



Analysis # 30639

05/16/2013 06:11 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	9
Created Keys	9
Deleted Keys	10
Set Values	11
Deleted Values	14
Network Activity	15
Network Events	15
Network Traffic	16
DNS Requests	17
Screen Shots	18
Virus Total Results	19

Analysis Summary	
Submitted File:	VAT_Returns_Repot_517794350.doc
MD5:	f49ba87bdcbb24ecf22f9b5b3a8c2a34
File Size:	475519
File Type:	Rich Text Format data, version 1, ANSI
Analysis Time:	2013-05-16 06:11:17
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Thu, 16 May 2013 10:14:32 +0000
Termination Time:	Thu, 16 May 2013 10:14:46 +0000
Analysis Time:	2013-05-16 06:11:17
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	13
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 10] C:\Documents and Settings\Administrator\Application Data\Kuzuj\lewfaqu.exe

[process 13] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Winword.exe

[process 13] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmpcd7e8f26.bat

Stored Modified Files
[process 1] C:\VAT_Returns_Repot_517794350.doc
[process 1] C:\~\$T_Returns_Repot_517794350.doc
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Winword.exe
[process 10] C:\Documents and Settings\Administrator\Application Data\Kuzuj\lewfaqu.exe
[process 10] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 10] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 10] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 10] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 10] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 10] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 10] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmpcd7e8f26.bat

Created Mutexes	
	mutex
[process 2]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: SHIMLIB_LOG_MUTEX 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
[process 7]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Global\{5B039399-8854-D5EB-89D3-085A9A492B48} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: MPSWabDataAccessMutex Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: MPSWABOIkStoreNotifyMutex Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: MSIdent Logon Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-9B8C-B06D8816937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Local\{E41AB6D2-AD1F-6AF2-89D3-085A9A492B48} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-238C-B06D3016937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-F38E-B06DE014937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-578F-B06D4415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-B78F-B06DA415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-9B8F-B06D8815937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-EF8F-B06DFC15937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-4F88-B06D5C12937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-8B88-B06D9812937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-0389-B06D1013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-7389-B06D6013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-8389-B06D9013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-7F8B-B06D6C11937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-5B8B-B06D4811937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-FF8D-B06DEC17937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-DB8D-B06DC817937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-1B8E-B06D0814937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-778E-B06D6414937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-778F-B06D6415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-378B-B06D2411937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-8F8B-B06D9C11937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-CF88-B06DDC12937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{2CBCD669-CDA4-A254-FF8C-B06DEC16937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-0F8B-B06D1C11937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{7EB084F0-9F3D-F058-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{A8B6B2C3-A90E-265E-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{A45A65F1-7E3C-2AB2-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{A45A65F6-7E3B-2AB2-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Local\{C5BCD3E2-C82F-4B54-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Local\{C5BCD3E3-C82E-4B54-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-238C-B06D3016937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-F38E-B06DE014937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-578F-B06D4415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-B78F-B06DA415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 12]	Name: Global\{2CBCD669-CDA4-A254-9B8F-B06D8815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-EF8F-B06DFC15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-4F88-B06D5C12937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-8B88-B06D9812937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-0389-B06D1013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-7389-B06D6013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-8389-B06D9013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-5B8B-B06D4811937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-FF8D-B06DEC17937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-DB8D-B06DC817937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-1B8E-B06D0814937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-778E-B06D6414937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-778F-B06D6415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-378B-B06D2411937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-8F8B-B06D9C11937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 12]	Name: Global\{2CBCD669-CDA4-A254-CF88-B06DDC12937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 13]	Name: Global\{2CBCD669-CDA4-A254-338A-B06D2010937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 13]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 10]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa
[process 10]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name
[process 10]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB
[process 10]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4
[process 10]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name
[process 12]	\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List
[process 12]	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\
[process 12]	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\

Deleted Keys	
	key
[process 3]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Office\14.0\Word\Resil iency\StartupItems

Set Values	
	key
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: ProductNonBootFiles
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: 16413e27
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

	Value: AppData
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Internet Account Manager Value: Server ID
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name Value:
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkContactRefresh
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkFolderRefresh
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Identity Ordinal
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: 16413e27
[process 11]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 11]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 11]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 11]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: 19dfebi9
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: 16413e27
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 12]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 12]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta

	ndardProfile\GloballyOpenPorts>List Value: 24759:UDP
[process 12]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 12]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 12]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts>List Value: 25946:TCP
[process 12]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: 2gagf50b
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: hd60cde
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: 2ai2gbe
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: 2ai2gbe
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: hd60cde
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: 2ai2gbe
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: 2ai2gbe
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\lgysa Value: 2ai2gbe
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 12]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 13]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

