

Baidu Antivirus 2013 With Windows Firewall (Updated and Modified Settings) Malware Security

User Interface:



The Only Thing I Modified Was Enabling "Browser Protection"!



System Memory:

- 6 Running Process (Including Windows Firewall)
- 24 Megabytes of ram
- Not heavy on system

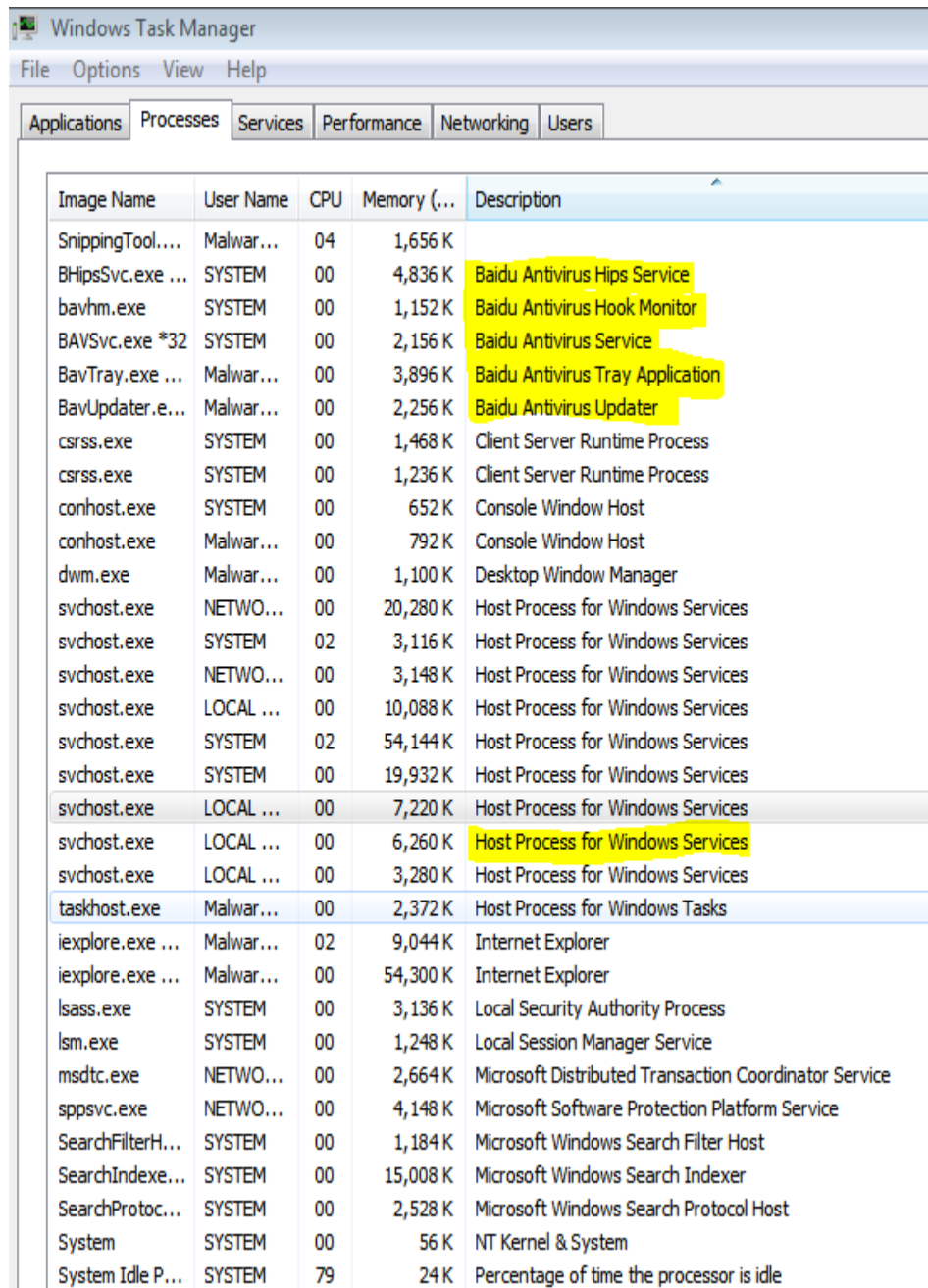


Image Name	User Name	CPU	Memory (...)	Description
SnippingTool...	Malwar...	04	1,656 K	
BHipsSvc.exe ...	SYSTEM	00	4,836 K	Baidu Antivirus Hips Service
bavhm.exe	SYSTEM	00	1,152 K	Baidu Antivirus Hook Monitor
BAVSvc.exe *32	SYSTEM	00	2,156 K	Baidu Antivirus Service
BavTray.exe ...	Malwar...	00	3,896 K	Baidu Antivirus Tray Application
BavUpdater.e...	Malwar...	00	2,256 K	Baidu Antivirus Updater
csrss.exe	SYSTEM	00	1,468 K	Client Server Runtime Process
csrss.exe	SYSTEM	00	1,236 K	Client Server Runtime Process
conhost.exe	SYSTEM	00	652 K	Console Window Host
conhost.exe	Malwar...	00	792 K	Console Window Host
dwm.exe	Malwar...	00	1,100 K	Desktop Window Manager
svchost.exe	NETWO...	00	20,280 K	Host Process for Windows Services
svchost.exe	SYSTEM	02	3,116 K	Host Process for Windows Services
svchost.exe	NETWO...	00	3,148 K	Host Process for Windows Services
