



Analysis # 31615

07/09/2013 03:51 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	10
Created Keys	10
Set Values	11
Deleted Values	16
Network Activity	17
Network Events	17
Network Traffic	18
DNS Requests	19
Virus Total Results	20

Analysis Summary	
Submitted File:	SCAN_129_07082013_18911.exe
MD5:	59de4453da8909e96762f2c8cd0d6f37
File Size:	117760
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-07-09 03:51:15
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Tue, 09 Jul 2013 07:53:27 +0000
Termination Time:	Tue, 09 Jul 2013 07:53:53 +0000
Analysis Time:	2013-07-09 03:51:15
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	12
Sample Notes:	

Digital Behavior Traits			
Alters Windows Firewall		Hooks Keyboard	
Checks For Debugger		Injected Code	
Copies to Windows		Makes Network Connection	
Could Not Load		Modifies File in System	
Creates DLL in System		Modifies Local DNS	
Creates EXE in System		More than 5 Processes	
Creates Hidden File		Opens Physical Memory	
Creates Mutex		Starts EXE in Documents	
Creates Service		Starts EXE in Recycle	
Deletes File in System		Starts EXE in System	
Deletes Original Sample		Windows/Run Registry Key Set	

Deleted Files
[process 6] C:\SCAN_129_07082013_18911.exe
[process 6] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\142078.bat
[process 10] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\140375.exe
[process 10] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\SSNB12.bat
[process 11] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\135140.exe
[process 11] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\HMHEF26.bat
[process 12] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\138750.exe
[process 12] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\WRB341.bat

Stored Modified Files
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\135140.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\138750.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\140375.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\142078.bat
[process 2] C:\Documents and Settings\Administrator\Application Data\Mimaju\ytow.exe
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\HMHEF26.bat
[process 3] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\WRB341.bat
[process 4] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\SSNB12.bat
[process 9] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 9] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 9] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 9] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 9] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab

Created Mutexes	
	mutex
[process 1]	Name: RasPbFile Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[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:YoNgf9TIAyd0477wzgfITWi4XXU= 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: RasPbFile 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 3]	Name: Global\{3F192A85-3148-B1F1-0382-B06D1018937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: RasPbFile 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 4]	Name: Global\{3F192A85-3148-B1F1-0B82-B06D1818937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: RasPbFile Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{5B039399-8854-D5EB-89D3-085A9A492B48} 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 5]	Name: Global\{3F192A85-3148-B1F1-3B82-B06D2818937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: RasPbFile Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\{E41AB6D2-AD1F-6AF2-89D3-085A9A492B48} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 5]	Name: Global\{3F192A85-3148-B1F1-238C-B06D3016937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-EF8E-B06DFC14937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-578F-B06D4415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-B78F-B06DA415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-9B8F-B06D8815937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-EF8F-B06DFC15937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-4F88-B06D5C12937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-8B88-B06D9812937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-0389-B06D1013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-7389-B06D6013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-B389-B06DA013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-778B-B06D6411937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-538B-B06D4011937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-DB8C-B06DC816937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-738E-B06D6014937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-AF8E-B06DBC14937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-8B8E-B06D9814937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-CB8E-B06DD814937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-278F-B06D3415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-CB88-B06DD812937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-E389-B06DF013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-C78A-B06DD410937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-D38C-B06DC016937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-1781-B06D041B937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 5]	Name: Global\{3F192A85-3148-B1F1-6F81-B06D7C1B937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 7]	Name: Global\{3F192A85-3148-B1F1-4781-B06D541B937F}

