



Analysis # 30642

05/16/2013 11:25 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 | 9 |
| Created Keys | 9 |
| Set Values | 10 |
| Deleted Values | 16 |
| Network Activity | 17 |
| Network Events | 17 |
| Network Traffic | 18 |
| DNS Requests | 19 |
| Virus Total Results | 20 |

| Analysis Summary | |
|---------------------|---|
| Submitted File: | SecureMessage.exe |
| MD5: | d5893c62d897d95a30c950cddcbdc604 |
| File Size: | 126464 |
| File Type: | PE32 executable for MS Windows (GUI) Intel 80386 3 |
| Analysis Time: | 2013-05-16 11:25:57 |
| Start Reason: | AnalysisTarget |
| Termination Reason: | TerminatedBySelf |
| Start Time: | Thu, 16 May 2013 15:29:03 +0000 |
| Termination Time: | Thu, 16 May 2013 15:29:27 +0000 |
| Analysis Time: | 2013-05-16 11:25:57 |
| 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\Qaseto\lyxyjl.exe |
| [process 3] C:\SecureMessage.exe |
| [process 3] C:\SECURE~1\ADMINI~1\LOCALS~1\Temp\12883031.EXE |
| [process 3] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\12883031.bat |
| [process 6] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\12881109.exe |
| [process 6] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmpe55eb44f.bat |

Stored Modified Files

[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\12881109.exe

[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\12883031.bat

[process 2] C:\Documents and Settings\Administrator\Application Data\Qaseto\lyxyjl.exe

[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmpe55eb44f.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\{4B69C74D-DC80-C581-3389-B06D2013937F} 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\{4B69C74D-DC80-C581-238C-B06D3016937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-F38E-B06DE014937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-578F-B06D4415937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-B78F-B06DA415937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-9B8F-B06D8815937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-EF8F-B06DFC15937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-4F88-B06D5C12937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-8B88-B06D9812937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-0389-B06D1013937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-7389-B06D6013937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-5B89-B06D4813937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |

| | |
|-------------|---|
| [process 4] | Name: Global\{4B69C74D-DC80-C581-FF8A-B06DEC10937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-E78B-B06DF411937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-E78D-B06DF417937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-0F8E-B06D1C14937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-678E-B06D7414937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-838E-B06D9014937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 4] | Name: Global\{4B69C74D-DC80-C581-738E-B06D6014937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-678A-B06D7410937F} 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\{4B69C74D-DC80-C581-238C-B06D3016937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-F38E-B06DE014937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-578F-B06D4415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-B78F-B06DA415937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-9B8F-B06D8815937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-EF8F-B06DFC15937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-4F88-B06D5C12937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-8B88-B06D9812937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-0389-B06D1013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-7389-B06D6013937F} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-5B89-B06D4813937F} |

| | |
|-------------|--|
| | Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-FF8A-B06DEC10937F} |
| | Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-E78D-B06DF417937F} |
| | Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-0F8E-B06D1C14937F} |
| | Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-678E-B06D7414937F} |
| | Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 5] | Name: Global\{4B69C74D-DC80-C581-838E-B06D9014937F} |
| | Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE |
| [process 6] | Name: Global\{4B69C74D-DC80-C581-738E-B06D6014937F} |
| | 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\Poibib |
| [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: e0b6f3a0090a03277820cc686467a031 |
| [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\12881109.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\12883031.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\Poibib Value: gf0921f |
| [process 4] | Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed |
| [process 4] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData |
| [process 4] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData |
| [process 4] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: bhcd0f1 |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: gf0921f |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48} |
| [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: 20942: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: 14864: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\Poibib Value: 1gc1idd3 |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48} |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48} |

| | |
|-------------|---|
| | entVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48} |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [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\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [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\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [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\Poibib Value: 84h007i |

| | |
|-------------|---|
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 1291dc1i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Poibib Value: 84h007i |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48} |
| [process 5] | Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48} |
| [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\Poibib Value: gf0921f |