svchost.exe	LOCAL ...	00	10,088 K	Host Process for Windows Services
svchost.exe	SYSTEM	02	54,144 K	Host Process for Windows Services
svchost.exe	SYSTEM	00	19,932 K	Host Process for Windows Services
svchost.exe	LOCAL ...	00	7,220 K	Host Process for Windows Services
svchost.exe	LOCAL ...	00	6,260 K	Host Process for Windows Services
svchost.exe	LOCAL ...	00	3,280 K	Host Process for Windows Services
taskhost.exe	Malwar...	00	2,372 K	Host Process for Windows Tasks
ieexplore.exe ...	Malwar...	02	9,044 K	Internet Explorer
ieexplore.exe ...	Malwar...	00	54,300 K	Internet Explorer
lsass.exe	SYSTEM	00	3,136 K	Local Security Authority Process
lsmd.exe	SYSTEM	00	1,248 K	Local Session Manager Service
msdtc.exe	NETWO...	00	2,664 K	Microsoft Distributed Transaction Coordinator Service
sppsvc.exe	NETWO...	00	4,148 K	Microsoft Software Protection Platform Service
SearchFilterH...	SYSTEM	00	1,184 K	Microsoft Windows Search Filter Host
SearchIndexe...	SYSTEM	00	15,008 K	Microsoft Windows Search Indexer
SearchProtoc...	SYSTEM	00	2,528 K	Microsoft Windows Search Protocol Host
System	SYSTEM	00	56 K	NT Kernel & System
System Idle P...	SYSTEM	79	24 K	Percentage of time the processor is idle

