



## **Analysis # 30261**

**04/26/2013 05:11 am**

## Table of Contents

<b>Analysis Summary</b>	<b>3</b>
<b>Analysis Summary</b>	<b>3</b>
<b>Digital Behavior Traits</b>	<b>3</b>
<b>File Activity</b>	<b>4</b>
<b>Deleted Files</b>	<b>4</b>
<b>Stored Modified Files</b>	<b>5</b>
<b>Created Mutexes</b>	<b>6</b>
<b>Created Mutexes</b>	<b>6</b>
<b>Registry Activity</b>	<b>9</b>
<b>Created Keys</b>	<b>9</b>
<b>Set Values</b>	<b>10</b>
<b>Deleted Values</b>	<b>14</b>
<b>Network Activity</b>	<b>15</b>
<b>Network Events</b>	<b>15</b>
<b>Network Traffic</b>	<b>16</b>
<b>DNS Requests</b>	<b>17</b>
<b>Virus Total Results</b>	<b>18</b>

Analysis Summary	
Submitted File:	LABEL_ID_56753547_GFK72.exe
MD5:	df81b21e9526c571d03bc1fb189f233c
File Size:	297984
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-04-26 05:11:59
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Fri, 26 Apr 2013 09:14:31 +0000
Termination Time:	Fri, 26 Apr 2013 09:14:36 +0000
Analysis Time:	2013-04-26 05:11:59
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	4
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 1] C:\Documents and Settings\Administrator\Application Data\Jefeaf\ufor.exe

[process 4] C:\LABEL\_ID\_56753547\_GFK72.exe

[process 4] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp8caad4f4.bat

Stored Modified Files
[process 1] C:\Documents and Settings\Administrator\Application Data\Jefeaf\ufor.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp8caad4f4.bat
[process 4] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 4] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 4] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 4] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 4] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab

Created Mutexes	
	mutex
[process 1]	Name: Global\{5B039399-8854-D5EB-89D3-085A9A492B48} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-FF89-B06DEC13937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\{E41AB6D2-AD1F-6AF2-89D3-085A9A492B48} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-238C-B06D3016937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-F38E-B06DE014937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-578F-B06D4415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-B78F-B06DA415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-9B8F-B06D8815937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-EF8F-B06DFC15937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-4F88-B06D5C12937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-8B88-B06D9812937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-0389-B06D1013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-7B89-B06D6813937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-AB89-B06DB813937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-2B8B-B06D3811937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-BF8B-B06DAC11937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-FB8D-B06DE817937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-278E-B06D3414937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-678E-B06D7414937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-778E-B06D6414937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-778F-B06D6415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-2789-B06D3413937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-F389-B06DE013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{1802AB04-B0C9-96EA-1388-B06D0012937F}

[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-C38A-B06DD010937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{7EB084F0-9F3D-F058-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{A8B6B2C3-A90E-265E-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{A45A65F1-7E3C-2AB2-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{A45A65F6-7E3B-2AB2-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Local\{C5BCD3E2-C82F-4B54-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Local\{C5BCD3E3-C82E-4B54-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-238C-B06D3016937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-F38E-B06DE014937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-578F-B06D4415937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-B78F-B06DA415937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-9B8F-B06D8815937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-EF8F-B06DFC15937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-4F88-B06D5C12937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-8B88-B06D9812937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-0389-B06D1013937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-7B89-B06D6813937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-AB89-B06DB813937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-BF8B-B06DAC11937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-FB8D-B06DE817937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-278E-B06D3414937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-678E-B06D7414937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-778E-B06D6414937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{1802AB04-B0C9-96EA-778F-B06D6415937F}

[process 3]	Name: Global\{1802AB04-B0C9-96EA-2789-B06D3413937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{1802AB04-B0C9-96EA-F389-B06DE013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{1802AB04-B0C9-96EA-B78A-B06DA410937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{1802AB04-B0C9-96EA-EF8E-B06DFC14937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{1802AB04-B0C9-96EA-0F8B-B06D1C11937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{1802AB04-B0C9-96EA-EF8C-B06DFC16937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{1802AB04-B0C9-96EA-078F-B06D1415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{1802AB04-B0C9-96EA-C389-B06DD013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{1802AB04-B0C9-96EA-2F8A-B06D3C10937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{1802AB04-B0C9-96EA-0789-B06D1413937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{1802AB04-B0C9-96EA-CF8D-B06DDC17937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{1802AB04-B0C9-96EA-CF8F-B06DDC15937F}
	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 4]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: MPSWabDataAccessMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: MPSWABOIkStoreNotifyMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE



Created Keys	
	key
[process 1]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz
[process 3]	\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List
[process 3]	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\
[process 3]	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\
[process 4]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name
[process 4]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\
[process 4]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\
[process 4]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\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-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: AppData
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: Local 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\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\O taz Value: 195d9ej0
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: AppData
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: Local AppData
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\O taz Value: 1cf7ac2a
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\O taz Value: 195d9ej0
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta ndardProfile Value: DisableNotifications
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta ndardProfile\GloballyOpenPorts\List Value: 26020:UDP
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta

	ndardProfile Value: DisableNotifications
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List Value: 21657:TCP
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 2hd2ac6g
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 1b44gfd
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 1b44gfd
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 1b44gfd
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 1b44gfd
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 1b44gfd
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 1b44gfd
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 1b44gfd
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 1b44gfd
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 1b44gfd
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1

