



Analysis # 30721

05/21/2013 05:01 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	13
Network Activity	14
Network Events	14
Network Traffic	15
DNS Requests	16
Virus Total Results	17

Analysis Summary	
Submitted File:	Delivery_Information_ID_000512453420234_Pdf_____.exe
MD5:	791a8d50acfea465868dfe89cdadc1fc
File Size:	317440
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-05-21 05:01:11
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Tue, 21 May 2013 09:04:25 +0000
Termination Time:	Tue, 21 May 2013 09:04:38 +0000
Analysis Time:	2013-05-21 05:01:11
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	5
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 5] C:\Delivery_Information_ID_000512453420234_Pdf_____
_____.exe

[process 5] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp3b6d70cd.bat

Stored Modified Files
[process 1] C:\Documents and Settings\Administrator\Application Data\Ywce\orfe.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\tmp3b6d70cd.bat

Created Mutexes	
	mutex
[process 1]	Name: __PDH_PLA_MUTEX_ Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[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 1]	Name: MPSWabDataAccessMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: MPSWABOIkStoreNotifyMutex 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 2]	Name: Global\{12291916-02DB-9CC1-2788-B06D3412937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: __PDH_PLA_MUTEX_ 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\{12291916-02DB-9CC1-238C-B06D3016937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-F38E-B06DE014937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-578F-B06D4415937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-B78F-B06DA415937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-9B8F-B06D8815937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-EF8F-B06DFC15937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-4F88-B06D5C12937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-8B88-B06D9812937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-0389-B06D1013937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-7389-B06D6013937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-AB89-B06DB813937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-678B-B06D7411937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-4B8B-B06D5811937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-8B8D-B06D9817937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-D78D-B06DC417937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Global\{12291916-02DB-9CC1-7F8E-B06D6C14937F}

[process 2]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-4F8E-B06D5C14937F}
[process 2]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-7B8F-B06D6815937F}
[process 2]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-EB8C-B06DF816937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-1F8A-B06D0C10937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{7EB084F0-9F3D-F058-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{A8B6B2C3-A90E-265E-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{A45A65F1-7E3C-2AB2-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{A45A65F6-7E3B-2AB2-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Local\{C5BCD3E2-C82F-4B54-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Local\{C5BCD3E3-C82E-4B54-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{CE6286DB-9D16-408A-89D3-085A9A492B48}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-238C-B06D3016937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-F38E-B06DE014937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-578F-B06D4415937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-B78F-B06DA415937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-9B8F-B06D8815937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-EF8F-B06DFC15937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-4F88-B06D5C12937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-8B88-B06D9812937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-0389-B06D1013937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-7389-B06D6013937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-AB89-B06DB813937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-4B8B-B06D5811937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-8B8D-B06D9817937F}
[process 3]	Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE Name: Global\{12291916-02DB-9CC1-D78D-B06DC417937F}

[process 3]	Name: Global\{12291916-02DB-9CC1-7F8E-B06D6C14937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{12291916-02DB-9CC1-4F8E-B06D5C14937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\{12291916-02DB-9CC1-7B8F-B06D6815937F} Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Global\{12291916-02DB-9CC1-EB8C-B06DF816937F} 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: 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\Microsoft\Xyanpue
[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\
[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 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\

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\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\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Internet Account 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\Xyanpue Value: 30963e5
[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\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

	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\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\Xyanpue Value: 6c6egeb
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Xyanpue Value: 30963e5
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: orfe
[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: 13556: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\StandardProfile Value: DisableNotifications
[process 3]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List Value: 26534: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\Xyanpue Value: 2a5b7a95
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Xyanpue Value: 15cdaejc
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Xyanpue Value: b61h4a8
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Xyanpue Value: 15cdaejc
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Xyanpue Value: 15cdaejc
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Xyanpue Value: 15cdaejc
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Xyanpue Value: 445hc1
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Xyanpue Value: 24f61bai
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Xyanpue

	Value: 4ggejcf
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Xyanpue Value: 30963e5
[process 5]	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 3]	194.94.127.98	10.20.25.247	none
[process 3]	190.65.205.245	10.20.25.247	none
[process 3]	211.209.241.213	10.20.25.247	none
[process 3]	211.209.241.213	10.20.25.247	none
[process 3]	90.154.167.206	10.20.25.247	none
[process 3]	189.224.226.182	10.20.25.247	none
[process 3]	69.77.132.197	10.20.25.247	none
[process 3]	180.241.97.79	10.20.25.247	none
[process 3]	190.42.161.35	10.20.25.247	none

Network Traffic		
	Remote IP	Local IP
Connection #1	10.20.25.255	10.20.25.247
Connection #2	194.94.127.98	10.20.25.247
Connection #3	190.65.205.245	10.20.25.247
Connection #4	211.209.241.213	10.20.25.247
Connection #5	90.154.167.206	10.20.25.247
Connection #6	189.224.226.182	10.20.25.247
Connection #7	69.77.132.197	10.20.25.247
Connection #8	180.241.97.79	10.20.25.247

DNS Requests	
Request	Result
No activity	--

Virus Total Results	
Last Scanned:	2013-05-21 08:18:05
MicroWorld-eScan:	Gen:Variant.Kazy.176238
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	BackDoor-FJW!791A8D50ACFE
Malwarebytes:	Malware.Packer.132
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
NANO-Antivirus:	Not Detected
F-Prot:	Not Detected
Symantec:	WS.Reputation.1
Norman:	Hlux.ZY
TotalDefense:	Not Detected
TrendMicro-HouseCall:	TROJ_GEN.F47V0520
Avast:	Win32:Malware-gen
eSafe:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Worm.Win32.Luder.attek
BitDefender:	Gen:Variant.Kazy.176238
Agnitum:	Not Detected
SUPERAntiSpyware:	Not Detected
Sophos:	Not Detected
Comodo:	Not Detected
F-Secure:	Gen:Variant.Kazy.176238
DrWeb:	Not Detected
VIPRE:	Not Detected
AntiVir:	TR/Kazy.176238.19
TrendMicro:	Not Detected
McAfee-GW-Edition:	Heuristic.BehavesLike.Win32.Suspicious-BAY.G
Emsisoft:	Gen:Variant.Kazy.176238 (B)
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Win32.Heur.KVMF31.hy.(kcloud)
Microsoft:	PWS:Win32/Zbot.gen!AM
ViRobot:	Not Detected
AhnLab-V3:	Not Detected
GData:	Gen:Variant.Kazy.176238
Commtouch:	Not Detected
ByteHero:	Not Detected
VBA32:	Not Detected
PCTools:	Not Detected
ESET-NOD32:	a variant of Win32/Kryptik.BBKN
Rising:	Not Detected
Ikarus:	Virus.Agent
Fortinet:	W32/Kryptik.AGAJ!tr
AVG:	Agent
Panda:	Trj/CI.A

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.