Analysis # 2642

09/16/2014 05:34 am

Table of Contents

Analysis Summary

Submitted File:	invoice_38898221_spt.exe
MD5:	2fb8c677c92b92eb2d1359f02c1dc10f
File Size:	254976
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-09-16 05:34:16
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Tue, 16 Sep 2014 09:39:01 +0000
Termination Time:	Tue, 16 Sep 2014 09:39:04 +0000
Analysis Time:	2014-09-16 05:34:16
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_38898221_spt.exe

Stored Modified Files
[process 1] C:\Documents and Settings\Charlie\Local Settings\Temp\Gapi\avezys.exe
[process 1] C:\DOCUME~1\Charlie\LOCALS~1\Temp\JSSB288.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\{51EB0BBF-9F11-4BFC-9499-7F4270E87AB9}
	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\{51EB0BBF-9F11-4BFC-389C-7F42DCED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-149F-7F42F0EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-A89F-7F424CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-909F-7F4274EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-E49F-7F4200EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-D89F-7F423CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-B898-7F425CE97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-E898-7F420CE97AB9}

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-7C99-7F4298E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-4C99-7F42A8E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-8C99-7F4268E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-0C9B-7F42E8EA7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-689B-7F428CEA7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-E49C-7F4200ED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-149E-7F42F0EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-E09E-7F4204EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-3C9F-7F42D8EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-A49D-7F4240EC7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{51EB0BBF-9F11-4BFC-0C9E-7F42E8EF7AB9}
	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\{51EB0BBF-9F11-4BFC-389C-7F42DCED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-149F-7F42F0EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-A89F-7F424CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-909F-7F4274EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-E49F-7F4200EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-D89F-7F423CEE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-B898-7F425CE97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-E898-7F420CE97AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-7C99-7F4298E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-4C99-7F42A8E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-8C99-7F4268E87AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-689B-7F428CEA7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-E49C-7F4200ED7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-149E-7F42F0EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-E09E-7F4204EF7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-3C9F-7F42D8EE7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-A49D-7F4240EC7AB9}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{51EB0BBF-9F11-4BFC-649D-7F4280EC7AB9}
	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\Yjdovyyr
[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\Yjdovyyr Value: 6f3a2c69
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Yjdovyyr Value: 7d8f8387
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: avezys
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Yjdovyyr Value: 7d8f8387
[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 Ac

	count Manager\Accounts
	Value: PreConfigVer
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac
	count Manager\Accounts
	Value: PreConfigVerNTDS
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac
	count 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 Ac
	count 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 Ac
	count 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 Ac
	count 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 Ac
	count 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 Ac
	count 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 Ac
	count 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 Ac
	count 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 Ac
	count 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 Ac
	count 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 Ac
	count 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 Ac
	count 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 Ac
	count Manager\Accounts\Bigfoot
	Value: Account Name
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac
	count Manager\Accounts\Bigfoot
	Value: LDAP Server
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac
	count Manager\Accounts\Bigfoot
	Value: LDAP URL
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac

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

	count Manager\Accounts\WhoWhere
	Value: LDAP Search Return
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac
	count Manager\Accounts\WhoWhere
	Value: LDAP Timeout
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac
	count Manager\Accounts\WhoWhere
	Value: LDAP Authentication
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac
	count Manager\Accounts\WhoWhere
	Value: LDAP Simple Search
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac
	count Manager\Accounts\WhoWhere
	Value: LDAP Logo
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac
	count Manager
	Value: Default LDAP Account
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Internet Ac
	count Manager
	Value: Server ID
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\WAB\WAB4\Wa
	b 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\Yjdovyyr
	Value: 7d8f8387
[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**
1vzsb5q1x1vvj21qj23q61yfan2h.org	NONE
1pq0v1bthue0l9h2fwp16iiywo.biz	NONE
bma6201nldzpkjtwatm15t8aec.net	NONE
uq20le4gth831oimq761up8qu7.com	NONE
vd5ehl4jh7xbwoo8131vtg7pg.net	NONE
f689331x75qke18z1div1xkaci2.biz	NONE
uc875to326ty1dm35mh1ruhyd3.org	NONE
12evutg14krf01vgj73r1ulox9g.com	NONE
tmrfnq1lrralu1qs2kvqbe4ftv.net	NONE
1gt8d5b1oqx63t1vj5zyw1fekffm.org	NONE
1jcuwxye36jmm1go343b168yiwv.net	NONE
fds8pkbelcs21nkjo051a1apnp.com	NONE
1vo6znmsmldvf1tdzhnvi57uln.org	NONE
1wr2oxl118kqx95z98rv198086i.biz	NONE
1ut36utj248lpyc6dwgblrn3c.net	NONE
iuag93v6ode9ulsffz1sbraln.com	NONE
mwquj71vtft0w6j3a9972jc50.net	NONE
17jfjwn1x2q2w6gc6ruk3xbcr8.biz	NONE
1clb0hp151qvmhofxlw512ckcu1.org	NONE
12wu3r11vt60qq1s2lzu71bueme7.com	NONE
fg63o21xnv0d2180w6m6x7s7y4.net	NONE
whrzfp1rxrxte1p2r0u51utzaph.org	NONE
1avp7onngzo66qip0wu1jmemir.net	NONE
1m8hiykaaua4413xbrhk1lmw17o.com	NONE
1xxiqxoe3du6e12h4kabnfj9i.org	NONE
1260e8peum7p38bcaqz1g2jcvk.biz	NONE
r3v6jr1oqm4x011it2z4fn7b7e.net	NONE
98npnghzwwg31y36w491q7zqih.com	NONE
1xukonqmfmwztbbbzhc1600cz9.net	NONE
8vu8dx1fub7s1imdjkz1wjtqcj.biz	NONE
13b86181g57wia17hq7stqxxtgw.org	NONE
mev5rc1ee8cmi9142bj476jcv.com	NONE
1xfwjtzfo5uiqh54mqv1241o8r.net	NONE
xepcwjyxc05w1hlnu2v1ah57g7.org	NONE
f1zwz1oojoxy1snojvd1yn6rbq.net	NONE
as5bn6uhogoz1sopx6z1vqlpky.com	NONE
1gnvi7yp0wzkt1huhm731815n5g.org	NONE
1uot2ho89d8b65qasb91remknp.biz	NONE
1o7vqy51qnm23gormf47auqnhg.net	NONE
pp6ee9khspt1cj6o6o136f6qr.com	NONE
10nuulbsszke1x3m12z1w1d97y.net	NONE
44zvcjnoowov189bfig1ja6b6s.biz	NONE
sal69016g8e6a116mncv18ks942.org	NONE

Virus Total Results	
Last Scanned:	**2014-09-16 09:05:50**
Bkav:	HW32.Paked.DD29
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
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
Agnitum:	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
NANO-Antivirus:	Not Detected
ViRobot:	Not Detected
Rising:	PE:Malware.FakePDF@CV!1.9C3A
Ad-Aware:	Not Detected
Sophos:	Not Detected
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
Zillya:	Not Detected
McAfee-GW-Edition:	Not Detected
Emsisoft:	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
Panda:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	Not Detected
Tencent:	Win32.Trojan.Bp-generic.Ixrn
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