



Analysis # 30572

05/13/2013 16:23 pm

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
Set Values	10
Deleted Values	15
Network Activity	16
Network Events	16
Network Traffic	17
DNS Requests	18
Virus Total Results	19

Analysis Summary	
Submitted File:	SecureMail.exe
MD5:	20de8bad8bf8279e4084e9db461bd140
File Size:	137216
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-05-13 16:23:26
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Mon, 13 May 2013 20:26:28 +0000
Termination Time:	Mon, 13 May 2013 20:26:52 +0000
Analysis Time:	2013-05-13 16:23:26
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
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 2] C:\Documents and Settings\Administrator\Application Data\ljgaeh\iteky.exe
[process 3] C:\SecureMail.exe
[process 3] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\10913062.bat
[process 6] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\10911171.exe
[process 6] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp5b74e813.bat

Stored Modified Files
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\10911171.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\10913062.bat
[process 2] C:\Documents and Settings\Administrator\Application Data\lggaeh\iteky.exe
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp5b74e813.bat
[process 6] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 6] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 6] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 6] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 6] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab

Created Mutexes	
	mutex
[process 1]	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 1]	Name: Local\c:\documents and settings\administrator\cookies! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	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 1]	Name: Local\WininetConnectionMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Groove:PathMutex:YoNgf9TIAyd0477wzgfTiWi4XXU= 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: Global\{5B039399-8854-D5EB-89D3-085A9A492B48} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-4F8A-B06D5C10937F} 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\{D7EF8F1D-94D0-5907-238C-B06D3016937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-2F8F-B06D3C15937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-578F-B06D4415937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-B78F-B06DA415937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-9B8F-B06D8815937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-EF8F-B06DFC15937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-4F88-B06D5C12937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-8B88-B06D9812937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-0389-B06D1013937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-7389-B06D6013937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-E789-B06DF413937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 4]	Name: Global\{D7EF8F1D-94D0-5907-638B-B06D7011937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-CB8B-B06DD811937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-FB8D-B06DE817937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-678E-B06D7414937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-438E-B06D5014937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-7F8F-B06D6C15937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 4]	Name: Global\{D7EF8F1D-94D0-5907-C78A-B06DD410937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-BB8B-B06DA811937F} 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\{D7EF8F1D-94D0-5907-238C-B06D3016937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-2F8F-B06D3C15937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-578F-B06D4415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-B78F-B06DA415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-9B8F-B06D8815937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-EF8F-B06DFC15937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-4F88-B06D5C12937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-8B88-B06D9812937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-0389-B06D1013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-7389-B06D6013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-E789-B06DF413937F}

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-CB8B-B06DD811937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-FB8D-B06DE817937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-678E-B06D7414937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-438E-B06D5014937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{D7EF8F1D-94D0-5907-7F8F-B06D6C15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Global\{D7EF8F1D-94D0-5907-C78A-B06DD410937F}
	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 6]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: MPSWabDataAccessMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	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\WinRAR
[process 2]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx
[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\
[process 6]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name
[process 6]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\
[process 6]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\
[process 6]	\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\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\WinRAR Value: HWID
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[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\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\CurrentVersion\Explorer\Shell Folders Value: History
[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\WinRAR Value: Client Hash
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR Value: 4e6202bb29f24b73696761d7b6c9531f
[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\{3259504d-e161-11e0-bf1d-806d6172696f} Value: BaseClass

	entVersion\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\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\Shell\NoRoam\MUICache Value: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\10911171.exe
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Shell\NoRoam\MUICache Value: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\10913062.bat
[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: AppData
[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\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\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 368j57f0
[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\Curr entVersion\Explorer\Shell Folders Value: AppData
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: Local AppData
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 32h5i5he
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 368j57f0
[process 5]	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 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta ndardProfile Value: DisableNotifications
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta ndardProfile\GloballyOpenPorts\List Value: 21606:UDP
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta ndardProfile Value: DisableNotifications
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta ndardProfile Value: DisableNotifications
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta ndardProfile\GloballyOpenPorts\List Value: 12639:TCP
[process 5]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta ndardProfile Value: DisableNotifications
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: j405994
[process 5]	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 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx

	Value: 1jchigih
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 1jchigih
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 1jchigih
[process 5]	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 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 1jchigih
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 1jchigih
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 1jchigih
[process 5]	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 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	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 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	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 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	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 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 2i3acdc1

[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Internet Account Manager Value: Server ID
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name Value:
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkContactRefresh
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkFolderRefresh
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Identity Ordinal
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Diyx Value: 368j57f0

Deleted Values	
	key
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Changing
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: IncomingID
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: OutgoingID

