GFI SandBox™
Automated malware analysis

Analysis # 20972

10/05/2012 16:34 pm

http://www.gfi.com/ATG

GFI ADVANCED TECHNOLOGY GROUP

Table of Contents

Analysis Summary

Submitted File:	google_born_help.exe
MD5:	584fe856bb348e0089f7b59ec31881a5
File Size:	540672
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2012-10-05 16:34:40
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Fri, 05 Oct 2012 20:35:49 +0000
Termination Time:	Fri, 05 Oct 2012 20:36:39 +0000
Analysis Time:	2012-10-05 16:34:40
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 4] C:\google_born_help.exe
[process 4] C:\GOOGLE~1.EXE
[process 4] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~unins5164.bat

Stored Modified Files
[process 1] C:\WINDOWS\system32\dpserial1.exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~unins5164.bat

Created Mutexes	
	mutex
[process 2]	Name: WBEMPROVIDERSTATICMUTEX
	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\MNWYQKAAQR
[process 1]	\REGISTRY\MACHINE\Software\MNWYQKAAQR
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
[process 1]	\Registry\Machine\System\CurrentControlSet\Control\Session Manager

Set Values

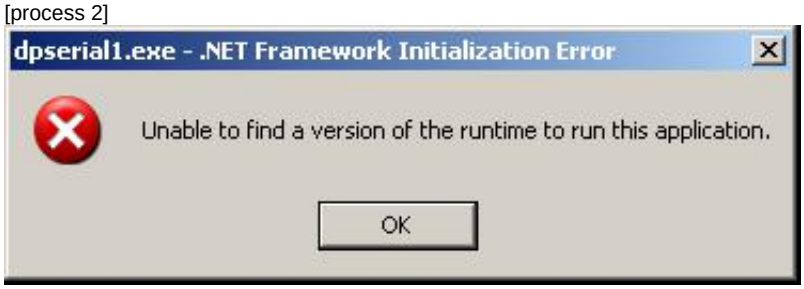
	key
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG 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\MNWYQKAAQR Value: Hy
[process 1]	Key Name: \REGISTRY\MACHINE\Software\MNWYQKAAQR Value: Hy
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Value: Pyio
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: 6
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: 6
[process 1]	Key Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Session Manager Value: PendingFileRenameOperations
[process 2]	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\ShellNoRoam\MUICache Value: C:\WINDOWS\system32\dpserial1.exe
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\SessionInformation Value: ProgramCount
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\SessionInformation Value: ProgramCount
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process 1]	88.216.164.117	10.20.25.247	GET /tg.aspx
[process 1]	88.216.164.117	10.20.25.247	GET /tg.aspx

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

DNS Requests	
Request	**Result**
intohave.com	64.179.44.188

[process 2]



Virus Total Results	
Last Scanned:	**2012-10-05 19:56:21**
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Not Detected
K7AntiVirus:	Not Detected
TheHacker:	Not Detected
F-Prot:	Not Detected
Symantec:	Suspicious.Cloud.5
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	Not Detected
Avast:	Not Detected
eSafe:	Not Detected
ClamAV:	Not Detected
BitDefender:	Not Detected
Agnitum:	Not Detected
SUPERAntiSpyware:	Not Detected
ByteHero:	Not Detected
Sophos:	Not Detected
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
VIPRE:	Not Detected
AntiVir:	Not Detected
TrendMicro:	Not Detected
McAfee-GW-Edition:	Not Detected
Emsisoft:	Not Detected
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
ViRobot:	Not Detected
Commtouch:	Not Detected
AhnLab-V3:	Not Detected
VBA32:	Not Detected
PCTools:	Not Detected
ESET-NOD32:	Not Detected
Rising:	Not Detected
Ikarus:	Not Detected
Fortinet:	W32/Kryptik.KO!tr
AVG:	Not Detected
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