[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 10ehj8g1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Internet Acc ount Manager Value: Server ID
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name Value:
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4

	Value: OlkContactRefresh
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkFolderRefresh
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Identity Ordinal
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Otaz Value: 195d9ej0

Deleted Values	
	key
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Changing
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: IncomingID
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: OutgoingID

Network Events			
	Remote IP	Local IP	HTTP Command
[process 3]	66.130.42.12	10.20.25.247	none
[process 3]	66.63.204.26	10.20.25.247	none
[process 3]	66.130.42.12	10.20.25.247	none
[process 3]	212.70.206.102	10.20.25.247	none
[process 3]	108.74.172.39	10.20.25.247	none
[process 3]	76.29.46.47	10.20.25.247	none
[process 3]	180.248.91.99	10.20.25.247	none
[process 3]	82.51.81.152	10.20.25.247	none
[process 3]	71.193.224.27	10.20.25.247	none
[process 3]	64.231.248.224	10.20.25.247	none
[process 3]	194.94.127.98	10.20.25.247	none
[process 3]	86.162.2.123	10.20.25.247	none
[process 3]	24.120.165.58	10.20.25.247	none
[process 3]	190.77.38.235	10.20.25.247	none
[process 3]	178.91.20.145	10.20.25.247	none
[process 3]	90.227.234.152	10.20.25.247	none
[process 3]	85.250.14.253	10.20.25.247	none
[process 3]	199.59.157.124	10.20.25.247	none
[process 3]	195.169.125.228	10.20.25.247	none
[process 3]	76.20.214.12	10.20.25.247	none
[process 3]	76.121.100.21	10.20.25.247	none
[process 3]	182.73.194.126	10.20.25.247	none
[process 3]	183.88.92.48	10.20.25.247	none
[process 3]	4.28.159.10	10.20.25.247	none
[process 3]	114.143.33.171	10.20.25.247	none
[process 3]	77.184.218.83	10.20.25.247	none
[process 3]	24.181.177.1	10.20.25.247	none

Network Traffic		
	Remote IP	Local IP
Connection #1	10.20.25.255	10.20.25.247
Connection #2	66.130.42.12	10.20.25.247
Connection #3	66.63.204.26	10.20.25.247
Connection #4	212.70.206.102	10.20.25.247
Connection #5	108.74.172.39	10.20.25.247
Connection #6	212.70.206.102	10.20.25.247
Connection #7	108.74.172.39	10.20.25.247
Connection #8	76.29.46.47	10.20.25.247
Connection #9	108.74.172.39	10.20.25.247
Connection #10	76.29.46.47	10.20.25.247
Connection #11	180.248.91.99	10.20.25.247
Connection #12	82.51.81.152	10.20.25.247
Connection #13	71.193.224.27	10.20.25.247
Connection #14	64.231.248.224	10.20.25.247
Connection #15	194.94.127.98	10.20.25.247
Connection #16	86.162.2.123	10.20.25.247
Connection #17	24.120.165.58	10.20.25.247
Connection #18	190.77.38.235	10.20.25.247
Connection #19	178.91.20.145	10.20.25.247
Connection #20	90.227.234.152	10.20.25.247
Connection #21	85.250.14.253	10.20.25.247
Connection #22	199.59.157.124	10.20.25.247
Connection #23	195.169.125.228	10.20.25.247
Connection #24	76.20.214.12	10.20.25.247
Connection #25	76.121.100.21	10.20.25.247
Connection #26	182.73.194.126	10.20.25.247
Connection #27	183.88.92.48	10.20.25.247
Connection #28	4.28.159.10	10.20.25.247
Connection #29	114.143.33.171	10.20.25.247
Connection #30	77.184.218.83	10.20.25.247



DNS Requests	
Request	Result
No activity	--

Virus Total Results	
<b>Last Scanned:</b>	<b>2013-04-26 09:13:33</b>
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Dropper-FEB!DF81B21E9526
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:	Worm.Win32.Luder.rlh
BitDefender:	Not Detected
Agnitum:	Not Detected
SUPERAntiSpyware:	Not Detected
Sophos:	Not Detected
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
VIPRE:	Not Detected
AntiVir:	Not Detected
TrendMicro:	Not Detected
McAfee-GW-Edition:	Not Detected
Emsisoft:	PWS.Win32.Zbot.AMN (A)
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	PWS:Win32/Zbot.gen!AM
ViRobot:	Not Detected
AhnLab-V3:	Not Detected
GData:	Not Detected
CommTouch:	W32/Trojan.GNAF-6198
ByteHero:	Not Detected
VBA32:	Not Detected
PCTools:	Not Detected
ESET-NOD32:	Not Detected
Ikarus:	Not Detected
Fortinet:	W32/ZeroAccess.NDY!tr
AVG:	Not Detected
Panda:	Suspicious file

**ThreatTrack Security, Inc.**

33 North Garden Avenue, Suite 1200, Clearwater, Florida, USA 33755

Telephone: (855) 443-4284 Intl: +1(813)367-9907

Email: [Sales@ThreatTrack.com](mailto:Sales@ThreatTrack.com)

Disclaimer © 2013. ThreatTrack Security, Inc. All rights reserved. All product and company names herein may be trademarks of their respective owners. The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. ThreatTrack Security, Inc. is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, ThreatTrack Security makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. ThreatTrack Security makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.