Analysis # 30378

05/02/2013 06:14 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 14
Network Activity 15
Network Events 15
Network Traffic 16
DNS Requests 17
Virus Total Results 18

Analysis Summary

Submitted File:	Receipt_on_payment_ID758_34.exe
MD5:	652d9919b209562bc8bb79b34e3af47d
File Size:	358912
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-05-02 06:14:48
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Thu, 02 May 2013 10:17:29 +0000
Termination Time:	Thu, 02 May 2013 10:17:35 +0000
Analysis Time:	2013-05-02 06:14:48
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	4
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:\Documents and Settings\Administrator\Application Data\Ibnyd\ykbi.exe
[process 4] C:\Receipt_on_payment_ID758_34.exe
[process 4] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmpa885fd60.bat

Stored Modified Files
[process 1] C:\Documents and Settings\Administrator\Application Data\Ibnyd\ykbi.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmpa885fd60.bat
[process 4] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 4] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 4] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 4] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
[process 4] C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab

Created Mutexes	
	mutex
[process 1]	Name: Global\{5B039399-8854-D5EB-89D3-085A9A492B48}
	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 2]	Name: Global\{F71B8D33-96FE-79F3-638D-B06D7017937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\{E41AB6D2-AD1F-6AF2-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-238C-B06D3016937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-EF8E-B06DFC14937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-578F-B06D4415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-B78F-B06DA415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-9B8F-B06D8815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-EF8F-B06DFC15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-4F88-B06D5C12937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-8B88-B06D9812937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-0389-B06D1013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-7389-B06D6013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-9789-B06D8413937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-EF8A-B06DFC10937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-AB8B-B06DB811937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-FB8D-B06DE817937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-678E-B06D7414937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-7F8E-B06D6C14937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-8B8E-B06D9814937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{F71B8D33-96FE-79F3-AB8A-B06DB810937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-3F8F-B06D2C15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{7EB084F0-9F3D-F058-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{A8B6B2C3-A90E-265E-89D3-085A9A492B48}

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{A45A65F1-7E3C-2AB2-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{A45A65F6-7E3B-2AB2-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Local\{C5BCD3E2-C82F-4B54-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Local\{C5BCD3E3-C82E-4B54-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-238C-B06D3016937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-EF8E-B06DFC14937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-578F-B06D4415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-B78F-B06DA415937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-9B8F-B06D8815937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-EF8F-B06DFC15937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-4F88-B06D5C12937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-8B88-B06D9812937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-0389-B06D1013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-7389-B06D6013937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-9789-B06D8413937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-EF8A-B06DFC10937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-FB8D-B06DE817937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-678E-B06D7414937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-7F8E-B06D6C14937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{F71B8D33-96FE-79F3-8B8E-B06D9814937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{F71B8D33-96FE-79F3-AB8A-B06DB810937F}
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: SHIMLIB_LOG_MUTEX
	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: MPSWabDataAccessMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 4]	Name: MPSWABOlkStoreNotifyMutex
	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\Microsoft\Moodyf
[process 3]	\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List
[process 3]	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\
[process 3]	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\
[process 4]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name
[process 4]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\
[process 4]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\
[process 4]	\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\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: 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\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: c6h60aj
[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\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: g31jhhh
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: c6h60aj
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List Value: 21464:UDP
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Sta

	ndardProfile Value: DisableNotifications
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List Value: 22260:TCP
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile Value: DisableNotifications
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 20e66hcf
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e

[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 9a7faif
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 1h669da4
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: e7ga461
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: i39g70e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e

[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: 4163d2e
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: {23A8AFC1-B40C-AD40-89D3-085A9A492B48}
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[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\Internet Account Manager Value: Server ID
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4\Wab File Name Value:
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkContactRefresh
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\WAB\WAB4 Value: OlkFolderRefresh
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities Value: Identity Ordinal
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Moodyf Value: c6h60aj

Deleted Values	
	key
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities
	Value: Changing
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities
	Value: IncomingID
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Identities
	Value: OutgoingID

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process 3]	174.89.43.79	10.20.25.247	none
[process 3]	98.226.120.96	10.20.25.247	none
[process 3]	174.89.43.79	10.20.25.247	none
[process 3]	189.223.135.118	10.20.25.247	none
[process 3]	81.133.189.232	10.20.25.247	none
[process 3]	195.169.125.228	10.20.25.247	none
[process 3]	186.134.152.195	10.20.25.247	none
[process 3]	194.94.127.98	10.20.25.247	none
[process 3]	2.185.69.145	10.20.25.247	none
[process 3]	95.246.163.58	10.20.25.247	none
[process 3]	83.8.171.214	10.20.25.247	none
[process 3]	64.231.249.250	10.20.25.247	none
[process 3]	72.20.156.250	10.20.25.247	none
[process 3]	199.59.157.124	10.20.25.247	none
[process 3]	75.61.139.23	10.20.25.247	none
[process 3]	199.59.157.124	10.20.25.247	none
[process 3]	81.149.242.235	10.20.25.247	none
[process 3]	201.211.95.80	10.20.25.247	none
[process 3]	41.97.224.181	10.20.25.247	none
[process 3]	2.51.17.211	10.20.25.247	none
[process 3]	122.161.2.112	10.20.25.247	none
[process 3]	14.99.12.0	10.20.25.247	none
[process 3]	122.161.2.112	10.20.25.247	none
[process 3]	2.100.209.12	10.20.25.247	none
[process 3]	96.47.81.4	10.20.25.247	none
[process 3]	58.8.105.185	10.20.25.247	none
[process 3]	108.250.41.166	10.20.25.247	none
[process 3]	82.152.152.20	10.20.25.247	none
[process 3]	176.73.141.26	10.20.25.247	none
[process 3]	176.67.74.200	10.20.25.247	none
[process 3]	106.217.225.134	10.20.25.247	none

