

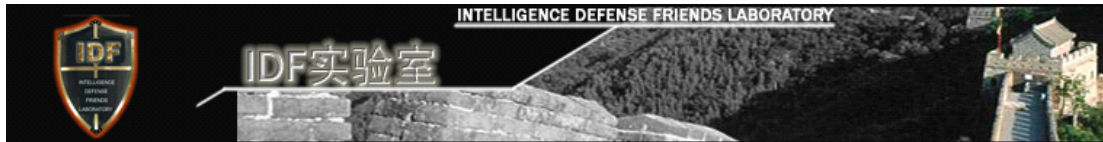


**Independent Report on Alleged “Hidden Backdoor” in
Qihoo 360 Secure Browser**

.



IDF Laboratory
Release Date: November 25, 2012



IDF Laboratory	Version: <1.4>
Independent Report on Alleged “Hidden Backdoor” in Qihoo 360 Secure Browser	Date: <24/11/2012>
Document Sign:IDF-REPDOC-20121124	

Copyright Statement

This research report is compiled by IDF laboratory, unless it is published and agreed, its copyright belongs to IDF laboratory. While the quoted parts in the report belong to the original writer or corresponding units. Without the permission of IDF laboratory and the writer, any unit and individual are not allowed to transfer the contents of this report or use for other purpose, and this report is only for the reference of the industry research without commercial purposes. Welcome your criticism and correction.

IDF Laboratory (Intelligence Defense Friends Laboratory) is a technical civil club for the enthusiasts of network information security, the backbone of which is made up of professionals, technicians and hobbyists from relevant fields. The research direction of IDF mainly focus on: the technical fields such as the development tendency of Internet threat, terminal security management, communication security of wireless network, botnet, as well as product research. IDF laboratory provides universal education of computer security knowledge for a great many enthusiasts of network information security, participates in the evaluation of the technology and market research for the products and development trends of relevant fields within the industry objectively and independently, thus providing the platform and bridge for the enthusiasts of network information security to be grow up as professional security or technical employees.



Contents

1. Executive Summary.....	3
2. Background.....	4
3. Objective.....	5
4. Testing Environment.....	6
5. Testing Procedures.....	6
5.1. System Environment Preparation.....	6
5.2. Detection of the function of ExtSmartWiz.dll.....	7
5.3. Monitoring File Operation of 360 Secure Browser.....	8
5.4. Monitoring Network Communication of 360 Secure Browser.....	11
5.5. Comparing the Network Communications of 360 Secure Browser with IE.....	14
5.6. Validating the caller of ExtSmartWiz.dll.....	14
a. Confirming the Timer Setting.....	15
b. Confirming the Request and Instruction Code of the Server.....	16
c. Confirming the Instruction Code of the Executive Program.....	16
5.7. Detection of the File of “Backdoor Program”.....	17
a. Analyzing STB*.tmp File Resources.....	17
b. Analysis of the Input Table of ExtSmartWiz.dll File.....	21
6. Testing Results.....	22
7. Appendix I.....	26
7.1. Comparing with the Technical Analysis by @独立调查员.....	26
7.2. “Public Letter to MIIT and the Ministry of Public Security for Public whistle-blowing of Qihoo 360”.....	27
8. Appendix II.....	30
8.1. Revision History.....	30
8.2. Acknowledgement.....	30

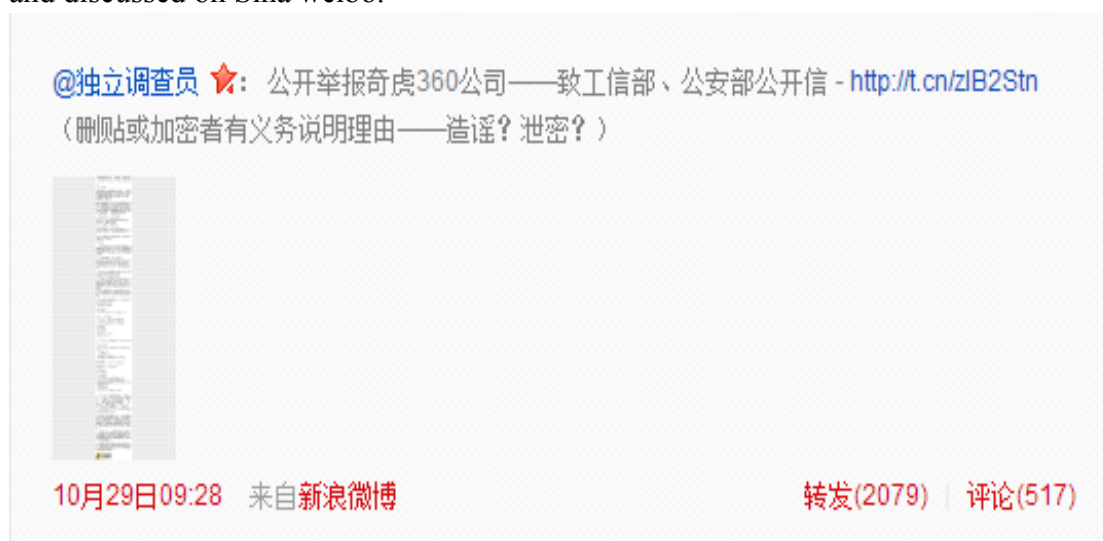


1.Executive Summary

We performed through testing on an alleged “hidden backdoor” in 360 secure browser. Our testing results are as follows: 1) 360 secure browser indeed has an undeclared mechanism (i.e., via ExtSmartWiz.dll) which connects to the server on a regular basis (e.g., every 5 minutes), and allows it to download files of any type (including executables) from the server. 2) In our testing, the downloaded file is a non-harmful resource file containing configuration data related to baidu. According to 360, this resource file is used to mitigate a cross site scripting (XSS) vulnerability in a script from Baidu that redirects users to baidu.com who click upon a baidu search result from within so.com. 3) Users are not given any notice when a file is downloaded from the server, and this mechanism is not declared in <360 Users Privacy Protection White Paper>. According to 360, this mechanism does not upload any user data thus it is not declared in the white paper. While this statement seems reasonable, we believe users should be made aware of this mechanism since it is capable of downloading executable files that could have impact on both user privacy and system security. Further, we strongly encourage 360 to review the necessity of mechanism and replace it, if it is not absolutely required, with a more transparent and less powerful approach that could both serve its business need, and address user concerns.

2. Background


On October 29, 2012, Sina weibo user @独立调查员 published a message titled of “*Public Letter to MIIT and the Ministry of Public Security for Public whistle-blowing of Qihoo 360*”(Hereinafter referred to as: public letter). The letter alledged, with the support of technical analysis that “360 Secure Browser of Qihoo 360 has ‘Hidden Backdoor’, which threatens both end users system security and its competitor’s product and service experience.” This public letter is widely circulated and discussed on Sina weibo.




On October 30, 2012, Tao Weihua, the Product Director of 360 Secure Browser responded to this letter in Sina weibo by saying “Whoever has a mind to beat a dog





will always be able to find a stick”. He criticized that @独立调查员 is here to “Smear 360 on behalf of Baidu”. @独立调查员 replied to Tao Weihua on November 3 by saying that Tao's response is the worst professional response in the history. He emphasized that the key point here is that 360 Secure Browser has a hidden backdoor, namely ExtSmartWiz.dll, which allows 360 to take control of all users’ computers within five minutes, and do whatever it likes to do.