[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{7EB084F0-9F3D-F058-89D3-085A9A492B48}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{A8B6B2C3-A90E-265E-89D3-085A9A492B48}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{A45A65F1-7E3C-2AB2-89D3-085A9A492B48}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{A45A65F6-7E3B-2AB2-89D3-085A9A492B48}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Local\{C5BCD3E2-C82F-4B54-89D3-085A9A492B48}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Local\{C5BCD3E3-C82E-4B54-89D3-085A9A492B48}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-238C-B06D3016937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-EF8E-B06DFC14937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-578F-B06D4415937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-B78F-B06DA415937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-9B8F-B06D8815937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-EF8F-B06DFC15937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-4F88-B06D5C12937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-8B88-B06D9812937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-0389-B06D1013937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-7389-B06D6013937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-B389-B06DA013937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-538B-B06D4011937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-DB8C-B06DC816937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-738E-B06D6014937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-AF8E-B06DBC14937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-8B8E-B06D9814937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-CB8E-B06DD814937F}
[process 7]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{3F192A85-3148-B1F1-278F-B06D3415937F}

[process 7]	Name: Global\{3F192A85-3148-B1F1-CB88-B06DD812937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: Global\{3F192A85-3148-B1F1-E389-B06DF013937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: Global\{3F192A85-3148-B1F1-C78A-B06DD410937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Global\{3F192A85-3148-B1F1-D38C-B06DC016937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: MPSWabDataAccessMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	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 10]	Name: SHIMLIB_LOG_Mutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 11]	Name: SHIMLIB_LOG_Mutex 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: SHIMLIB_LOG_Mutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 1]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR
[process 2]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu
[process 7]	\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List
[process 7]	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\
[process 7]	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\
[process 9]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name
[process 9]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\
[process 9]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\
[process 9]	\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: 21dcbdd5fc7145386960600cb169ef72
[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}

	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\135140.exe
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR Value: acf6ea4d174ba71e1a2a4170c6841f64
[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\138750.exe
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR Value: 21dcbdd5fc7145386960600cb169ef72
[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\140375.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\142078.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 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 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 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 7i44i71
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 360fihf
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: ytow

[process 7]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 7]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts>List Value: 7879:UDP
[process 7]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 7]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 7]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts>List Value: 3141:TCP
[process 7]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 28946447
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a

	Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 16j4f546
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: bajje9a
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 360fihf
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Internet Account Manager Value: Server ID
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name Value:
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkContactRefresh
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkFolderRefresh
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Identity Ordinal
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Avlowofiamu Value: 360fihf
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 11]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

Deleted Values	
	key
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Changing
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: IncomingID
[process 9]	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]	64.94.100.116	10.20.25.247	POST /ponyb/gate.php
[process 1]	89.248.106.177	10.20.25.247	GET /bts1.exe
[process 1]	212.58.2.22	10.20.25.247	GET /FzPfH6.exe
[process 1]	198.173.93.218	10.20.25.247	GET /oEoASW64.exe
[process 1]	50.62.228.1	10.20.25.247	GET /qbSTq.exe
[process 7]	14.97.190.216	10.20.25.247	none
[process 7]	87.18.47.40	10.20.25.247	none
[process 7]	87.18.47.40	10.20.25.247	none
[process 7]	77.30.83.91	10.20.25.247	none
[process 7]	190.202.83.105	10.20.25.247	none
[process 7]	78.131.54.252	10.20.25.247	none
[process 7]	122.60.12.36	10.20.25.247	none
[process 7]	200.91.49.183	10.20.25.247	none
[process 7]	107.217.117.139	10.20.25.247	none
[process 7]	190.117.157.233	10.20.25.247	none
[process 7]	84.59.131.0	10.20.25.247	none
[process 7]	76.226.114.217	10.20.25.247	none
[process 7]	66.63.204.26	10.20.25.247	none
[process 7]	221.215.31.50	10.20.25.247	none
[process 7]	85.107.90.53	10.20.25.247	none
[process 7]	64.136.115.72	10.20.25.247	none
[process 7]	108.234.133.110	10.20.25.247	none
[process 7]	95.246.170.150	10.20.25.247	none
[process 7]	98.166.156.69	10.20.25.247	none
[process 7]	213.219.135.113	10.20.25.247	none

