Analysis # 33106

09/25/2013 13:35 pm

Table of Contents

Analysis Summary

Submitted File:	Invoice_092513.exe
MD5:	b9c4166cd597a5d9f49127d1bc13ae01
File Size:	26624
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-09-25 13:35:53
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Wed, 25 Sep 2013 17:36:44 +0000
Termination Time:	Wed, 25 Sep 2013 17:37:17 +0000
Analysis Time:	2013-09-25 13:35:53
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
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 2] C:\Invoice_092513.exe
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\CabF.tmp
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Tar10.tmp
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Cab11.tmp
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Tar12.tmp
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Cab13.tmp
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Tar14.tmp
[process 7] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\wezedame.exe
[process 7] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\KJHAE19.bat

Stored Modified Files
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\wezeda.exe
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\CabF.tmp
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Tar10.tmp
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Cab11.tmp
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Tar12.tmp
[process 2] C:\Documents and Settings\Administrator\Application Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004
[process 2] C:\Documents and Settings\Administrator\Application Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004
[process 2] C:\Documents and Settings\Administrator\Application Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015
[process 2] C:\Documents and Settings\Administrator\Application Data\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Cab13.tmp
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Tar14.tmp
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\wezedame.exe
[process 3] C:\Documents and Settings\Administrator\Application Data\Guuwhi\uzta.exe
[process 3] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 3] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 3] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 3] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 3] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 3] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\KJHAE19.bat

Created Mutexes	
	mutex
[process 1]	Name: Groove:PathMutex:YoNgf9TlAyd0477wzgfiTWi4XXU=
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\ZonesCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\c:!documents and settings!administrator!local settings!temporary internet files!content.
	ie5!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\c:!documents and settings!administrator!cookies!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\c:!documents and settings!administrator!local settings!history!history.ie5!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\WininetConnectionMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZonesCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Groove:PathMutex:YoNgf9TlAyd0477wzgfiTWi4XXU=
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{5B039399-8854-D5EB-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: MPSWabDataAccessMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: MPSWABOlkStoreNotifyMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: MSIdent Logon
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-838E-B06D9014937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\{E41AB6D2-AD1F-6AF2-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-238C-B06D3016937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-F78E-B06DE414937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 4]	Name: Global\{4B9139DE-2213-C579-578F-B06D4415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-B78F-B06DA415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-9B8F-B06D8815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-EF8F-B06DFC15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-4F88-B06D5C12937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-8B88-B06D9812937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-0389-B06D1013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-7389-B06D6013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-AB89-B06DB813937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-FB8A-B06DE810937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-EB8B-B06DF811937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-6F8D-B06D7C17937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-0F8E-B06D1C14937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-1B8E-B06D0814937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-2B8F-B06D3815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-BF8A-B06DAC10937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{4B9139DE-2213-C579-EB89-B06DF813937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-DF83-B06DCC19937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{7EB084F0-9F3D-F058-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{A8B6B2C3-A90E-265E-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{A45A65F1-7E3C-2AB2-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{A45A65F6-7E3B-2AB2-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\{C5BCD3E2-C82F-4B54-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\{C5BCD3E3-C82E-4B54-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-238C-B06D3016937F}

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-F78E-B06DE414937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-578F-B06D4415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-B78F-B06DA415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-9B8F-B06D8815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-EF8F-B06DFC15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-4F88-B06D5C12937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-8B88-B06D9812937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-0389-B06D1013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-7389-B06D6013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-AB89-B06DB813937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-FB8A-B06DE810937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-6F8D-B06D7C17937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-0F8E-B06D1C14937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-1B8E-B06D0814937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-2B8F-B06D3815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{4B9139DE-2213-C579-BF8A-B06DAC10937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Global\{4B9139DE-2213-C579-EB89-B06DF813937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	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 3]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Atyriqipy
[process 3]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name
[process 3]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\
[process 3]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\
[process 3]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\
[process 5]	\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List
[process 5]	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\
[process 5]	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\

Set Values

	key
[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 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\CurrentVersion\Explorer\Shell Folders Value: Personal
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{3259504d-e161-11e0-bf1d-806d6172696f} Value: BaseClass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{3259504b-e161-11e0-bf1d-806d6172696f} Value: BaseClass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{3259504a-e161-11e0-bf1d-806d6172696f} Value: BaseClass
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common Documents
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Desktop
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common Desktop
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet

[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\ShellNoRoam\MUICache Value: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\wezeda.exe
[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\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 2]	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\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	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\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData

[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Personal
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{3259504d-e161-11e0-bf1d-806d6172696f} Value: BaseClass
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{3259504b-e161-11e0-bf1d-806d6172696f} Value: BaseClass
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{3259504a-e161-11e0-bf1d-806d6172696f} Value: BaseClass

[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common Documents
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Desktop
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common Desktop
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\ShellNoRoam\MUICache Value: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\wezedame.exe
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Internet Account Manager Value: Server ID
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name Value:
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkContactRefresh
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkFolderRefresh
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Identity Ordinal
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Atyriqipy Value: c231b06
[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\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Atyriqipy Value: fhechd4
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Atyriqipy Value: c231b06
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: uzta
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List Value: 6591:UDP
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List Value: 7306:TCP
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Atyriqipy Value: 209c281e
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Atyriqipy Value: hifbjhf
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Atyriqipy Value: 3h3917f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Atyriqipy Value: hifbjhf
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Atyriqipy Value: c231b06
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

Deleted Values	
	key
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Changing
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: IncomingID
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: OutgoingID

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process 2]	78.157.201.219	10.20.25.247	none
[process 2]	205.185.204.34	10.20.25.247	GET /msdownload/update/v3/static/trustedr/en/authrootseq.txt
			GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab
[process 5]	99.157.164.179	10.20.25.247	none
[process 5]	174.76.94.24	10.20.25.247	none
[process 5]	99.60.68.114	10.20.25.247	none
[process 5]	217.35.75.232	10.20.25.247	none
[process 5]	217.35.75.232	10.20.25.247	none
[process 5]	184.145.205.63	10.20.25.247	none

Network Traffic		
	Remote IP	**Local IP**
Connection #1	99.157.164.179	10.20.25.247
Connection #2	174.76.94.24	10.20.25.247
Connection #3	99.60.68.114	10.20.25.247
Connection #4	217.35.75.232	10.20.25.247

DNS Requests	
Request	**Result**
gidleybuilders.com	78.157.201.219
www.download.windowsupdate.com	205.185.204.34
	205.185.204.19
	205.185.204.88
	205.185.204.97
	205.185.204.99
	205.185.204.33
	205.185.204.75
	205.185.204.10
	205.185.204.56

Virus Total Results	
Last Scanned:	**2013-09-25 17:35:29**
Bkav:	Not Detected
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	PWSZbot-FFA!B9C4166CD597
Malwarebytes:	Trojan.Email.FA
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:	UDS:DangerousObject.Multi.Generic
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:	Not Detected
McAfee-GW-Edition:	Artemis!B9C4166CD597
Sophos:	Not Detected
Jiangmin:	Not Detected
Baidu-International:	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
Rising:	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