



Analysis # 35917

01/21/2014 08:31 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	16
Network Events	16
Network Traffic	17
DNS Requests	18
Virus Total Results	19

Analysis Summary	
Submitted File:	Mitteilung,_Rechnungsruckstande_9901169820005294_Telekom_Deutschland_GmbH_vom_Januar_2014.exe
MD5:	0a907b46e277c9bdeffa7e9464095627
File Size:	172032
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-01-21 08:31:51
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Tue, 21 Jan 2014 13:37:39 +0000
Termination Time:	Tue, 21 Jan 2014 13:37:49 +0000
Analysis Time:	2014-01-21 08:31:51
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	10
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:\Mitteilung,_Rechnungsruckstande_9901169820005294_Telekom_Deutschland_GmbH_vom_Januar_2014.exe

[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp1.tmp.bat

[process 4] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\2MB9vCAAAA[1].htm

[process 4] C:\Documents and Settings\Administrator\Application Data\9CC20790\9CC20790.srv

[process 4] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\2MB9vCAAAA[1].htm

[process 4] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\2MB9vCAAAA[2].htm

[process 8] C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Outlook\k\~Outlook.pst.tmp

[process 8] C:\Documents and Settings\Administrator\Application Data\mail.txt

[process 9] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp2.tmp.exe

[process 9] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp4.tmp.bat

Stored Modified Files
[process 1] C:\Documents and Settings\Administrator\Application Data\KB00635017.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp1.tmp.bat
[process 4] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\2MB9vCAAAA[1].htm
[process 4] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp2.tmp.exe
[process 4] C:\Documents and Settings\Administrator\Application Data\9CC20790\9CC20790
[process 4] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp3.tmp.exe
[process 4] C:\Documents and Settings\Administrator\Application Data\9CC20790\9CC20790
[process 4] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\2MB9vCAAAA[1].htm
[process 4] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\2MB9vCAAAA[2].htm
[process 7] C:\Documents and Settings\Administrator\Application Data\KB00635017.exe
[process 7] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp4.tmp.bat
[process 8] C:\Documents and Settings\Administrator\Application Data\mail.txt
[process 8] C:\Documents and Settings\Administrator\Application Data\mail.txt
[process 8] C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Outlook\k\~Outlook.pst.tmp

Created Mutexes	
	mutex
[process 1]	Name: DirectSound DIIMain mutex (0x000003FC) Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\XMM000003FC Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\XMI000003FC Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: DirectSound DIIMain mutex (0x00000818) Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Local\XMM00000818 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\XMI00000818 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\XMM000007CC Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\XMI000007CC Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\XMQ426FB97F Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\XMR426FB97F Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\XMS426FB97F Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	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 4]	Name: Local\c:\documents and settings\administrator\cookies! Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	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 4]	Name: Local\WininetConnectionMutex Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\c:\documents and settings\administrator\ietldcache! Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\XMM0000011C Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\XMI0000011C Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Local\XMR426FB97F Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Local\XMM0000024C Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Local\XMI0000024C Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: Local\XMR426FB97F Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: DirectSound DIIMain mutex (0x00000C18) Desired Access: DELETE_READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 7]	Name: Local\XMM00000C18 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: Local\XMI00000C18 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\XMR426FB97F Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: DirectSound DllMain mutex (0x00000C78) Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\XMM00000C78 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\XMI00000C78 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\XMR426FB97F Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\OfficeSharedLocks_Heap_00_S-1-5-21-299502267-926492609-1801674531-500 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\OfficeSharedLocks_BootMutex_00_S-1-5-21-299502267-926492609-1801674531-500 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\4D4150494C6F676F6E0070B872C47FD7101B8BEA00AA0038C699_S-1-5-21-299502267-926492609-1801674531-500 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\OLKCRPC.OBJ=SharedMemoryMutex_S-1-5-21-299502267-926492609-1801674531-500 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\4F75746C6F6F6BEB498DBE739637498B3F9F6F820746DA_S-1-5-21-299502267-926492609-1801674531-500 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\4F75746C6F6F6BBCBE4FAF7A86B74781BAE296613AE61C_S-1-5-21-299502267-926492609-1801674531-500 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\4F75746C6F6F6BCEDF90DC33021940A52196694B62F8D8_S-1-5-21-299502267-926492609-1801674531-500 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: F802864900030000000028C7_CACHEMUTEX Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\TC-Rebuild-Mutex-00000040-0000808e Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\TC-Rebuild-Mutex-00000040-000080ce Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\TC-Rebuild-Mutex-00000040-000081ce Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\TC-Rebuild-Mutex-00000040-000081ee Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\TC-Rebuild-Mutex-00000040-0000820e Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: RasPbFile Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\ZonesCounterMutex Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\ZoneAttributeCacheCounterMutex Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\ZonesCacheCounterMutex