30 Web Links (Zero to 1 Day Old Links):

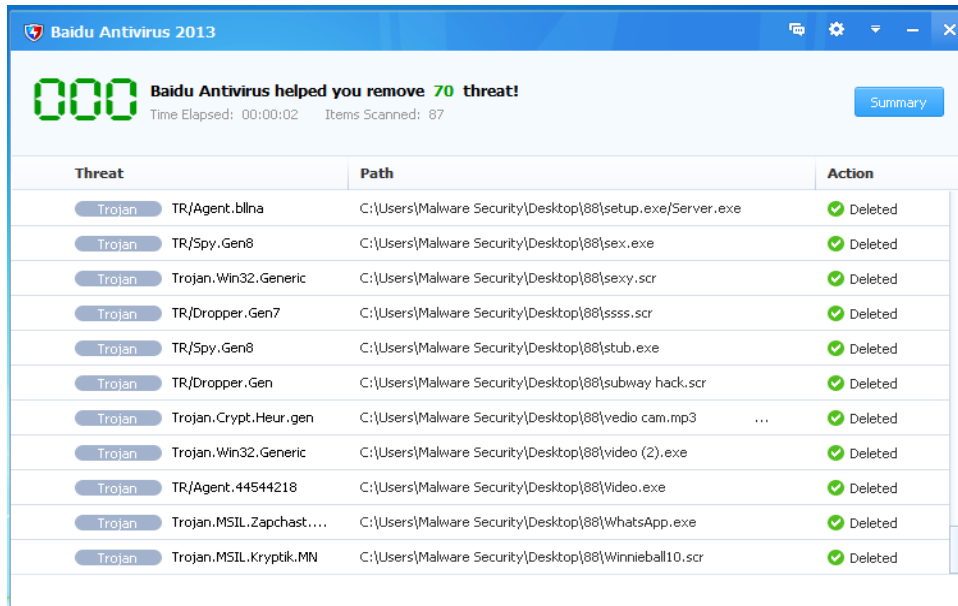
- **19/30 Links Blocked**

Missed Links:

1.	download-sponsor.de/exe/campaigns/gutscheinfilter_19062013.exe---	6/39	virus	Total	Blocked
2.	54.227.80.146/xtra.exe-----	12/39	virus	Total	Blocked
3.	update.multispeed.co.kr/set/multispeedsetup_scn.exe-----	11/39	virus	Total	Missed
4.	twpost.com.tw/css/Facebook.zip-----	3/39	virus	Total	Blocked
5.	img.zing.vn/longtuong/images/data/11_09_2013/long_tuong.rar-----	3/38	virus	Total	Blocked
6.	i1.stylefun.info/addons/agent_setup.exe-----	13/39	virus	Total	Blocked
7.	forextraderobot.org/sec.exe-----	14/39	virus	Total	Blocked
8.	farmacia237.hol.es/site/Nfe-Emitida.PDF.zip-----	3/39	virus	Total	Blocked
9.	bytesprotector.org/faqs/Iserve.bin-----	12/39	virus	Total	Missed
10.	clientpadfile.info/files/MTI_Car2_Img_Puzzle.exe-----	4/39	virus	Total	Missed
11.	all4kids.at/Fotos.zip-----	6/39	virus	Total	Blocked
12.	37.9.53.121/Mony.exe?ts=7a35aeb15ed3e7b98c5e022b81bfb89b6c696a96-----	8/39	virus	Total	Blocked
13.	3cubed.com.au/download/support.exe-----	4/39	virus	Total	Blocked
14.	3rdgengraphix.com/img/hh56.exe-----	11/39	virus	Total	Blocked
15.	61.156.8.95/JINING/jwxclient-sd.exe-----	10/39	virus	Total	Blocked
16.	68.228.8.88/GG0sqZw9.exe-----	12/39	virus	Total	Blocked
17.	74.208.147.18/install_flashplayer11x32_mssa_aaa_aih.exe-----	9/39	virus	Total	Blocked
18.	81.17.28.154/b.exe-----	12/39	virus	Total	Blocked
19.	93.89.236.171/soft.exe-----	10/39	virus	Total	Blocked
20.	94.102.50.37/met.exe-----	8/39	virus	Total	Blocked
21.	abensoft.com/download/ac.exe-----	3/39	virus	Total	Missed
22.	adamasit.com/7GaE.exe-----	10/39	virus	Total	Missed
23.	adexprt.me/get/vlc-1.1.10-win32-Final.exe-----	6/39	virus	Total	Missed
24.	akl.waw.pl/modules/mod_menu/install_flashplayer.cpl-----	11/39	virus	Total	Blocked
25.	alllinuxapplicationsy.asia/v713?byt&q=d0015690.rar&installer_file_name=d0015690.rar&product_name=d0015690.rar-----	3/39	virus	Total	Missed
26.	app.updateserv.net/u/update/FunkLyrics_1060-2060_v133.exe?id=106942c7838E609A-----	5/39	virus	Total	Missed
27.	aresplus.com/descargar/AresPlus_MN.exe-----	8/39	virus	Total	Missed
28.	atl.org.mx/images/stories/ebayfattura.pif?cmd=_Processing&dispatch=5885d80a13c0db1fb6947b0a6e66fdbfb2119927117e3a6f876e0fd34af4365165f8e3ce4d30224a1c298ecc89c1a5e165f8e3ce4d30224a1c298ecc89c1a5e-----	5/39	virus	Total	Blocked
29.	atlandtic.fr/wp-content/uploads/atlandtic.exe-----	6/39	virus	Total	Missed
30.	bddx1.newyx.net/nizhanxzhusoufzhuv139.exe-----	7/39	virus	Total	Missed

