Analysis # 31012

06/03/2013 16:00 pm

Table of Contents

Analysis Summary

Submitted File:	SecureMessage_06032013.exe
MD5:	2994f3319096ad15b31f3f3135add304
File Size:	112640
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-06-03 16:00:12
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Mon, 03 Jun 2013 20:03:51 +0000
Termination Time:	Mon, 03 Jun 2013 20:04:24 +0000
Analysis Time:	2013-06-03 16:00:12
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	13
Sample Notes:	

Digital Behavior Traits

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

Deleted Files
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\mmc11B925B5.xml
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\mmc02FF7B64.xml
[process 3] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\mmc159BAFEC.xml
[process 4] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\mmc2B7CEC20.xml
[process 7] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2035359.exe
[process 7] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\KLJF970.bat
[process 8] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\mmc03FF8EAA.xml
[process 9] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\mmc1692FD71.xml
[process 10] C:\SecureMessage_06032013.exe
[process 10] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2051515.bat
[process 11] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2045734.exe
[process 11] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\IIMCBFF.bat
[process 12] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2047156.exe
[process 12] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\WLSA55E.bat
[process 13] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2049953.exe
[process 13] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\MZKA747.bat

Stored Modified Files
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2035359.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2045734.exe
[process 1] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 1] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 1] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 1] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 1] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2047156.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2049953.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2051515.bat
[process 2] C:\Documents and Settings\Administrator\Application Data\Urrij\reexy.exe
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\KLJF970.bat
[process 4] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\IIMCBFF.bat
[process 8] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\WLSA55E.bat
[process 9] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\MZKA747.bat

Created Mutexes	
	mutex
[process 1]	Name: oleacc-msaa-loaded
	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: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 1]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: MPSWabDataAccessMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: MPSWABOlkStoreNotifyMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: MSIdent Logon
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Global\{BA2F5D4C-4681-34C7-F78B-B06DE411937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Global\{BA2F5D4C-4681-34C7-AB8E-B06DB814937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{BA2F5D4C-4681-34C7-BF8A-B06DAC10937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: oleacc-msaa-loaded
	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\{BA2F5D4C-4681-34C7-A78C-B06DB416937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: oleacc-msaa-loaded
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Local\{E41AB6D2-AD1F-6AF2-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-238C-B06D3016937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 3]	Name: Global\{BA2F5D4C-4681-34C7-F38E-B06DE014937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-578F-B06D4415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-B78F-B06DA415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-9B8F-B06D8815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-EF8F-B06DFC15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-4F88-B06D5C12937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-8B88-B06D9812937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-0389-B06D1013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-7389-B06D6013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-AB89-B06DB813937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-678B-B06D7411937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-478B-B06D5411937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-838D-B06D9017937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-CF8D-B06DDC17937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-6B8E-B06D7814937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-478E-B06D5414937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-4F8F-B06D5C15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-CB8F-B06DD815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-7B8F-B06D6815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-778F-B06D6415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-178D-B06D0417937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{BA2F5D4C-4681-34C7-BB8C-B06DA816937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{BA2F5D4C-4681-34C7-3F8B-B06D2C11937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: oleacc-msaa-loaded
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{5B039399-8854-D5EB-89D3-085A9A492B48}

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-BB8E-B06DA814937F}
	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\{BA2F5D4C-4681-34C7-238C-B06D3016937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-F38E-B06DE014937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-578F-B06D4415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-B78F-B06DA415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-9B8F-B06D8815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-EF8F-B06DFC15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-4F88-B06D5C12937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-8B88-B06D9812937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-0389-B06D1013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-7389-B06D6013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-AB89-B06DB813937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-478B-B06D5411937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-838D-B06D9017937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-CF8D-B06DDC17937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-6B8E-B06D7814937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-478E-B06D5414937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-4F8F-B06D5C15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 5]	Name: Global\{BA2F5D4C-4681-34C7-CB8F-B06DD815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-7B8F-B06D6815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-778F-B06D6415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\{BA2F5D4C-4681-34C7-F78B-B06DE411937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Global\{BA2F5D4C-4681-34C7-AB8E-B06DB814937F}
	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
[process 8]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: oleacc-msaa-loaded
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Global\{5B039399-8854-D5EB-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: Global\{BA2F5D4C-4681-34C7-338F-B06D2015937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: oleacc-msaa-loaded
	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\{5B039399-8854-D5EB-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Global\{BA2F5D4C-4681-34C7-DF8A-B06DCC10937F}
	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
[process 13]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 13]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 1]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR
[process 1]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name
[process 1]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB
[process 1]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4
[process 1]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name
[process 2]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa
[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\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: 4e9d3250899795810d85dc5973c3579b
[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\Curr

	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\Curr
	entVersion\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\Curr
	entVersion\Internet Settings\ZoneMap
	Value: ProxyBypass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Internet Settings\ZoneMap
	Value: IntranetName
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Internet Settings\ZoneMap
	Value: UNCAsIntranet
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Internet Settings\ZoneMap
	Value: AutoDetect
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Internet Settings\ZoneMap
	Value: ProxyBypass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Internet Settings\ZoneMap
	Value: IntranetName
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Internet Settings\ZoneMap
	Value: UNCAsIntranet
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Internet Settings\ZoneMap
	Value: AutoDetect
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Shel
	lNoRoam\MUICache
	Value: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2035359.exe
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR
	Value: 4e9d3250899795810d85dc5973c3579b
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Shel
	lNoRoam\MUICache
	Value: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2045734.exe
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Internet Acc
	ount Manager
	Value: Server ID
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab
	File Name
	Value:
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4
	Value: OlkContactRefresh
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4
	Value: OlkFolderRefresh