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: LocalZonesLockedCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: LocalXMM00000CDC Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: LocalXMI00000CDC Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: LocalXMR426FB97F Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: DirectSound DllMain mutex (0x00000D00) Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: LocalXMM00000D00 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 4]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows NT\S9CC20790
[process 4]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows NT\CBA6D3F36

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\Curr entVersion\Explorer\Shell Folders Value: AppData
[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\Curr entVersion\Explorer\Shell Folders Value: AppData
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: AppData
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: History
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Internet Settings Value: GlobalUserOffline
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: AppData
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Internet Settings Value: ProxyEnable
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Internet Settings Value: ProxyEnable
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Internet Settings Value: ProxyEnable
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: KB00635017.exe
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: KB00635017.exe
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: KB00635017.exe

	entVersion\Run Value: KB00635017.exe
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows NT\S 9CC20790 Value:
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: KB00635017.exe
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows NT\C BA6D3F36 Value:
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Internet Settings Value: ProxyEnable
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: KB00635017.exe
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: KB00635017.exe
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Run Value: KB00635017.exe
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: AppData
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: AppData
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Value: AppData
[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\Curr entVersion\Explorer\Shell Folders Value: AppData
[process 8]	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\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed

	Value: Seed
[process 8]	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\Office\14.0\Common\LanguageResources\EnabledLanguages Value: 1033
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages Value: 1033
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[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\Internet Settings Value: ProxyEnable
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

	Value: UNCAsIntranet
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[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 10]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData

Deleted Values	
	key
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer

ThreatAnalyzer Analysis # 35917

Sample: Mitteilung,_Rechnungsruckstande_9901169820005294_Telekom_Deutschland_Gm
bH_vom_Januar_2014.exe (0a907b46e277c9bdeffa7e9464095627)

	entVersion\Internet Settings
	Value: ProxyOverride
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Internet Settings
	Value: AutoConfigURL

Network Events			
	Remote IP	Local IP	HTTP Command
[process 4]	185.5.55.75	10.20.25.247	POST /J9/vp//EGa+AAAAAA/2MB9vCAAAA/
[process 8]	185.5.55.75	10.20.25.247	POST /m4/in/data.php?id=JONATHAN-C561E0_00:0C:29:5E:B4: D8

Network Traffic		
	Remote IP	Local IP
Connection #1	10.20.25.255	10.20.25.247
Connection #2	10.20.25.249	10.20.25.247
Connection #3	10.20.25.255	10.20.25.247

DNS Requests	
Request	Result
dshfyyst.ru	185.5.55.75

Virus Total Results	
Last Scanned:	2014-01-21 13:29:18
Bkav:	HW32.CDB.127b
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	PWSZbot-FPK!0A907B46E277
Malwarebytes:	Not Detected
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
NANO-Antivirus:	Not Detected
F-Prot:	Not Detected
Symantec:	Not Detected
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	Not Detected
Avast:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Not Detected
Agnitum:	Not Detected
SUPERAntiSpyware:	Not Detected
Ad-Aware:	Not Detected
Emsisoft:	Not Detected
Comodo:	Not Detected
DrWeb:	Not Detected
VIPRE:	Not Detected
AntiVir:	Not Detected
TrendMicro:	Not Detected
McAfee-GW-Edition:	PWSZbot-FPK!0A907B46E277
Sophos:	Not Detected
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Worm:Win32/Cridex.E
ViRobot:	Not Detected
AhnLab-V3:	Not Detected
GData:	Not Detected
Commtouch:	Not Detected
ByteHero:	Not Detected
VBA32:	Not Detected
ESET-NOD32:	a variant of Win32/Kryptik.BQRO
Rising:	PE:Malware.XPACK/RDM!5.1
Ikarus:	Not Detected
Fortinet:	Not Detected
AVG:	Not Detected
Baidu-International:	Not Detected
Qihoo-360:	HEUR/Malware.QVM20.Gen

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.