8r515szfg51tie3k.com	NONE
1as21n3v1w2e0rwc319ot8syr.net	NONE
1pcux02u8xauoxmsra84rga0e.biz	NONE
iideh71hv1cm8on533k15oklyp.org	NONE
1xkm742fknl0ia7drjv1l5h8z7.com	NONE
45157270b8jf13rxoyh1763v33.net	NONE
1ml8fhl1prnw7b5juw8b1k9vf90.org	NONE
1fnodbh1riq3h3p3ftfw22yi84.net	NONE
1kvq1m44blm5vzokno411hnk0t.com	NONE
dv3pr5cop3pzz32v0w11a724b.org	NONE
13xg79q3orpxg1pqo0xi15f7i33.biz	NONE
mbm0l3lldaebtdkdjad38u4t.net	NONE
5mip3b26ykcr14pxexh10sdgpr.com	NONE
1kkcju1ndoo924wmyhw1xnr9lu.net	NONE
v1ttk5ah8hlg27q8pofsjou2.biz	NONE
npohos18brqi1ywvbb316husgo.org	NONE
1n1rvxrsrpnz51xy4nf81l2g44q.com	NONE
1rnle2h1myq9qsw8mxs1demc49.net	NONE
fjd521q9njg01vg973t1k1gzx8.org	NONE
wycuord15wzhxhfykhf1yryt.net	NONE
lx3me8n224nmky7gwfbayd42.com	NONE
1aa24alrbml0se7hb661ycmgtv.org	NONE
1t2qncg1xj4hzfwhfj9asl7cor.biz	NONE
1n2icuzujfs221x6xn311xq17xo.net	NONE
1kzgqdk1y2vo3717lq4q3hipdix.com	NONE

Virus Total Results	
Last Scanned:	**2014-09-10 12:28:13**
Bkav:	HW32.Paked.D48D
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Not Detected
Malwarebytes:	Not Detected
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
NANO-Antivirus:	Not Detected
Cyren:	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
ViRobot:	Not Detected
SUPERAntiSpyware:	Not Detected
ByteHero:	Not Detected
Ad-Aware:	Not Detected
Comodo:	Not Detected
VIPRE:	Not Detected
McAfee-GW-Edition:	Not Detected
Emsisoft:	Not Detected
F-Prot:	Not Detected
Jiangmin:	Not Detected
Avira:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
AegisLab:	Not Detected
GData:	Not Detected
AhnLab-V3:	Not Detected
AVware:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	Not Detected
Tencent:	Not Detected
Fortinet:	Not Detected
Baidu-International:	Not Detected

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