[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Identity Ordinal
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2338jife
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR Value: 4e9d3250899795810d85dc5973c3579b
[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\2047156.exe
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR Value: 4e9d3250899795810d85dc5973c3579b
[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\2049953.exe
[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\2051515.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 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 27e630f8
[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\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2338jife
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: reexy
[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: 23611: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: 19992: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\Qeohzeneeqa Value: 48hjabi
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2e4jdi4f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2e4jdi4f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2e4jdi4f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2e4jdi4f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2e4jdi4f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2e4jdi4f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2e4jdi4f

[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2e4jdi4f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2e4jdi4f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 1ech792f
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Qeohzeneeqa Value: 2338jife
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 9]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG

	Value: Seed
[process 11]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
	Value: Seed
[process 12]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
	Value: Seed
[process 13]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
	Value: Seed

Deleted Values	
	key
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities
	Value: Changing
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities
	Value: IncomingID
[process 1]	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]	116.122.158.195	10.20.25.247	POST /ponyb/gate.php
[process 1]	194.184.71.7	10.20.25.247	GET /2L6L.exe
[process 1]	190.147.81.28	10.20.25.247	GET /yqRSQ.exe
[process 1]	74.54.147.146	10.20.25.247	GET /ngY.exe
[process 1]	207.204.5.170	10.20.25.247	GET /PXVYGJx.exe
[process 5]	112.207.193.168	10.20.25.247	none
[process 5]	79.45.133.216	10.20.25.247	none
[process 5]	79.45.133.216	10.20.25.247	none
[process 5]	94.66.31.106	10.20.25.247	none
[process 5]	142.136.161.103	10.20.25.247	none
[process 5]	181.67.50.91	10.20.25.247	none
[process 5]	77.78.226.228	10.20.25.247	none
[process 5]	76.226.112.216	10.20.25.247	none
[process 5]	67.36.72.62	10.20.25.247	none
[process 5]	94.43.47.107	10.20.25.247	none
[process 5]	108.234.133.110	10.20.25.247	none
[process 5]	188.121.218.120	10.20.25.247	none
[process 5]	188.169.204.227	10.20.25.247	none
[process 5]	84.59.222.81	10.20.25.247	none
[process 5]	189.235.146.89	10.20.25.247	none
[process 5]	178.205.128.203	10.20.25.247	none
[process 5]	78.139.151.101	10.20.25.247	none
[process 5]	108.215.99.94	10.20.25.247	none
[process 5]	108.215.44.142	10.20.25.247	none
[process 5]	108.215.44.142	10.20.25.247	none
[process 5]	75.150.217.189	10.20.25.247	none

Network Traffic		
	Remote IP	**Local IP**
Connection #1	10.20.25.255	10.20.25.247
Connection #2	112.207.193.168	10.20.25.247
Connection #3	79.45.133.216	10.20.25.247
Connection #4	94.66.31.106	10.20.25.247
Connection #5	142.136.161.103	10.20.25.247
Connection #6	181.67.50.91	10.20.25.247
Connection #7	77.78.226.228	10.20.25.247
Connection #8	181.67.50.91	10.20.25.247
Connection #9	77.78.226.228	10.20.25.247
Connection #10	76.226.112.216	10.20.25.247
Connection #11	67.36.72.62	10.20.25.247
Connection #12	94.43.47.107	10.20.25.247
Connection #13	108.234.133.110	10.20.25.247
Connection #14	188.121.218.120	10.20.25.247
Connection #15	188.169.204.227	10.20.25.247
Connection #16	84.59.222.81	10.20.25.247
Connection #17	189.235.146.89	10.20.25.247
Connection #18	178.205.128.203	10.20.25.247
Connection #19	78.139.151.101	10.20.25.247
Connection #20	108.215.99.94	10.20.25.247
Connection #21	108.215.44.142	10.20.25.247

DNS Requests	
Request	**Result**
www.netnet-viaggi.it	194.184.71.7
paulcblake.com	74.54.147.146

Virus Total Results	
Last Scanned:	**2013-06-03 20:00:57**
MicroWorld-eScan:	Gen:Heur.VIZ.7
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Ransom-FCFH!2994F3319096
Malwarebytes:	Trojan.Agent.zrf
TheHacker:	Not Detected
K7GW:	Not Detected
K7AntiVirus:	Not Detected
Agnitum:	Not Detected
F-Prot:	W32/Trojan3.FJC
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.lnga
BitDefender:	Gen:Heur.VIZ.7
NANO-Antivirus:	Not Detected
SUPERAntiSpyware:	Not Detected
Emsisoft:	Gen:Heur.VIZ.7 (B)
Comodo:	Heur.Packed.Unknown
F-Secure:	Gen:Heur.VIZ.7
DrWeb:	Trojan.Packed.196
VIPRE:	Not Detected
AntiVir:	Not Detected
TrendMicro:	Not Detected
McAfee-GW-Edition:	Heuristic.LooksLike.Win32.Suspicious.B
Sophos:	Not Detected
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
ViRobot:	Not Detected
AhnLab-V3:	Trojan/Win32.Tepfer
GData:	Gen:Heur.VIZ.7
Commtouch:	W32/Trojan.FCBK-1398
ByteHero:	Not Detected
VBA32:	Not Detected
PCTools:	Not Detected
ESET-NOD32:	Win32/PSW.Fareit.A
Rising:	Not Detected
Ikarus:	Not Detected
Fortinet:	W32/Kryptik.AGAJ!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