Malware Pack Containing 88 Files (1 Day Old Files):

70/88 Files detected = 79.55%



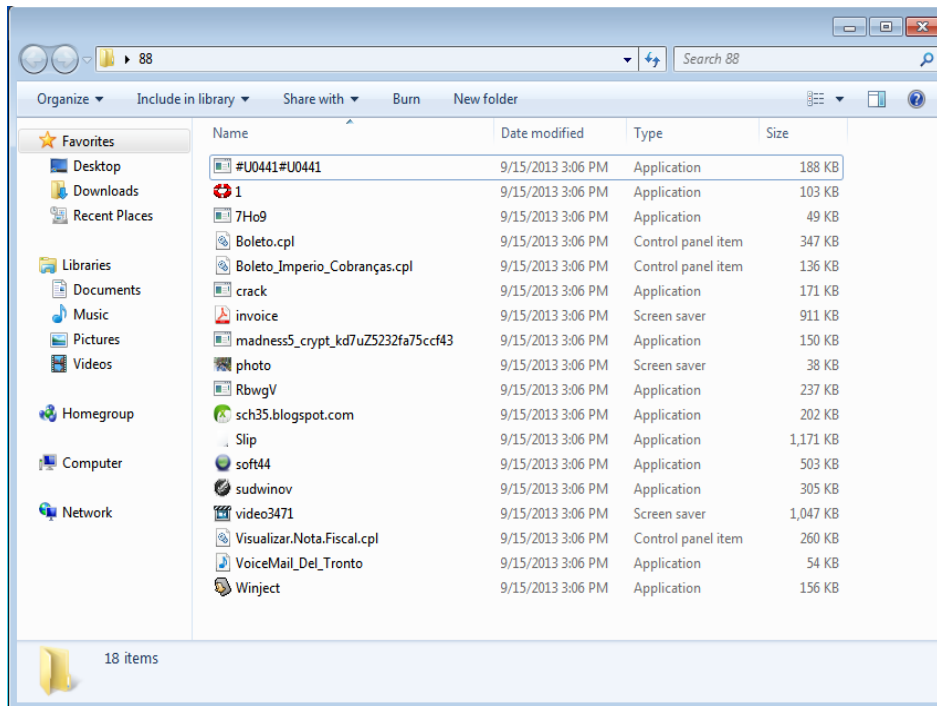
Baidu Antivirus 2013

Baidu Antivirus helped you remove 70 threat!

Time Elapsed: 00:00:02 Items Scanned: 87

[Summary](#)

Threat	Path	Action
Trojan	TR/Agent.blna C:\Users\Malware Security\Desktop\88\setup.exe/Server.exe	Deleted
Trojan	TR/Spy.Gen8 C:\Users\Malware Security\Desktop\88\sex.exe	Deleted
Trojan	Trojan.Win32.Generic C:\Users\Malware Security\Desktop\88\sexy.scr	Deleted
Trojan	TR/Dropper.Gen7 C:\Users\Malware Security\Desktop\88\ssss.scr	Deleted
Trojan	TR/Spy.Gen8 C:\Users\Malware Security\Desktop\88\stub.exe	Deleted
Trojan	TR/Dropper.Gen C:\Users\Malware Security\Desktop\88\subway hack.scr	Deleted
Trojan	Trojan.Crypt.Heur.gen C:\Users\Malware Security\Desktop\88\vedio cam.mp3 ...	Deleted
Trojan	Trojan.Win32.Generic C:\Users\Malware Security\Desktop\88\video (2).exe	Deleted
Trojan	TR/Agent.44544218 C:\Users\Malware Security\Desktop\88\Video.exe	Deleted
Trojan	Trojan.MSIL.Zapchast.... C:\Users\Malware Security\Desktop\88\WhatsApp.exe	Deleted
Trojan	Trojan.MSIL.Kryptik.MN C:\Users\Malware Security\Desktop\88\Winnieball10.scr	Deleted



