



**GFI SandBox**<sup>™</sup>  
*Automated malware analysis*

**Analysis # 20972**

10/05/2012 16:34 pm

## Table of Contents

<b>Analysis Summary</b> .....	<b>3</b>
<b>Analysis Summary</b> .....	<b>3</b>
<b>Digital Behavior Traits</b> .....	<b>3</b>
<b>File Activity</b> .....	<b>4</b>
<b>Deleted Files</b> .....	<b>4</b>
<b>Stored Modified Files</b> .....	<b>5</b>
<b>Created Mutexes</b> .....	<b>6</b>
<b>Created Mutexes</b> .....	<b>6</b>
<b>Registry Activity</b> .....	<b>7</b>
<b>Created Keys</b> .....	<b>7</b>
<b>Set Values</b> .....	<b>8</b>
<b>Network Activity</b> .....	<b>9</b>
<b>Network Events</b> .....	<b>9</b>
<b>Network Traffic</b> .....	<b>10</b>
<b>DNS Requests</b> .....	<b>11</b>
<b>Screen Shots</b> .....	<b>12</b>
<b>Virus Total Results</b> .....	<b>13</b>

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			
<b>Alters Windows Firewall</b>		<b>Hooks Keyboard</b>	
<b>Checks For Debugger</b>		<b>Injected Code</b>	
<b>Copies to Windows</b>		<b>Makes Network Connection</b>	
<b>Could Not Load</b>		<b>Modifies File in System</b>	
<b>Creates DLL in System</b>		<b>Modifies Local DNS</b>	
<b>Creates EXE in System</b>		<b>More than 5 Processes</b>	
<b>Creates Hidden File</b>		<b>Opens Physical Memory</b>	
<b>Creates Mutex</b>		<b>Starts EXE in Documents</b>	
<b>Creates Service</b>		<b>Starts EXE in Recycle</b>	
<b>Deletes File in System</b>		<b>Starts EXE in System</b>	
<b>Deletes Original Sample</b>		<b>Windows/Run Registry Key Set</b>	

**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	
	<b>mutex</b>
[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\MNWHYQKAAQR Value: Hy
[process 1]	Key Name: \REGISTRY\MACHINE\Software\MNWHYQKAAQR 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\Shell\NoRoam\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

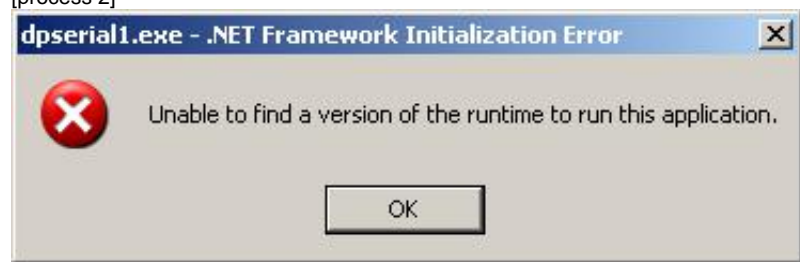


Network Events			
	Remote IP	Local IP	HTTP Command
[process 1]	88.216.164.117	10.20.25.247	GET /tg.aspx
[process 1]	88.216.164.117	10.20.25.247	GET /tg.aspx

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	
<b>Last Scanned:</b>	<b>2012-10-05 19:56:21</b>
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](mailto:atg@gfi.com)

Disclaimer © 2011. GFI Software. 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. GFI Software 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, GFI 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. GFI 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.