Analysis # 31603

07/08/2013 14:43 pm

Table of Contents

Analysis Summary

Submitted File:	Document_948357853____.exe
MD5:	d0b2d0f5b7e4b7adb6afe6928fa84c89
File Size:	990208
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-07-08 14:43:57
Start Reason:	AnalysisTarget
Termination Reason:	Timeout
Start Time:	Mon, 08 Jul 2013 18:44:36 +0000
Termination Time:	Mon, 08 Jul 2013 18:45:36 +0000
Analysis Time:	2013-07-08 14:43:57
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	1
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**	—

Stored Modified Files
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\89OC5JKA\ss32[1].exe
[process 1] C:\Documents and Settings\Administrator\Application Data\ss32.exe

Created Mutexes	
	mutex
[process 1]	Name: RasPbFile
	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

Set Values	
	key
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system Value: EnableLUA
[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: 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\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common 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\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\Internet Settings Value: ProxyEnable
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[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\CurrentVersion\Internet Settings
	Value: ProxyEnable
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
	Value: SavedLegacySettings

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

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process 1]	176.32.99.121	10.20.25.247	GET /mik49/ss32.exe
[process 1]	127.0.0.1	127.0.0.1	none

Network Traffic		
	Remote IP	**Local IP**
Connection #1	10.20.25.255	10.20.25.247

DNS Requests	
Request	**Result**
s3.amazonaws.com	176.32.99.121
mpa.one.microsoft.com	94.245.126.106
	207.46.84.65

Virus Total Results	
Last Scanned:	**2013-07-08 18:09:19**
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CAT-QuickHeal:	(Suspicious) - DNAScan
McAfee:	Not Detected
Malwarebytes:	Trojan.Downloader.VM
K7AntiVirus:	Trojan
K7GW:	Trojan
TheHacker:	Not Detected
NANO-Antivirus:	Not Detected
F-Prot:	Not Detected
Symantec:	Suspicious.MH690.A
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	Not Detected
Avast:	Not Detected
eSafe:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Gen:Variant.Symmi.7971
Agnitum:	Suspicious!SA
ViRobot:	Not Detected
Sophos:	Mal/Agent-AKZ
Comodo:	Not Detected
F-Secure:	Gen:Variant.Symmi.7971
DrWeb:	Not Detected
VIPRE:	Not Detected
AntiVir:	TR/Crypt.TPM.Gen
TrendMicro:	Not Detected
McAfee-GW-Edition:	Heuristic.LooksLike.Win32.EPO.F
Emsisoft:	Gen:Variant.Symmi.7971 (B)
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
SUPERAntiSpyware:	Not Detected
AhnLab-V3:	Dropper/Win32.Dapato
GData:	Gen:Variant.Symmi.7971
Commtouch:	Not Detected
ByteHero:	Trojan.Win32.Heur.087
PCTools:	HeurEngine.MaliciousPacker
ESET-NOD32:	Not Detected
Rising:	Not Detected
Ikarus:	Not Detected
Fortinet:	Not Detected
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