88

Search 88

Organize Include in library Share with Burn New folder

Name	Date modified	Type	Size
#U0441#U0441	9/15/2013 3:06 PM	Application	188 KB
1	9/15/2013 3:06 PM	Application	103 KB
7Ho9	9/15/2013 3:06 PM	Application	49 KB
Boleto.cpl	9/15/2013 3:06 PM	Control panel item	347 KB
Boleto_Imperio_Cobranças.cpl	9/15/2013 3:06 PM	Control panel item	136 KB
crack	9/15/2013 3:06 PM	Application	171 KB
invoice	9/15/2013 3:06 PM	Screen saver	911 KB
madness5_crypt_kd7uZ5232fa75ccf43	9/15/2013 3:06 PM	Application	150 KB
photo	9/15/2013 3:06 PM	Screen saver	38 KB
RbwgV	9/15/2013 3:06 PM	Application	237 KB
sch35.blogspot.com	9/15/2013 3:06 PM	Application	202 KB
Slip	9/15/2013 3:06 PM	Application	1,171 KB
soft44	9/15/2013 3:06 PM	Application	503 KB
sudwinov	9/15/2013 3:06 PM	Application	305 KB
video3471	9/15/2013 3:06 PM	Screen saver	1,047 KB
Visualizar.Nota.Fiscal.cpl	9/15/2013 3:06 PM	Control panel item	260 KB
VoiceMail_Del_Tronto	9/15/2013 3:06 PM	Application	54 KB
Winject	9/15/2013 3:06 PM	Application	156 KB

18 items

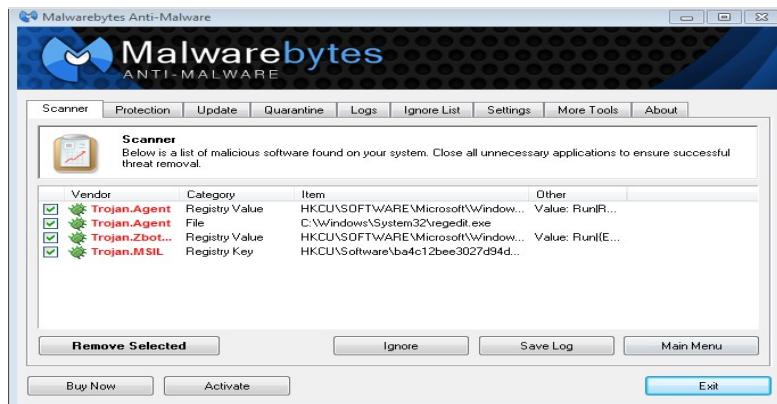
Caught Later By Behavioral Blocking, Firewall, Etc.:

I executed all missed 18 files in malware pack and Baidu detected 6/18 files!

Hitmanpro and Malwarebytes results after behavioral blocking test:

Not including the "Destop\88\," Hitmanpro detected 11 System infections!