| 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 /forum/viewtopic.php |
| [process 1] | 69.89.21.99 | 10.20.25.247 | GET /Gsdw1.exe |
| [process 5] | 14.98.41.204 | 10.20.25.247 | none |
| [process 5] | 69.77.132.197 | 10.20.25.247 | none |
| [process 5] | 180.241.97.79 | 10.20.25.247 | none |
| [process 5] | 69.77.132.197 | 10.20.25.247 | none |
| [process 5] | 98.201.143.22 | 10.20.25.247 | none |
| [process 5] | 78.166.89.166 | 10.20.25.247 | none |
| [process 5] | 94.65.39.115 | 10.20.25.247 | none |
| [process 5] | 211.209.241.213 | 10.20.25.247 | none |
| [process 5] | 190.42.161.35 | 10.20.25.247 | none |
| [process 5] | 84.59.222.81 | 10.20.25.247 | none |
| [process 5] | 78.139.151.101 | 10.20.25.247 | none |
| [process 5] | 122.174.9.23 | 10.20.25.247 | none |
| [process 5] | 83.213.35.105 | 10.20.25.247 | none |
| [process 5] | 180.248.91.99 | 10.20.25.247 | none |
| [process 5] | 83.213.35.105 | 10.20.25.247 | none |
| [process 5] | 62.194.30.232 | 10.20.25.247 | none |
| [process 5] | 125.26.133.226 | 10.20.25.247 | none |
| [process 5] | 199.59.157.124 | 10.20.25.247 | none |
| [process 5] | 217.247.58.227 | 10.20.25.247 | none |
| [process 5] | 78.139.187.6 | 10.20.25.247 | none |
| [process 5] | 14.97.232.238 | 10.20.25.247 | none |

| Network Traffic | | |
|-----------------|-----------------|--------------|
| | Remote IP | Local IP |
| Connection #1 | 10.20.25.255 | 10.20.25.247 |
| Connection #2 | 14.98.41.204 | 10.20.25.247 |
| Connection #3 | 69.77.132.197 | 10.20.25.247 |
| Connection #4 | 180.241.97.79 | 10.20.25.247 |
| Connection #5 | 69.77.132.197 | 10.20.25.247 |
| Connection #6 | 180.241.97.79 | 10.20.25.247 |
| Connection #7 | 98.201.143.22 | 10.20.25.247 |
| Connection #8 | 180.241.97.79 | 10.20.25.247 |
| Connection #9 | 98.201.143.22 | 10.20.25.247 |
| Connection #10 | 180.241.97.79 | 10.20.25.247 |
| Connection #11 | 98.201.143.22 | 10.20.25.247 |
| Connection #12 | 78.166.89.166 | 10.20.25.247 |
| Connection #13 | 94.65.39.115 | 10.20.25.247 |
| Connection #14 | 211.209.241.213 | 10.20.25.247 |
| Connection #15 | 94.65.39.115 | 10.20.25.247 |
| Connection #16 | 211.209.241.213 | 10.20.25.247 |
| Connection #17 | 190.42.161.35 | 10.20.25.247 |
| Connection #18 | 84.59.222.81 | 10.20.25.247 |
| Connection #19 | 190.42.161.35 | 10.20.25.247 |
| Connection #20 | 84.59.222.81 | 10.20.25.247 |
| Connection #21 | 78.139.151.101 | 10.20.25.247 |
| Connection #22 | 84.59.222.81 | 10.20.25.247 |
| Connection #23 | 122.174.9.23 | 10.20.25.247 |
| Connection #24 | 83.213.35.105 | 10.20.25.247 |
| Connection #25 | 180.248.91.99 | 10.20.25.247 |
| Connection #26 | 83.213.35.105 | 10.20.25.247 |
| Connection #27 | 180.248.91.99 | 10.20.25.247 |
| Connection #28 | 62.194.30.232 | 10.20.25.247 |
| Connection #29 | 180.248.91.99 | 10.20.25.247 |
| Connection #30 | 62.194.30.232 | 10.20.25.247 |
| Connection #31 | 125.26.133.226 | 10.20.25.247 |
| Connection #32 | 62.194.30.232 | 10.20.25.247 |
| Connection #33 | 125.26.133.226 | 10.20.25.247 |
| Connection #34 | 199.59.157.124 | 10.20.25.247 |
| Connection #35 | 125.26.133.226 | 10.20.25.247 |
| Connection #36 | 199.59.157.124 | 10.20.25.247 |
| Connection #37 | 217.247.58.227 | 10.20.25.247 |
| Connection #38 | 78.139.187.6 | 10.20.25.247 |

| DNS Requests | |
|-------------------|-------------|
| Request | Result |
| mail.yaklasim.com | 212.58.4.13 |
| ryulawgroup.com | 69.89.21.99 |

Virus Total Results

No Results

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.