@360陶伟华 : 方舟子转发一篇名为《公开举报奇虎360公司——致工信部、公安部公开信》，作者是一直给他提供材料的“独立调查员”。方舟子说《公开信》“写得很清楚”，但哪里写得清楚？方舟子自己也没说清楚。对《公开信》提出的问题，我们做一一解答如下，也请方舟子看一看我们解答得清楚不清楚。



10月30日20:27 来自360浏览器超速版 转发(283) | 评论(347)

On November 5, 2012, @独立调查员 published a video showing the evidence of “360 Secure Browser Set up Hidden Backdoor”.

@独立调查员 : 【视频证据】《360安全浏览器暗设后门》反向分析测试过程全记录。这道后门对用户信息与系统安全、互联网整体安全均构成严重威胁，证据确凿，毋庸置疑。360早前回应纯属欺骗用户。详情及原始视频请进 - <http://t.cn/zlKpjOG> 在线播放(播放器右下角选择高清并进入全屏) - <http://t.cn/zlFkoYL> 



11月6日 22:16 来自新浪微博 转发(311) | 评论(108)

3. Objective

The objective of this report is responded to the disputed hot topics regarding the rights and interests of number Internet users and the reputation of Internet security industry objectively and scientifically from the perspective of the civil independent third party.

The detection of this report based on the contents and test methods described in “Public Letter to MIIT and the Ministry of Public Security for public whistle-blowing



of *Qihoo 360* published in the Sina weibo by @独立调查员. The purpose is to test whether the evidence contents, detection phenomenon, detection methods for 360 Secure Browser's "hidden backdoor" described in the public letter are correct, true, non-repudiation or not, so as to assess whether the issue of 360 Secure Browser has hidden backdoor deduced in the public letter is real or not, as well as the credibility of the conclusion that this issue threatens information security system and system security of the ordinary users, thus providing reference for the judgment of relevant competent department of the government, authorized detection department, Internet security industry and enthusiast.

4. Testing Environment

360 Secure Browser:

Version: v5.0.8.7

MD5: C9F83C447966502B8B937F534F59E5DD

Download Address: http://down.360safe.com/se/360se_5.0_20121025.exe

Virtual Machine Environment	
VMware Workstation	v8.0.4 build-744019
Operation System	Windows XP Professional SP3
Detection Tools	
Document Monitoring Tool	Filemon
Process Monitoring Tool	procexp
Network Monitoring Tool	SocketSniff
Decompilation Tool	OllyICE
PE View Tool	LoadPE
Resource View Tool	Restorator 2007

5. Testing Procedures

According to the description in the public letter of @独立调查员, ExtSmartWiz.dll in the installation path of 360 Secure Browser is the backdoor program, so we will confirm whether ExtSmartWiz.dll is doubtful or not via the detection and monitoring of this program, and the monitoring of the operation and network communication data of 360 Secure Browser v5.0.8.7 file.

5.1. System Environment Preparation

In order to avoid interference of other software or program in detection, the software not to be detected will be closed or unloaded, the program execution condition in the system environment is as shown by figure 1:



Figure 1

5.2. Detection of the function of ExtSmartWiz.dll

Finish the initial installation of 360 Secure Browser v5.0.8.7 and operate it, and we can see the expansion use of 360 default installation (Figure 2) in “360 Expansion Center” and “My Expansion”. According to the description of public letter of @独立调查员, the expansion applications installed in %AppData%\360se\Apps of Windows XP System, backup AppsLocal.ver file under this path, in accordance with the file name and contents, we can infer that the type of the expansion, version and the download address of the corresponding server for this file is the browser of the local users,

Delete all the extended application in “My Expansion”, reopen the AppsLocal.ver file, there is only configuration information about ExtSmartWiz.dll (Figure 3), compare with the backup of AppsLocal.ver, we find that ExtSmartWiz.dll is not the expansion application of 360 Secure Browser.



Figure 2

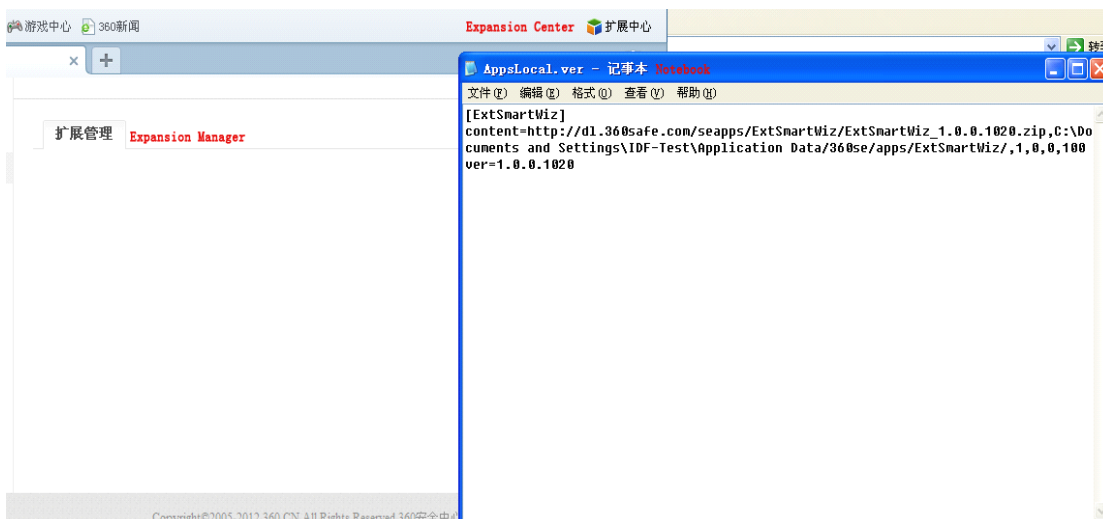


Figure 3

5.3. Monitoring File Operation of 360 Secure Browser

Operate file monitoring software filemon and then operate 360 Secure Browser v5.0.8.7. In order to reduce the intervention of file monitoring not belongs to 360 Secure Browser progress, set file monitoring filtering condition in filemon containing operation record of “360” file(Figure 4).

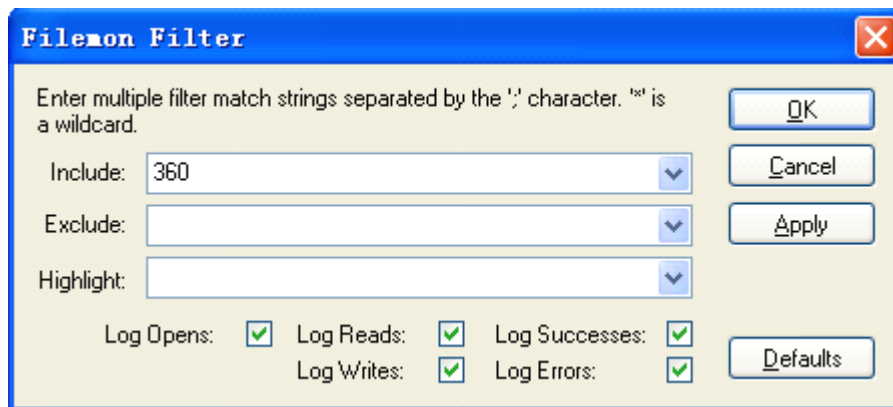


Figure 4

This monitoring took 22:00 on the detection day as the start time, under the condition without user operation; the file operation record of the file monitoring program is as the following figure:

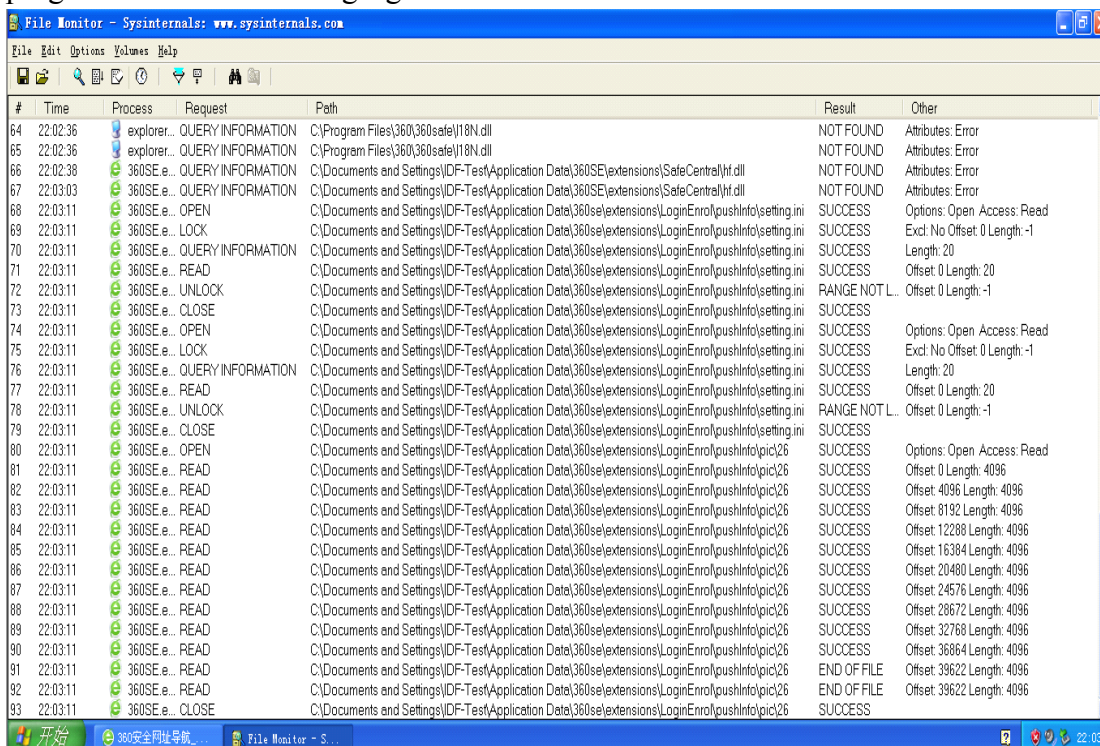


Figure 5

Seen from figure 5, we know 360 Secure Browser will first read 360se\extensions\LoginEnrol\pushInfo\setting.ini under the path of %AppData% under the condition without user operation, and then read 360se\extensions\LoginEnrol\pushInfo\pic\26 file.

Within the monitoring time (22:00 to 22:10), 360 Secure Browser v5.0.8.7 read setting.ini file every minute as well as read the behavior record of the file named 26.



#	Time	Process	Request	Path	Result	Other
135	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp	SUCCESS	Options: Open Access: Read-Attributes
136	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp	SUCCESS	FileFsVolumeInformation
137	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp	SUCCESS	FileInternalInformation
138	22:04:17	360SE.exe:280	CREATE	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Options: Create Access: Read
139	22:04:17	360SE.exe:280	OPEN	C:\	SUCCESS	Options: Open Directory Access: 00100001
140	22:04:17	360SE.exe:280	DIRECTORY	C:\	SUCCESS	FileBothDirectoryInformation: DOCUME~1
141	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\	SUCCESS	Options: Open Directory Access: 00100001
142	22:04:17	360SE.exe:280	DIRECTORY	C:\DOCUME~1\IDF-Test\	SUCCESS	FileBothDirectoryInformation: LOCALS~1
143	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	FileFsVolumeInformation
144	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	FileInternalInformation
145	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Length: 0
146	22:04:17	360SE.exe:280	CLOSE	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	
147	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp	SUCCESS	Options: Open Access: Read-Attributes
148	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp	SUCCESS	FileFsVolumeInformation
149	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp	SUCCESS	FileInternalInformation
150	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Options: Open Access: Read-Attributes
151	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	FileFsVolumeInformation
152	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	FileInternalInformation
153	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Length: 0
154	22:04:17	360SE.exe:280	CREATE	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Options: Overwriteif Access: 00120196
155	22:04:17	360SE.exe:280	OPEN	C:\	SUCCESS	Options: Open Directory Access: 00100001
156	22:04:17	360SE.exe:280	DIRECTORY	C:\	SUCCESS	FileBothDirectoryInformation: DOCUME~1
157	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\	SUCCESS	Options: Open Directory Access: 00100001
158	22:04:17	360SE.exe:280	DIRECTORY	C:\DOCUME~1\IDF-Test\	SUCCESS	FileBothDirectoryInformation: LOCALS~1
159	22:04:17	360SE.exe:280	WRITE	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Offset 0 Length: 9080
160	22:04:17	360SE.exe:280	CLOSE	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	
161	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Options: Open Access: Read
162	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Length: 9080
163	22:04:17	360SE.exe:280	READ	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Offset 0 Length: 9080
164	22:04:17	360SE.exe:280	READ	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Offset 3584 Length: 8

Figure 6

#	Time	Process	Request	Path	Result	Other
174	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	FileNamedInformation
175	22:04:17	360SE.exe:280	OPEN	C:\	SUCCESS	Options: Open Directory Access: 00100001
176	22:04:17	360SE.exe:280	DIRECTORY	C:\	SUCCESS	FileBothDirectoryInformation: DOCUME~1
177	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\	SUCCESS	Options: Open Directory Access: 00100001
178	22:04:17	360SE.exe:280	DIRECTORY	C:\DOCUME~1\IDF-Test\	SUCCESS	FileBothDirectoryInformation: LOCALS~1
179	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Length: 9080
180	22:04:17	360SE.exe:280	CLOSE	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	
181	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Attributes: A
182	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Attributes: A
183	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Options: Open Access: 00100020
184	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	FileNamedInformation
185	22:04:17	360SE.exe:280	OPEN	C:\	SUCCESS	Options: Open Directory Access: 00100001
186	22:04:17	360SE.exe:280	DIRECTORY	C:\	SUCCESS	FileBothDirectoryInformation: DOCUME~1
187	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\	SUCCESS	Options: Open Directory Access: 00100001
188	22:04:17	360SE.exe:280	DIRECTORY	C:\DOCUME~1\IDF-Test\	SUCCESS	FileBothDirectoryInformation: LOCALS~1
189	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Length: 9080
190	22:04:17	360SE.exe:280	CLOSE	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	
191	22:04:17	360SE.exe:280	READ	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Offset 3072 Length: 512
192	22:04:17	360SE.exe:280	READ	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Offset 1024 Length: 2048
193	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	Options: Open Access: 00010080
194	22:04:17	360SE.exe:280	OPEN	C:\	SUCCESS	Options: Open Directory Access: 00100001
195	22:04:17	360SE.exe:280	DIRECTORY	C:\	SUCCESS	FileBothDirectoryInformation: DOCUME~1
196	22:04:17	360SE.exe:280	OPEN	C:\DOCUME~1\IDF-Test\	SUCCESS	Options: Open Directory Access: 00100001
197	22:04:17	360SE.exe:280	DIRECTORY	C:\DOCUME~1\IDF-Test\	SUCCESS	FileBothDirectoryInformation: LOCALS~1
198	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	FileFsVolumeInformation
199	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	FileInternalInformation
200	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	FileStandardInformation
201	22:04:17	360SE.exe:280	QUERY INFORMATION	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	FileAttributeTagInformation
202	22:04:17	360SE.exe:280	DELETE	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	
203	22:04:17	360SE.exe:280	CLOSE	C:\DOCUME~1\IDF-Test\LOCALS~1\Temp\STB9.tmp	SUCCESS	

Figure 7

In this monitoring of the behavior of file operation, 360 Secure Browser v5.0.8.7 will create and write the temporary file of STB9.tmp under the path of %Temp% under the condition that no user is operating, with size of 9,080 bytes, and then delete this file after read it (Figure 6 and Figure 7).

