Analysis # 2621

09/15/2014 06:15 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 10
Created Keys 10
Set Values 11
Deleted Values 15
Network Activity 16
Network Events 16
Network Traffic 17
DNS Requests 18
Virus Total Results 19

Analysis Summary

Submitted File:	333.exe
MD5:	e33a9ba53fd5377dd7817266d4c89c01
File Size:	226152
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-09-15 06:15:36
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Mon, 15 Sep 2014 15:20:19 +0000
Termination Time:	Mon, 15 Sep 2014 15:20:22 +0000
Analysis Time:	2014-09-15 06:15:36
Sandbox:	XP-SP2 - 00-0C-29-B2-D2-62
Total Processes:	7
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 7] C:\333.exe

Stored Modified Files
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temp\Ovyl\fuce.exe
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\QZSB028.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\{2996F1E5-654B-3381-8099-7F4264E87AB9}
	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\{2996F1E5-654B-3381-389C-7F42DCED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-149F-7F42F0EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-A89F-7F424CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-909F-7F4274EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-E49F-7F4200EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-D89F-7F423CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-B498-7F4250E97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-E498-7F4200E97AB9}

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-7899-7F429CE87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-4C99-7F42A8E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-9099-7F4274E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-1C9B-7F42F8EA7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-649B-7F4280EA7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-E49C-7F4200ED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-089E-7F42ECEF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-E09E-7F4204EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-389F-7F42DCEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-989D-7F427CEC7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-2099-7F42C4E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{2996F1E5-654B-3381-4C9E-7F42A8EF7AB9}
	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\{2996F1E5-654B-3381-389C-7F42DCED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 3]	Name: Global\{2996F1E5-654B-3381-149F-7F42F0EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-A89F-7F424CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-909F-7F4274EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-E49F-7F4200EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-D89F-7F423CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-B498-7F4250E97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-E498-7F4200E97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-7899-7F429CE87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-4C99-7F42A8E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-9099-7F4274E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-649B-7F4280EA7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-E49C-7F4200ED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-089E-7F42ECEF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-E09E-7F4204EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-389F-7F42DCEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-989D-7F427CEC7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-2099-7F42C4E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{2996F1E5-654B-3381-C898-7F422CE97AB9}
	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 7]	Name: Global\{C7A62370-B7DE-DDB1-6BF3-F5458F82F0BE}
	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

Created Keys	
	key
[process 1]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Zupicoke
[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\Zupicoke Value: 64aa7fbd
[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\Ovyl\fuce.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\Zupicoke Value: 761fd053
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: fuce
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Zupicoke Value: 761fd053
[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\Zupicoke
	Value: 761fd053
[process 7]	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**
s9gin91jmn1o41bjzjex100mbps.biz	NONE
887ft2cdlx16n4tvvb157audv.org	NONE
1msuqh7bn8ahz1xgv9lbv8gzej.com	NONE
jr9calqwok0jt8x3j7xvkxqk.net	NONE
3q3chi59db01qrzx5yobgezk.org	NONE
oz36c6l0m13p1ls5wv71r0kj81.net	NONE
1gtitiu1hj7ziby2t17213bvmwr.com	NONE
feen51410ooo15clid6g130lj.org	NONE
ey5v7u1upkirtqa84gfv2jsx4.biz	NONE
163jqqn14c0n360ldu91fmq1t5.net	NONE
1yh9s5m1gg7xfzpodqq41eluz7f.com	NONE
6ny5pu1vzjltu1ax02pxwx435d.net	NONE
1kixnpd1086wlt17x24kv8n380i.biz	NONE
1ftq8hs188p9avb8atoi2van4t.org	NONE
1ot78bm1igsw49iew6yc3917qg.com	NONE
m3j0z618sq4ya8xlms21iing86.net	NONE
iwrj061w2wdg1xd1nybum1tif.org	NONE
kjao1m1g0ki8p5srqb1182lgg.net	NONE
1wmhk294snt0a5g93tnmobuwp.com	NONE
h25gbosuwkfksjw2z51mjukh0.org	NONE
o5ffp51hylo2q11jhams1e73y8n.biz	NONE
rt0mrh8iu5xj1sns2b31s2hww6.net	NONE
1hbn34uqrup7a13tewkp5q624a.com	NONE
qmr30zoyswr21cdxolg1oyxy6n.net	NONE
198dvp51u4obij101rhkjf75m6b.biz	NONE
1qmqnbetqx2h61997e3wioxtoa.org	NONE
1b5f8uzv26q2qvdjjrkiljqt.com	NONE
1gb3q971tbjlrd18ft2uh5tsmz5.net	NONE
1efbtogsmutk2zyhh6czimwgp.org	NONE
k1gt6r19jmt6fx2agaxp2vxxl.net	NONE
g0dha01iqc3c1on0yqp1m61h4b.com	NONE
x8ccf41mdxlqm1mok81014bzu6s.org	NONE
1oy1sb71jyrccc1vscury84q4bs.biz	NONE
czb9lpxhzfxl6jwt9czfrq2.net	NONE
43kky91vtwoaplwv92q1cnxmkb.com	NONE
1t932ij11gaayiesv0gdbk2knu.net	NONE
1cv2fd11ta4oml6ollbu16js9qg.biz	NONE
ig5fgwxxiiic1pi2v441varm1h.org	NONE
13t1g4gbvvf2e2reoxq1se45ix.com	NONE
kg8fwac5dixpttql9r1deq8x6.net	NONE

Virus Total Results	
Last Scanned:	**2014-09-15 10:19:06**
Bkav:	HW32.Paked.69FE
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Not Detected
Malwarebytes:	Not Detected
VIPRE:	Not Detected
SUPERAntiSpyware:	Not Detected
TheHacker:	Not Detected
K7GW:	Not Detected
K7AntiVirus:	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
Tencent:	Not Detected
Ad-Aware:	Not Detected
Emsisoft:	Not Detected
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
Zillya:	Not Detected
TrendMicro:	Not Detected
McAfee-GW-Edition:	Not Detected
Sophos:	Not Detected
Cyren:	Not Detected
Jiangmin:	Not Detected
Avira:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
ViRobot:	Not Detected
AhnLab-V3:	Spyware/Win32.Zbot
GData:	Not Detected
ByteHero:	Not Detected
VBA32:	Not Detected
AVware:	Not Detected
Panda:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	Not Detected
Rising:	Not Detected
Ikarus:	Not Detected
Fortinet:	Not Detected
AVG:	Not Detected
Baidu-International:	Not Detected
Qihoo-360:	Not Detected

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