Network Events			
	Remote IP	Local IP	HTTP Command
[process 1]	212.58.4.13	10.20.25.247	POST /ponyb/gate.php
[process 1]	62.233.104.156	10.20.25.247	GET /tHjeFFt.exe
[process 5]	72.242.102.130	10.20.25.247	none
[process 5]	78.139.151.101	10.20.25.247	none
[process 5]	72.242.102.130	10.20.25.247	none
[process 5]	84.59.222.81	10.20.25.247	none
[process 5]	180.241.97.79	10.20.25.247	none
[process 5]	190.111.231.3	10.20.25.247	none
[process 5]	81.149.242.235	10.20.25.247	none
[process 5]	76.245.44.216	10.20.25.247	none
[process 5]	211.209.241.213	10.20.25.247	none
[process 5]	76.245.44.216	10.20.25.247	none
[process 5]	142.136.161.103	10.20.25.247	none
[process 5]	180.248.91.99	10.20.25.247	none
[process 5]	94.43.47.107	10.20.25.247	none
[process 5]	78.139.187.6	10.20.25.247	none
[process 5]	94.43.47.107	10.20.25.247	none
[process 5]	190.42.161.35	10.20.25.247	none
[process 5]	92.241.153.135	10.20.25.247	none
[process 5]	79.129.141.111	10.20.25.247	none
[process 5]	98.201.143.22	10.20.25.247	none
[process 5]	83.11.107.212	10.20.25.247	none
[process 5]	71.80.71.70	10.20.25.247	none
[process 5]	62.178.183.239	10.20.25.247	none

Network Traffic		
	Remote IP	Local IP
Connection #1	10.20.25.255	10.20.25.247
Connection #2	72.242.102.130	10.20.25.247
Connection #3	78.139.151.101	10.20.25.247
Connection #4	72.242.102.130	10.20.25.247
Connection #5	78.139.151.101	10.20.25.247
Connection #6	84.59.222.81	10.20.25.247
Connection #7	180.241.97.79	10.20.25.247
Connection #8	84.59.222.81	10.20.25.247
Connection #9	190.111.231.3	10.20.25.247
Connection #10	81.149.242.235	10.20.25.247
Connection #11	76.245.44.216	10.20.25.247
Connection #12	211.209.241.213	10.20.25.247
Connection #13	76.245.44.216	10.20.25.247
Connection #14	211.209.241.213	10.20.25.247
Connection #15	142.136.161.103	10.20.25.247
Connection #16	180.248.91.99	10.20.25.247
Connection #17	142.136.161.103	10.20.25.247
Connection #18	180.248.91.99	10.20.25.247
Connection #19	94.43.47.107	10.20.25.247
Connection #20	180.248.91.99	10.20.25.247
Connection #21	94.43.47.107	10.20.25.247
Connection #22	78.139.187.6	10.20.25.247
Connection #23	94.43.47.107	10.20.25.247
Connection #24	78.139.187.6	10.20.25.247
Connection #25	190.42.161.35	10.20.25.247
Connection #26	92.241.153.135	10.20.25.247
Connection #27	190.42.161.35	10.20.25.247
Connection #28	92.241.153.135	10.20.25.247
Connection #29	79.129.141.111	10.20.25.247
Connection #30	92.241.153.135	10.20.25.247
Connection #31	98.201.143.22	10.20.25.247
Connection #32	83.11.107.212	10.20.25.247
Connection #33	71.80.71.70	10.20.25.247
Connection #34	83.11.107.212	10.20.25.247
Connection #35	71.80.71.70	10.20.25.247

DNS Requests	
Request	Result
mail.yaklasim.com	212.58.4.13

Virus Total Results	
Last Scanned:	2013-05-13 20:25:16
MicroWorld-eScan:	Gen:Variant.Kazy.173648
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	PWS-Zbot-FAUS!20DE8BAD8BF8
Malwarebytes:	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
eSafe:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Trojan-PSW.Win32.Tepfer.kabv
BitDefender:	Gen:Variant.Kazy.173648
NANO-Antivirus:	Not Detected
SUPERAntiSpyware:	Not Detected
Emsisoft:	Gen:Variant.Kazy.173660 (B)
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Trojan.PWS.Stealer.2877
VIPRE:	Not Detected
AntiVir:	TR/Crypt.XPACK.Gen5
TrendMicro:	Not Detected
McAfee-GW-Edition:	Not Detected
Sophos:	Mal/FakeAV-OY
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
ViRobot:	Not Detected
AhnLab-V3:	Trojan/Win32.FakeAV
GData:	Gen:Variant.Kazy.173648
CommTouch:	W32/Trojan.ZVIS-5521
ByteHero:	Not Detected
VBA32:	Not Detected
PCTools:	Not Detected
ESET-NOD32:	a variant of Win32/Kryptik.BAUT
Ikarus:	Win32.SuspectCrc
Fortinet:	W32/Kryptik.AGAJ!tr
AVG:	Agent
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.