During the monitoring time (22:00 to 22:10), 360 Secure Browser creates, writes and reads the temporary file and then delete this temporary file at 22:04 and 22:09 respectively. Temporary file created at 22:04 named STB9.tmp, while the one created at 22:09 named STBA.tmp.

Now we can verify @独立调查员's description in the public letter: in every five



minutes, 360 Secure Browser will generate the temporary file with “STB” as the prefix.

5.4. Monitoring Network Communication of 360 Secure Browser

In order to avoid the network communication of 360 Cloud Security Plan interfere with this monitoring of net socket, set up that 360 Secure Browser v5.0.8.7 canceled the participation of “Improvement Plan of User Experience”, and close the security function in the security center (Figure 8). As to the “Download Cloud Security” and “Online Bank Cloud Security” that can not be closed, the security functions both effective when downloading and using Online Bank will be introduced at 360 Secure Browser security function experience page. During network monitoring process, the page of 360 Secure Browser is always the common Website of se:blank, therefore, there is no download and Online Bank unfold.

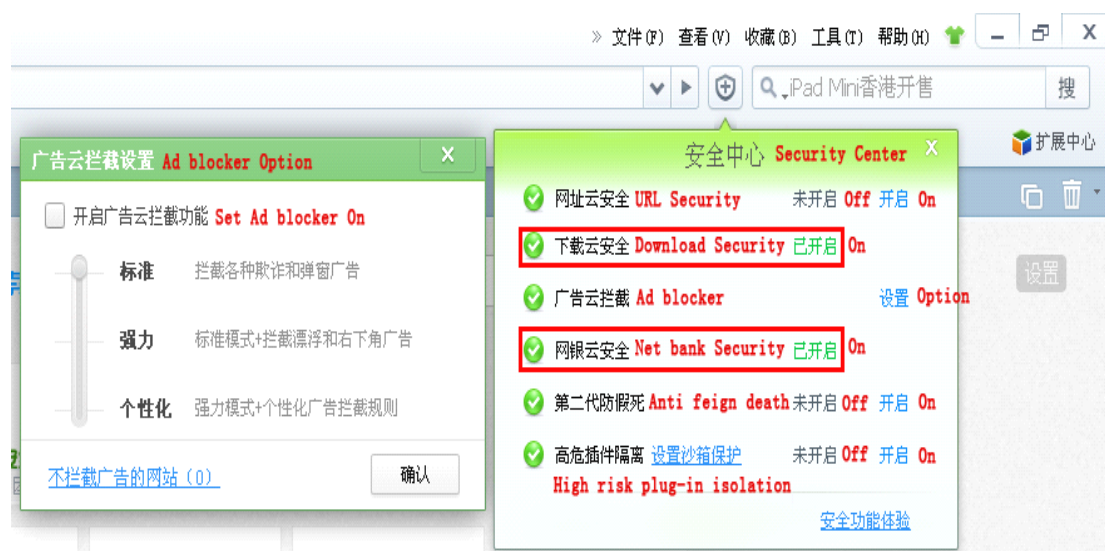


Figure 8

Operate network of SocketSniff, and set the network monitoring process of this tool as the process of 360 Secure Browser 360SE.exe.

The start time for this network monitoring is 22:28, and the finish time is 22:43, the duration is 15 minutes. The record for the network monitoring is as the following figure:

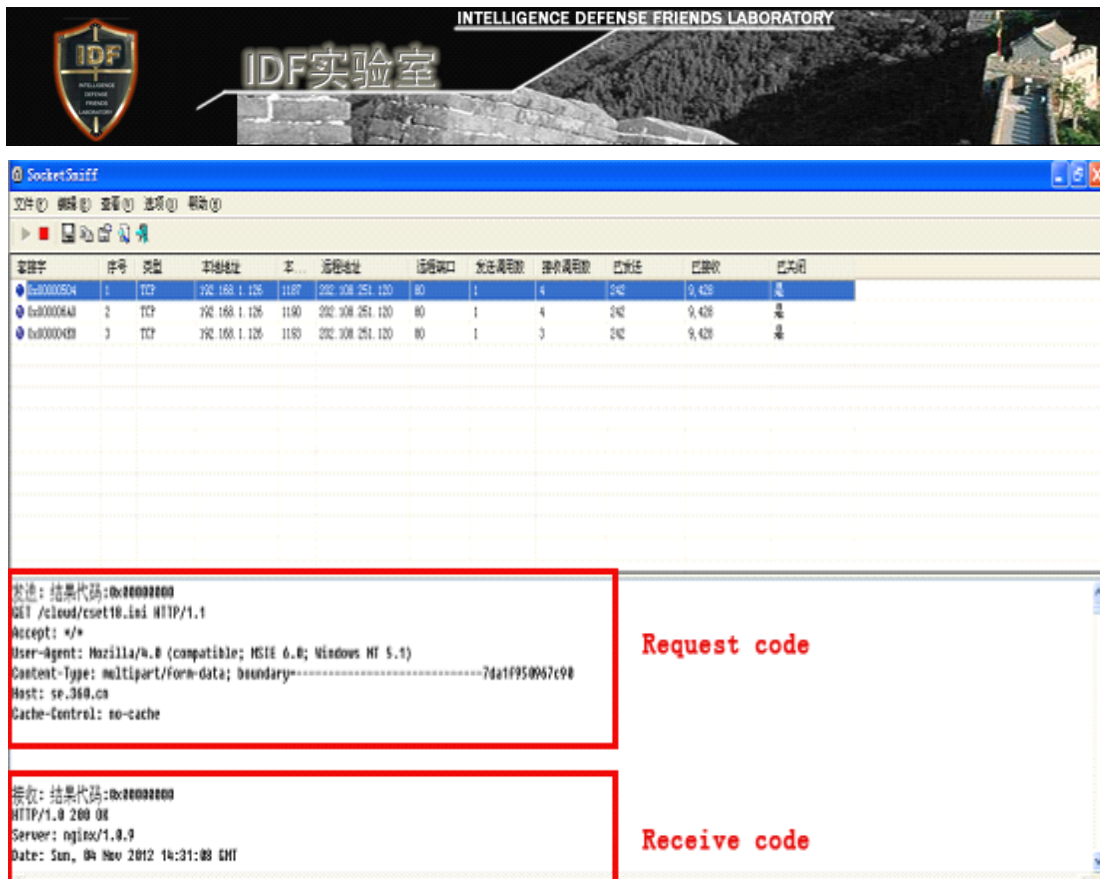


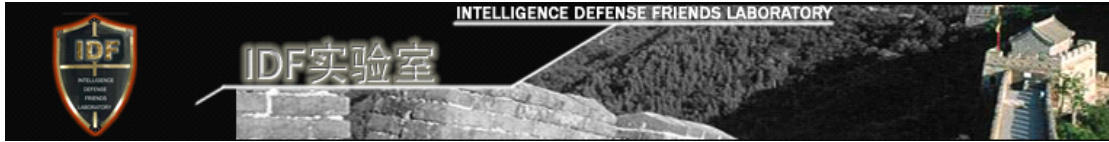
Figure 9

Seen from figure 9, every five minutes during the 15 minutes, 360 Secure Browserv5.0.8.7 will request the data packet from IP: 202.185.251.120, and receive the data packet.