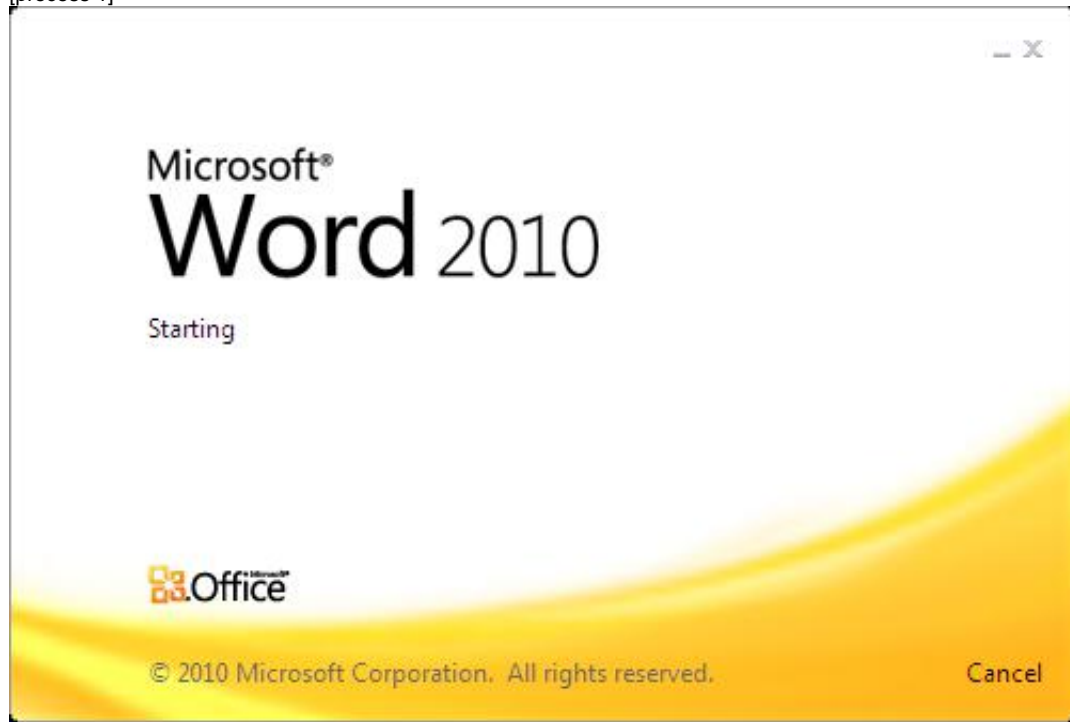
Deleted Values	
	key
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Changing
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: IncomingID
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: OutgoingID

Network Events			
	Remote IP	Local IP	HTTP Command
[process 12]	86.124.111.218	10.20.25.247	none
[process 12]	76.245.44.216	10.20.25.247	none
[process 12]	92.241.139.165	10.20.25.247	none
[process 12]	76.245.44.216	10.20.25.247	none
[process 12]	62.103.27.242	10.20.25.247	none
[process 12]	190.42.161.35	10.20.25.247	none
[process 12]	122.179.128.38	10.20.25.247	none
[process 12]	190.42.161.35	10.20.25.247	none
[process 12]	189.223.139.172	10.20.25.247	none

Network Traffic		
	Remote IP	Local IP
Connection #1	10.20.25.255	10.20.25.247
Connection #2	86.124.111.218	10.20.25.247
Connection #3	76.245.44.216	10.20.25.247
Connection #4	92.241.139.165	10.20.25.247
Connection #5	76.245.44.216	10.20.25.247
Connection #6	62.103.27.242	10.20.25.247
Connection #7	190.42.161.35	10.20.25.247
Connection #8	122.179.128.38	10.20.25.247
Connection #9	190.42.161.35	10.20.25.247

DNS Requests	
Request	Result
No activity	--

[process 1]



Virus Total Results	
Last Scanned:	2013-05-16 10:05:19
MicroWorld-eScan:	Not Detected
nProtect:	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
F-Prot:	Not Detected
Symantec:	Not Detected
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	Not Detected
Avast:	Not Detected
eSafe:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Not Detected
Agnitum:	Not Detected
SUPERAntiSpyware:	Not Detected
Emsisoft:	Not Detected
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
VIPRE:	Not Detected
AntiVir:	Not Detected
TrendMicro:	HEUR_RTFMALFORME
McAfee-GW-Edition:	Not Detected
Sophos:	Not Detected
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
ViRobot:	Not Detected
AhnLab-V3:	Not Detected
GData:	Not Detected
Commtouch:	Not Detected
ByteHero:	Not Detected
VBA32:	Not Detected
PCTools:	Not Detected
ESET-NOD32:	Not Detected
Ikarus:	Not Detected
Fortinet:	Not Detected
AVG:	Not Detected
Panda:	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

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.