Visualizar.Nota.Fiscal.cpl C:\Users\Malware Security\Desktop\88\	Trojan	Sun 15 Sep 2013 15:23	Deleted
rezyula.exe C:\Users\Malware Security\AppData\Roaming\Qyifors\	Remnant	Sun 15 Sep 2013 15:23	Deleted
nviert.dll C:\Users\Malware Security\AppData\Roaming\	Trojan	Sun 15 Sep 2013 15:23	Deleted
neprt.dll C:\Users\Malware Security\AppData\Roaming\	Trojan	Sun 15 Sep 2013 15:23	Deleted
ba4c12bee3027d94da5c81db2d196bfd.exe C:\Users\Malware Security\AppData\Roaming\Microsoft\Wind	Trojan	Sun 15 Sep 2013 15:23	Deleted
pearomzobdoz.exe C:\Users\Malware Security\	Trojan	Sun 15 Sep 2013 15:23	Deleted
Winject.exe C:\Users\Malware Security\Desktop\88\	Malware	Sun 15 Sep 2013 15:23	Deleted
Winject.exe C:\Users\Malware Security\Desktop\88\	Malware	Sun 15 Sep 2013 15:23	Deleted
soft44.exe C:\Users\Malware Security\Desktop\88\	Trojan	Sun 15 Sep 2013 15:23	Deleted
photo.scr C:\Users\Malware Security\Desktop\88\	Trojan	Sun 15 Sep 2013 15:23	Deleted
madness5_crypt_kd7uZ5232fa75ccf43.exe C:\Users\Malware Security\Desktop\88\	Ransomware	Sun 15 Sep 2013 15:23	Deleted
crack.exe C:\Users\Malware Security\Desktop\88\	Trojan	Sun 15 Sep 2013 15:23	Deleted
Boleto_Imperio_Cobranças.cpl C:\Users\Malware Security\Desktop\88\	Trojan	Sun 15 Sep 2013 15:23	Deleted
Boleto.cpl C:\Users\Malware Security\Desktop\88\	Trojan	Sun 15 Sep 2013 15:23	Deleted
Boleto.cpl C:\Users\Malware Security\Desktop\88\	Trojan	Sun 15 Sep 2013 15:23	Deleted
1.exe C:\Users\Malware Security\Desktop\88\	Malware	Sun 15 Sep 2013 15:23	Deleted
issu.exe C:\Users\Malware Security\AppData\Roaming\Vaum\	Trojan	Sun 15 Sep 2013 15:23	Deleted
ba4c12bee3027d94da5c81db2d196bfd.exe C:\Users\Malware Security\AppData\Roaming\Microsoft\Wind	Trojan	Sun 15 Sep 2013 15:23	Deleted
svchost.exe C:\Users\Malware Security\AppData\Local\Temp\	Trojan	Sun 15 Sep 2013 15:23	Deleted
cxsoxnar.exe C:\Users\Malware Security\AppData\Local\	Trojan	Sun 15 Sep 2013 15:23	Deleted
A6Q8k4S.exe C:\Users\Malware Security\AppData\Local\0z3X4Y5R3N\	Malware	Sun 15 Sep 2013 15:23	Deleted
A6Q8k4S.exe C:\Users\Malware Security\AppData\Local\0z3X4Y5R3N\	Malware	Sun 15 Sep 2013 15:23	Deleted
A0z3X4Y.exe C:\Users\Malware Security\AppData\Local\0z3X4Y5R3N\	Trojan	Sun 15 Sep 2013 15:23	Deleted



5 Star Rating:

- **1 Star: User-friendly: 1/1 Star**
- **1 Star: Low Ram Usage, 60mb or less: 1/1 Star**
- **1 Star: 24/30 Web Links, 80%: 0/1 Star**
- **1 Star: Detection 85%+: 0/1 Star**
- **1 Star: Behavioral Blocking, 50%+: 0/1 Star**

2/5

Summary:

Advantages:

- It has a nice and easy user interface
- Really low ram usage including windows firewall with it!
- Really quick scan and removal
- Its free

Disadvantages:

- **Not great on web protection**
- **Not so great on detection rate!**
- **Behavioral blocking seems to work, but couldn't stay consistent!**
- **It kept giving me the same “start up is being modified alert” on the same files even though I click “block it”. So basically, it couldn't block the “start up is being modified alert”!**

According to my testings, Baidu needs to improve on the disadvantages. Since there are other antivirus programs that are free and better, Baidu is literally going to disappear in the black hole if they do not step it up. I would not recommend this antivirus to users unless they show improvements!