The following are some of the data grasped from SocketSniff, and analyse the grabbed communication data we can find:

① The demand file is cset18.ini file under the cloud path on the target IP server, and the domain name of the host computer corresponding to target IP is se.360.cn. Therefore, in accordance with the domain name of the target server and the path of the file, we even can download the file requested by 360 Secure Browser v5.0.8.7 through browsing <http://se.360.cn/cloud/cset18.ini>.

② Acquire the file with size of 9,080 bytes, and the last revision time is October 18, 2012, and we can preliminary determine the obtained file type is PE file according to the content of the grasped data, but it's not a ini file type in the record of file request. So we can verify the description of the download file type of @ 独立调查员 's public letter: "the new instruction disguised that INI (Plain Text File Type) was sent out, but in fact it is Dll file (executable program library or resource library)".



发送(Send): 结果代码(Result code):0x00000000
GET /cloud/cset18.ini HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: multipart/form-data; boundary=-----7dc9b950967ee8
Host: se.360.cn
Cache-Control: no-cache

接收(Receive): 结果代码(Result code):0x00000000
HTTP/1.0 200 OK
Server: nginx/1.0.9
Date: Sun, 04 Nov 2012 14:41:08 GMT
Content-Type: application/octet-stream
Content-Length: 9080
Last-Modified: Thu, 18 Oct 2012 06:19:51 GMT
Expires: Sun, 04 Nov 2012 14:46:08 GMT
Cache-Control: max-age=300
Accept-Ranges: bytes
Age: 100
Powered-By-ChinaCache: HIT from 060010D3B7
Connection: close

接收(Receive): 结果代码(Result code):0x00000000

00000000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....
00000010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....
00000020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030	00 00 00 00 00 00 00 00 00 00 00 00 C0 00 00 00
00000040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68!..L.!Th
00000050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
00000060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
00000070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode...\$......
00000080	5F EF 1F DB 1B 8E 71 88 1B 8E 71 88 1B 8E 71 88	_...q...q...q.
00000090	2D A8 7A 88 1A 8E 71 88 DC 88 77 88 1A 8E 71 88	-z...q...w...q.
000000A0	52 69 63 68 1B 8E 71 88 00 00 00 00 00 00 00 00	Rich..q.....
000000B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000C0	50 45 00 00 4C 01 02 00 C8 6D 41 50 00 00 00 00	PE..L...mAP...
000000D0	00 00 00 00 E0 00 0E 21 0B 01 06 00 00 00 00 00!.....
000000E0	00 0A 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00
000000F0	00 10 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00
00000100	04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00
00000110	00 30 00 00 00 04 00 00 D1 7A 00 00 02 00 00 00	.0.....z.....
00000120	00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00



5.5. Comparing the Network Communications of 360 Secure Browser with IE

According to the introduction of the Official Website (<http://se.360.cn/>) of Qihoo 360 Secure Browser, 360 Secure Browser use IE 8 core, in order to verify whether the automatic request and data receive of IE core Browser is caused by IE core or not, this monitoring use IE browser (8.0.6001.18702 version) to implement network monitoring. The start time for the monitoring is 22:55, and the finish time is 23:10, and the monitoring duration is 15 minutes.

Figure 10

As shown by the above figure, during the monitoring time period, IE browser does not request or receive any data packet, thus we conclude that it is 360 Secure Browser v5.0.8.7, not the IE8 core, that, automatically requests and receives data packet.

5.6. Validating the caller of ExtSmartWiz.dll

In order to verify whether or not ExtSmartWiz.dll is really called by 360 Secure Browser, operate process monitoring tool procexp, search ExtSmartWiz.dll. And the research results are as the figure below:

名称	描述	公司名	版本
explorer.exe		Microsoft Corporation	7,376 K Windows Explorer
vmtoolsd.exe		VMware, Inc.	12,324 K VMware Tools Core Ser...
ctfmon.exe		Microsoft Corporation	3,520 K CTF Loader
360SE.exe		360.cn	18,784 K 360安全浏览器
urlproc.exe		360.cn	6,120 K 360安全浏览器 安全中心...
c_20127.nls			
clbcatq.dll		Microsoft Corporation	2001.12.4414...
comctl32.dll	User Experience Controls L...	Microsoft Corporation	6.0.2900.6028
comdlg32.dll	Common Dialogs DLL	Microsoft Corporation	6.0.2900.5512
comres.dll		Microsoft Corporation	2001.12.4414...
crypt32.dll	Crypto API32	Microsoft Corporation	5.131.2600.6237
cryptdll.dll	Cryptography Manager	Microsoft Corporation	5.1.2600.5512
ctype.nls			
dciman32.dll	DCI Manager	Microsoft Corporation	5.1.2600.5512
ddraw.dll	Microsoft DirectDraw	Microsoft Corporation	5.3.2600.5512
ddrawex.dll	Direct Draw Ex	Microsoft Corporation	5.3.2600.5512
dnsapi.dll	DNS Client API DLL	Microsoft Corporation	5.1.2600.6089
Doctor.dll	360安全浏览器 浏览器医生	360.cn	5.0.0.1008
dsound.dll	DirectSound	Microsoft Corporation	5.3.2600.5512
ExtNetIncrement.dll	360安全浏览器 ExtNetIncrement	360.cn	1.0.0.1006
ExtSmartWiz.dll	360安全浏览器 ExtSmartWiz	360.cn	1.0.0.1020

CPU 使用: 7.25% | 认可用量: 20.88% | 进程: 26 | 物理内存使用: 41.16%



Figure 11

In the public letter of @独立调查员, we know about the internal process of the file via the decompilation of ExtSmartWiz.dll under the path of 360 Secure Browser. So we decompile ExtSmartWiz.dll with OllyICE tool, and compare the result with the decompilation contents described in the public letter, so as to detect whether the description of the decompilation of this file described by @独立调查员 is true or not.

a. Confirming the Timer Setting

地址	HEX 数据	反汇编 Reverse assembler
100B451F	. 8B45 F8	mov eax,[local.2]
100B4522	. 8B48 04	mov ecx,dword ptr ds:[eax+4]
100B4525	. 8B12	mov edx,dword ptr ds:[edx]
100B4527	. 8B42 08	mov eax,dword ptr ds:[edx+8]
100B452A	. FFD0	call eax
100B452C	. 8945 EC	mov [local.5],eax
100B452F	. 68 E0930400	push 493E0
100B4534	. 6A 64	push 64
100B4536	. 8B4D EC	mov ecx,[local.5]
100B4539	. 8B11	mov edx,dword ptr ds:[ecx]
100B453B	. 8B4D EC	mov ecx,[local.5]
100B453E	. 8B42 08	mov eax,dword ptr ds:[edx+8]
100B4541	. FFD0	call eax
100B4543	> 8BE5	mov esp,eop
100B4545	. 5D	pop ebp
100B4546	. C3	retn

