GFI SandBox™
Automated malware analysis

Analysis # 20236

09/19/2012 18:24 pm

http://www.gfi.com/ATG

GFI ADVANCED TECHNOLOGY GROUP

Table of Contents

Analysis Summary

Submitted File:	Lab03-04.exe
MD5:	b94af4a4d4af6eac81fc135abda1c40c
File Size:	61440
File Type:	PE32 executable for MS Windows (console) Intel 803
Analysis Time:	2012-09-19 18:24:54
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Wed, 19 Sep 2012 22:25:36 +0000
Termination Time:	Wed, 19 Sep 2012 22:25:37 +0000
Analysis Time:	2012-09-19 18:24:54
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	2
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:\Lab03-04.exe

Created Mutexes	
	mutex
[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

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\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\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\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\{3259504a-e161-11e0-bf1d-806d6172696f} Value: BaseClass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\ShellNoRoam\MUICache Value: C:\WINDOWS\system32\cmd.exe
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process]			none

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

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

Virus Total Results	
Last Scanned:	**2012-09-09 12:52:55**
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Artemis!B94AF4A4D4AF
K7AntiVirus:	Not Detected
TheHacker:	Not Detected
VirusBuster:	Not Detected
F-Prot:	Not Detected
Symantec:	Trojan.Gen.2
Norman:	W32/Suspicious_Gen2.VHYUP
TotalDefense:	Not Detected
TrendMicro-HouseCall:	TROJ_GEN.R4FH1EI
Avast:	Win32:Malware-gen
eSafe:	Win32.TRDownloader
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Not Detected
ViRobot:	Not Detected
ByteHero:	Not Detected
Emsisoft:	Trojan-Downloader!IK
Comodo:	UnclassifiedMalware
F-Secure:	Not Detected
DrWeb:	Not Detected
VIPRE:	Trojan.Win32.Generic!BT
AntiVir:	TR/Downloader.Gen
TrendMicro:	Not Detected
McAfee-GW-Edition:	Artemis!B94AF4A4D4AF
Sophos:	Not Detected
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Microsoft:	Not Detected
SUPERAntiSpyware:	Not Detected
GData:	Win32:Malware-gen
Commtouch:	Not Detected
AhnLab-V3:	Not Detected
VBA32:	Not Detected
PCTools:	Trojan.Gen
ESET-NOD32:	Not Detected
Rising:	Not Detected
Ikarus:	Trojan-Downloader
Fortinet:	Not Detected
AVG:	Downloader.Generic12.CGOL
Panda:	Not Detected

GFI Advanced Technology Group
33 North Garden Avenue, Suite 1200, Clearwater, Florida, USA 33755
Telephone: (855) 4-GFI-ATG (855-443-4284) Intl: +1(813)367-9907
Email: atg@gfi.com