Network Traffic		
	Remote IP	**Local IP**
Connection #1	10.20.25.255	10.20.25.247
Connection #2	174.89.43.79	10.20.25.247
Connection #3	98.226.120.96	10.20.25.247
Connection #4	174.89.43.79	10.20.25.247
Connection #5	98.226.120.96	10.20.25.247
Connection #6	189.223.135.118	10.20.25.247
Connection #7	81.133.189.232	10.20.25.247
Connection #8	189.223.135.118	10.20.25.247
Connection #9	81.133.189.232	10.20.25.247
Connection #10	195.169.125.228	10.20.25.247
Connection #11	81.133.189.232	10.20.25.247
Connection #12	195.169.125.228	10.20.25.247
Connection #13	186.134.152.195	10.20.25.247
Connection #14	194.94.127.98	10.20.25.247
Connection #15	2.185.69.145	10.20.25.247
Connection #16	95.246.163.58	10.20.25.247
Connection #17	2.185.69.145	10.20.25.247
Connection #18	95.246.163.58	10.20.25.247
Connection #19	83.8.171.214	10.20.25.247
Connection #20	95.246.163.58	10.20.25.247
Connection #21	64.231.249.250	10.20.25.247
Connection #22	72.20.156.250	10.20.25.247
Connection #23	64.231.249.250	10.20.25.247
Connection #24	199.59.157.124	10.20.25.247
Connection #25	75.61.139.23	10.20.25.247
Connection #26	81.149.242.235	10.20.25.247
Connection #27	75.61.139.23	10.20.25.247
Connection #28	81.149.242.235	10.20.25.247
Connection #29	201.211.95.80	10.20.25.247
Connection #30	81.149.242.235	10.20.25.247
Connection #31	201.211.95.80	10.20.25.247
Connection #32	41.97.224.181	10.20.25.247
Connection #33	201.211.95.80	10.20.25.247
Connection #34	2.51.17.211	10.20.25.247
Connection #35	122.161.2.112	10.20.25.247
Connection #36	14.99.12.0	10.20.25.247
Connection #37	122.161.2.112	10.20.25.247
Connection #38	14.99.12.0	10.20.25.247
Connection #39	2.100.209.12	10.20.25.247
Connection #40	96.47.81.4	10.20.25.247
Connection #41	58.8.105.185	10.20.25.247
Connection #42	108.250.41.166	10.20.25.247
Connection #43	82.152.152.20	10.20.25.247
Connection #44	176.73.141.26	10.20.25.247
Connection #45	176.67.74.200	10.20.25.247

DNS Requests	
Request	**Result**
No activity	--

Virus Total Results	
Last Scanned:	**2013-05-02 10:15:52**
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	RDN/Generic PWS.y!nv
Malwarebytes:	Not Detected
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
Agnitum:	Not Detected
F-Prot:	W32/Trojan3.CEL
Symantec:	Trojan.Zbot
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	TROJ_GEN.F47V0501
Avast:	Not Detected
eSafe:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Trojan-Spy.Win32.Zbot.lazm
BitDefender:	Not Detected
NANO-Antivirus:	Not Detected
ViRobot:	Not Detected
Sophos:	Troj/Zbot-EXF
Comodo:	UnclassifiedMalware
F-Secure:	Not Detected
DrWeb:	Trojan.PWS.Panda.3734
VIPRE:	Not Detected
AntiVir:	Not Detected
TrendMicro:	TROJ_GEN.F47V0501
McAfee-GW-Edition:	Artemis!652D9919B209
Emsisoft:	Trojan.Win32.Agent.AMN (A)
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	PWS:Win32/Zbot
SUPERAntiSpyware:	Not Detected
AhnLab-V3:	Not Detected
GData:	Not Detected
Commtouch:	W32/Trojan.RBJZ-2752
ByteHero:	Virus.Win32.Heur.i
VBA32:	Not Detected
PCTools:	Trojan.Zbot
ESET-NOD32:	Win32/Spy.Zbot.AAU
Ikarus:	Trojan-PWS.Tepfer
Fortinet:	W32/Luder.VRQ!worm
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