Figure 12

地址	HEX 数据	反汇编 Reverse assembler	注释 Notes
100BB99C	. 74 22	je short ExtSmart.100BB9C0	
100BB99E	. 8B55 F4	mov edx,[local.3]	
100BB9A1	. 8B42 3C	mov eax,dword ptr ds:[edx+3C]	
100BB9A4	. 83C0 04	add eax,4	
100BB9A7	. 8945 F8	mov [local.2],eax	
100BB9AA	. 6A 00	push 0	Timerproc = NULL
100BB9AC	. 8B4D 0C	mov ecx,[arg.2]	Timeout
100BB9AF	. 51	push ecx	TimerID
100BB9B0	. 8B55 08	mov edx,[arg.1]	
100BB9B3	. 52	push edx	
100BB9B4	. 8B45 F8	mov eax,[local.2]	
100BB9B7	. 8B08	mov ecx,dword ptr ds:[eax]	
100BB9B9	. 51	push ecx	hWnd
100BB9BA	. FF15 84441211	call dword ptr ds:[<USER32.SetTimer>]	SetTimer
100BB9C0	> 8BE5	mov esp,eop	
100BB9C2	. 5D	pop ebp	
100BB9C3	. C2 0800	retn 8	



Figure 13

As shown by figure 12, ExtSmartWiz.dll call the function of the file address 100BB970 after setting the timer as 493E0 (30000 milliseconds), and the content of this function is as the figure, and call the SetTimer from it to set the timer.

b. Confirming the Request and Instruction Code of the Server

地址	HEX 数据	反汇编 Reverse assembler	注释 Notes
100C2F16	75 14	jnz short ExtSmart.100C2F2C	
100C2F18	C785 9CFBFFFI	mov dword ptr ss:[ebp-464],-2	
100C2F22	E9 EC0C0000	jmp ExtSmart.100C3C13	
100C2F27	E9 E70C0000	jmp ExtSmart.100C3C13	
100C2F2C	6A 00	push 0	
100C2F2E	6A 00	push 0	
100C2F30	6A 00	push 0	
100C2F32	6A 00	push 0	
100C2F34	68 AC491210	push ExtSmart.101249AC	
100C2F39	FF15 64451211	call dword ptr ds:[<&WININET.InternetOpenW]	wininet.InternetOpenW
100C2F3F	8985 E8FDFFFI	mov dword ptr ss:[ebp-218],eax	
100C2F45	83BD E8FDFFFI	cmp dword ptr ss:[ebp-218],0	
100C2F4C	75 14	jnz short ExtSmart.100C2F62	
100C2F4E	C785 9CFBFFFI	mov dword ptr ss:[ebp-464],-3	
100C2F58	E9 B60C0000	jmp ExtSmart.100C3C13	
100C2F5D	E9 B10C0000	jmp ExtSmart.100C3C13	
100C2F62	6A 00	push 0	

Figure 14

As shown by figure 14, ExtSmartWiz.dll call InternetOpenW function to send domain name request from the function at the file address of 100C2D90.

c. Confirming the Instruction Code of the Executive Program

地址	HEX 数据	反汇编 Reverse assembler	注释 Notes
100B89BE	51	push ecx	
100B89BF	FF15 08431211	call dword ptr ds:[<&KERNEL32.LoadLibraryW]	LoadLibraryW
100B89C5	8945 F0	mov [local.4],eax	
100B89C8	837D F0 00	cmp [local.4],0	
100B89CC	0F84 C9000000	je ExtSmart.100B8A9B	
100B89D2	837D 0C 00	cmp [arg.2],0	
100B89D6	0F84 B5000000	je ExtSmart.100B8A91	
100B89DC	68 3E080000	push 83E	ResourceType = 83E
100B89E1	8B55 0C	mov edx,[arg.2]	
100B89E4	52	push edx	ResourceName
100B89E5	8B45 F0	mov eax,[local.4]	
100B89E8	50	push eax	hModule
100B89E9	FF15 1C431211	call dword ptr ds:[<&KERNEL32.FindResourceW]	FindResourceW
100B89EF	8945 CC	mov [local.13],eax	
100B89F2	837D CC 00	cmp [local.13],0	
100B89F6	0F84 95000000	je ExtSmart.100B8A91	
100B89FC	8B4D CC	mov ecx,[local.13]	

Figure 15

As shown by figure 15, ExtSmartWiz.dll call LoadLibraryW function from the function at file address of 100B8970 to load the file, and search and lock the resource in DLL file after loading, namely, reach the resources in DLL file.



According to the above code detection, as described in the public letter of @独立调查员, there are indeed timer setting, file for application of serve and the file code of the sever after loading or downloading existing in ExtSmartWiz.dll File.

5.7. Detection of the File of “Backdoor Program”

a. Analyzing STB*.tmp File Resources

In order to confirm that the remote server request and the function of download DLL File is provided by ExtSmartWiz.dll, we backed up this file and then deleted it, via file monitoring and network monitoring, we did not find any record about temporary file creation or reception of the request file. So we verify the function of this file contain the request and reception of data packet from the Server.

As ExtSmartWiz.dll will delete the downloaded file after obtaining the Server File, therefore, set the user permission of content Temp as refuse deletion (Figure 16).

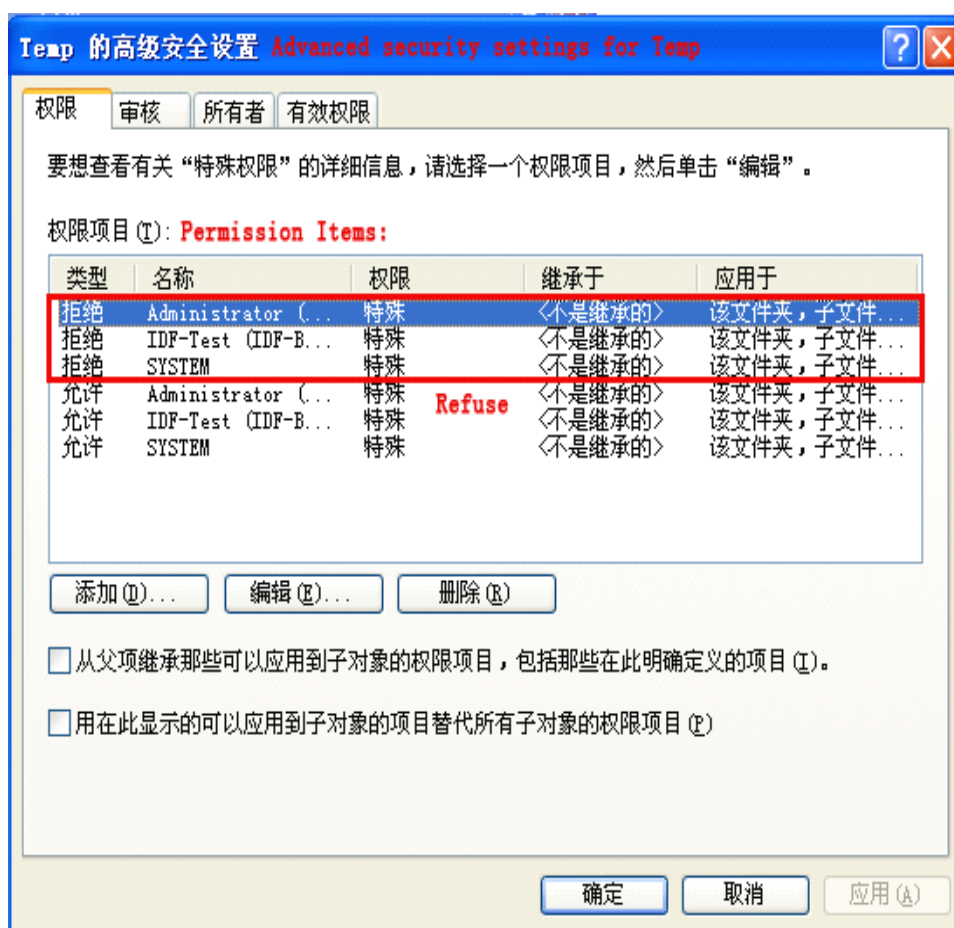


Figure 16

Wait for about 5 minutes when 360 secure Browser is operating, we obtain the download file of STB7C.tmp from the Server, for the convenience of detection, copy this file to the desktop. Unfold this file with LoadPE tool, and check up eigenvalue (Figure 17), and we can see the type of this file is .dll. Check up the File Directory Table we find this file has no input list nor output list. But this file contains RCData type resource and self-defined 2110 type INI resource (Figure 18).