Network Traffic		
	Remote IP	Local IP
Connection #1	10.20.25.255	10.20.25.247
Connection #2	14.97.190.216	10.20.25.247
Connection #3	87.18.47.40	10.20.25.247
Connection #4	77.30.83.91	10.20.25.247
Connection #5	87.18.47.40	10.20.25.247
Connection #6	77.30.83.91	10.20.25.247
Connection #7	190.202.83.105	10.20.25.247
Connection #8	78.131.54.252	10.20.25.247
Connection #9	122.60.12.36	10.20.25.247
Connection #10	200.91.49.183	10.20.25.247
Connection #11	107.217.117.139	10.20.25.247
Connection #12	200.91.49.183	10.20.25.247
Connection #13	107.217.117.139	10.20.25.247
Connection #14	190.117.157.233	10.20.25.247
Connection #15	10.20.25.255	10.20.25.247
Connection #16	10.20.25.236	10.20.25.247
Connection #17	84.59.131.0	10.20.25.247
Connection #18	76.226.114.217	10.20.25.247
Connection #19	66.63.204.26	10.20.25.247
Connection #20	221.215.31.50	10.20.25.247
Connection #21	85.107.90.53	10.20.25.247
Connection #22	10.20.25.255	10.20.25.247
Connection #23	10.20.25.236	10.20.25.247
Connection #24	85.107.90.53	10.20.25.247
Connection #25	64.136.115.72	10.20.25.247
Connection #26	108.234.133.110	10.20.25.247
Connection #27	95.246.170.150	10.20.25.247
Connection #28	98.166.156.69	10.20.25.247

DNS Requests	
Request	Result
2ndtimearoundweddingphotography.com	64.94.100.116
lacasadelmovilusado.com	89.248.106.177
common.karsak.com.tr	212.58.2.22
ftp.vickibettger.com	198.173.93.218
qualitydoorblog.com	50.62.228.1

Virus Total Results	
Last Scanned:	2013-07-09 07:45:28
MicroWorld-eScan:	Trojan.GenericKD.1097543
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	RDN/Generic.grp!fk
Malwarebytes:	Malware.Packer.rf
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
NANO-Antivirus:	Not Detected
F-Prot:	W32/Trojan3.FMT
Symantec:	Not Detected
Norman:	Troj_Generic.MQDUZ
TotalDefense:	Not Detected
TrendMicro-HouseCall:	TROJ_GEN.F0D1H0ZG813
Avast:	Win32:Dropper-gen [Drp]
eSafe:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Trojan-PSW.Win32.Tepfer.nppd
BitDefender:	Trojan.GenericKD.1097543
Agnitum:	Not Detected
ViRobot:	Not Detected
ByteHero:	Not Detected
Sophos:	Mal/EncPk-AKE
Comodo:	UnclassifiedMalware
F-Secure:	Trojan.GenericKD.1097543
DrWeb:	Trojan.PWS.Stealer.3128
VIPRE:	Win32.Malware!Drop
AntiVir:	TR/Agent.117760.48
TrendMicro:	Not Detected
McAfee-GW-Edition:	Artemis!59DE4453DA89
Emsisoft:	Trojan.GenericKD.1097543 (B)
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Win32.HeurC.KVMH004.a.(kcloud)
Microsoft:	PWS:Win32/Fareit.gen!C
SUPERAntiSpyware:	Trojan.Agent/Gen-Fareit
GData:	Trojan.GenericKD.1097543
CommTouch:	W32/Trojan.QKKN-5761
AhnLab-V3:	Trojan/Win32.Inject
VBA32:	Not Detected
PCTools:	Not Detected
ESET-NOD32:	Win32/Kryptik.BFHP
Rising:	Not Detected
Ikarus:	Win32.SuspectCrc
Fortinet:	W32/EncPK.AKE!tr
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.