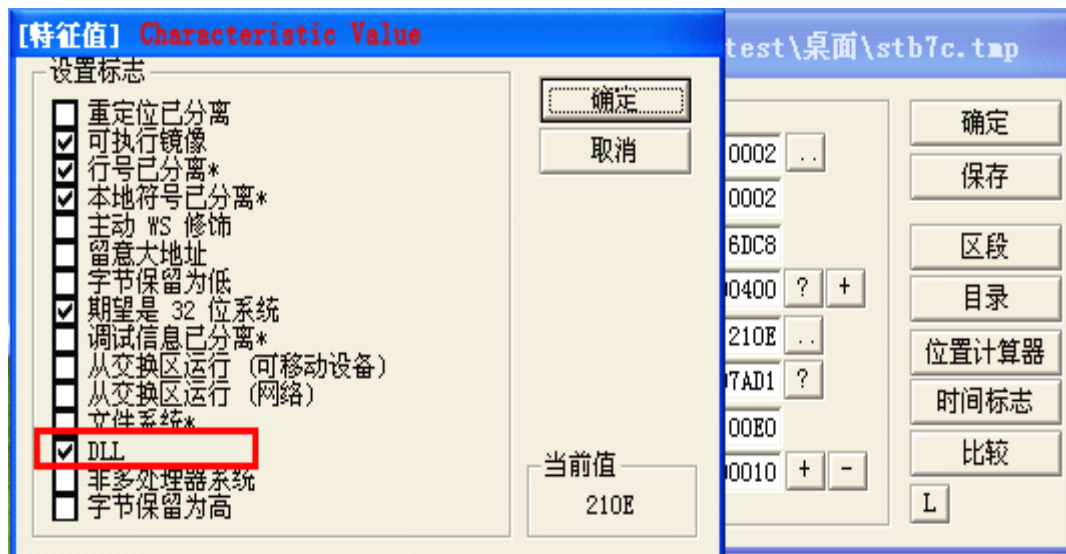


Figure 17

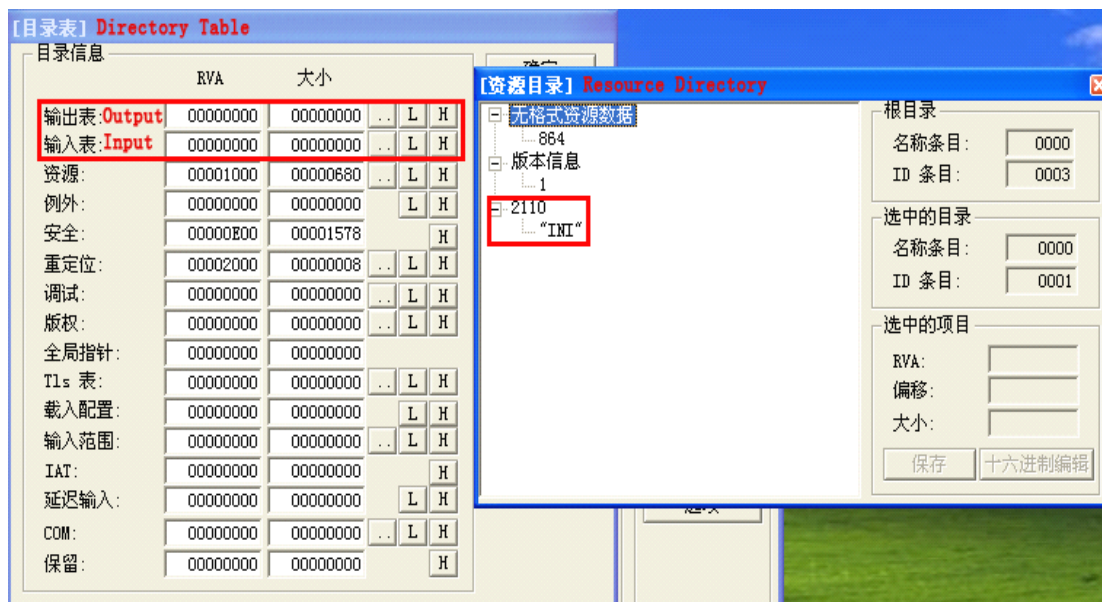


Figure 18

To understand the actual file type of STB7C.tmp file, we changed the name of this file to STB7C.dll, and checked its attributes, we saw that the description of the file is "360 Secure Browser Secure Online Bank", with product name of DataDll (Figure 19).



Figure 19

Operate Restorator 2007, unfold STBC7.dll file, and check up INI resource contents under 2110 resource type, and the content of it is encoded by the method of BASE64 (Figure 20).

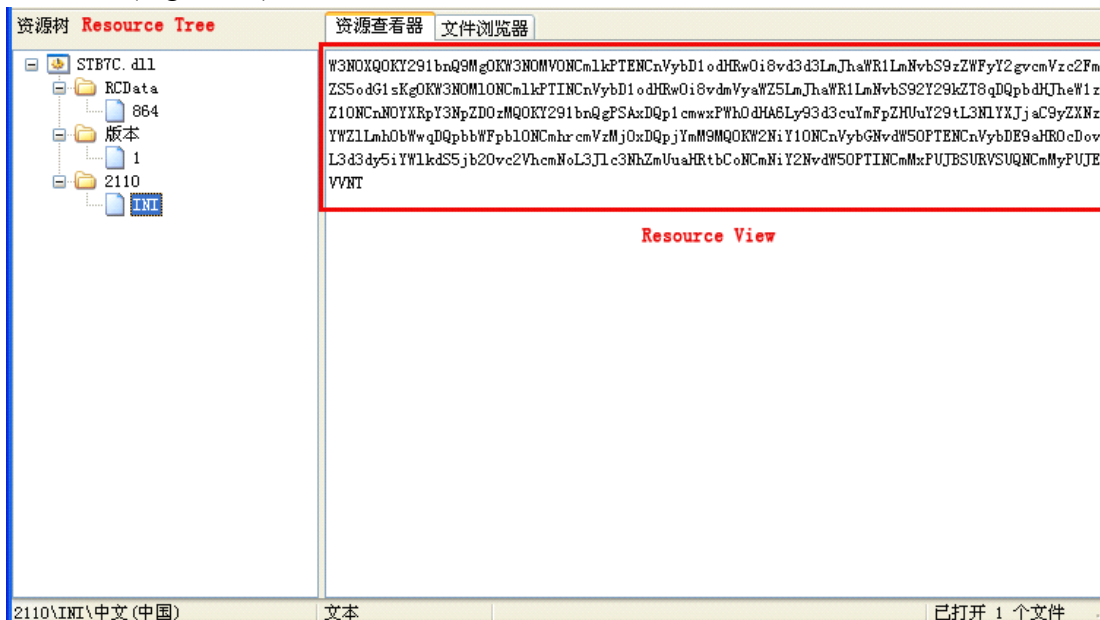


Figure 20

Unfold online BASE64 decoding page <http://www.mxzc.net/>, conduct BASE64 decoding of the code of INI resource in STBC7.dll file (Figure 21).



Base64

```

W3NOXQOKY291bnQ9MgOKW3NOMVONCm1kPTENCnVybD1odHRwOi8vd3d3LmJhaWR1LmNvbS9zZWZyY2gvcmVzc2FmZS5odG1sKgOKW3NOML0
NCm1kPTINCnVybD1odHRwOi8vdnVyaWZ5LmJhaWR1LmNvbS92Y29kZT8qdQpbdHJheW1zZ10NCnNOYXRpY3NpZD0zMOKY291bnQpSAXDQ
p1cmwxPWh0dHA6Ly93d3cuYmFpZHUuY29tL3NlYXJjY29yZkZkZmVzc2FmZS5odG1sKgOKW3NOMVONCm1kPTINCnVybD1odHRwOi8vd3d3LmJhaWR1LmNvbS9zZWZyY2gvcmVzc2FmZS5odG1sKgOKW3NOML0
SUQNcmMyPUJEVWNT
  
```

UTF-8
 简体中文(GB2312)
 繁体中文(BIG5)
 日语(EUC-JP)
 朝鲜语(EUC-KR)

UTF-8

```

[st]
count=2
[st1]
id=1
url=http://www.baidu.com/search/ressafe.html*
[st2]
id=2
url=http://verify.baidu.com/vcode?*
[traymsg]
staticsid=31
count = 1
url1=http://www.baidu.com/search/ressafe.html*
[main]
  
```

中文(简体)
 字数限制1000字

Figure 21

The result of the above BASE64 decoding as follows:

```

[st]
count=2
[st1]
id=1
url=http://www.baidu.com/search/ressafe.html*
[st2]
id=2
url=http://verify.baidu.com/vcode?*
[traymsg]
staticsid=31
count = 1
url1=http://www.baidu.com/search/ressafe.html*
[main]
hkres2=1
cbc=1
[cbc]
urlcount=1
url1=http://www.baidu.com/search/ressafe.html*
cbccount=2
c1=BAIDUID
c2=BDUSS
  
```



Seen from here, DLL file requested and obtained by ExtSmartWiz.dll from 360 Server (domain name: se.360.cn) exists no function of itself to threaten the system security and user's information security, but it exists configure file resources, with Baidu—Search Engine as relevant configuration information, moreover, it is not consistent with file description of DLL file. Known from the former decompilation content of ExtSmartWiz.dll, ExtSmartWiz.dll's operation after loading this file is to read its resources, by the read resource file, 360 Secure Browser can execute corresponding operation based on the configuration information.

b. Analysis of the Input Table of ExtSmartWiz.dll File

Continue to use LoadPE to load ExtSmartWiz.dll file, check up the call list of API Interface in the input table (Figure 22 to Figure 25), via checking up API function of the input table, we know the functions of the program include: intercept/conceal of the behavior of the application, thread creation, deletion of file and progress and retrieval of the progress module, operation registry, hook creation and so on.

DLL名称	OriginalFir...	日期时间标志	ForwarderChain	名称	FirstThunk
KERNEL32.dll	00156C2C	00000000	00000000	0015781C	00124100
USER32.dll	00156F44	00000000	00000000	00157C60	00124418
GDI32.dll	00156B80	00000000	00000000	00157F00	00124054
ADVAPI32.dll	00156B2C	00000000	00000000	00157FD0	00124000
SHELL32.dll	00156F04	00000000	00000000	00158008	001243D8

ThunkRVA	Thunk 偏移	Thunk 值	提示	API名称
00124184	00122784	001575A6	023C	GetPrivateProfileIntW
00124188	00122788	00157588	052B	WritePrivateProfileStringW
0012418C	0012278C	00157570	0158	FlushInstructionCache
00124190	00122790	00157564	03C0	ReadFile
00124194	00122794	00158902	02BF	GlobalMemoryStatus
00124198	00122798	001588F4	02A2	GetVersion
0012419C	0012279C	001588DA	0346	LocalFileTimeToFileTime
001241A0	001227A0	001588C8	00DD	DeviceIoControl

Thunk 数: A4h / 164d (FirstThunk chain) 总是查看 FirstThunk (V)

Figure 22

DLL名称	OriginalFir...	日期时间标志	ForwarderChain	名称	FirstThunk
KERNEL32.dll	00156C2C	00000000	00000000	0015781C	00124100
USER32.dll	00156F44	00000000	00000000	00157C60	00124418
GDI32.dll	00156B80	00000000	00000000	00157F00	00124054
ADVAPI32.dll	00156B2C	00000000	00000000	00157FD0	00124000
SHELL32.dll	00156F04	00000000	00000000	00158008	001243D8

ThunkRVA	Thunk 偏移	Thunk 值	提示	API名称
00124418	00122A18	00157BF6	02CF	SetWindowsHookExW
0012441C	00122A1C	0015782A	00AF	DispatchMessageW
00124420	00122A20	0015783E	02FC	TranslateMessage
00124424	00122A24	00157852	0233	PeekMessageW
00124428	00122A28	00157C0A	0300	UnhookWindowsHookEx
0012442C	00122A2C	00157C20	01FA	LoadStringW
00124430	00122A30	00157BE4	001C	CallNextHookEx
00124434	00122A34	00157BD0	0123	GetDesktopWindow

Thunk 数: 49h / 73d (FirstThunk chain) 总是查看 FirstThunk (V)

Figure 23

INTELLIGENCE DEFENSE FRIENDS LABORATORY

IDF实验室

[输入表] Input Table

DLL名称	OriginalFir...	日期时间标志	ForwarderChain	名称	FirstThunk
KERNEL32.dll	00156C2C	00000000	00000000	0015781C	00124100
USER32.dll	00156F44	00000000	00000000	00157C60	00124418
GDI32.dll	00156B80	00000000	00000000	00157F00	00124054
ADVAPI32.dll	00156B2C	00000000	00000000	00157FD0	00124000
SHELL32.dll	00156F04	00000000	00000000	00158008	001243D8

ThunkRVA	Thunk 偏移	Thunk 值	提示	API名称
00124000	00122600	00157F56	0230	RegCloseKey
00124004	00122604	00157F46	0261	RegOpenKeyExW
00124008	00122608	00157F34	0248	RegDeleteValueW
0012400C	0012260C	00157F1E	015A	GetTokenInformation
00124010	00122610	00157F0A	01F7	OpenProcessToken
00124014	00122614	0015898E	00DB	DeregisterEventSource
00124018	00122618	00158976	0283	RegisterEventSourceW
0012401C	0012261C	00158962	026D	RegQueryValueExA

Thunk 数: Fh / 15d (FirstThunk chain) 总是查看 FirstThunk (V)

Figure 24

[输入表] Input Table

DLL名称	OriginalFir...	日期时间标志	ForwarderChain	名称	FirstThunk
WININET.dll	0015707C	00000000	00000000	00158346	00124550
PSAPI.DLL	00156EF4	00000000	00000000	00158390	001243C8
gdiplus.dll	001570C4	00000000	00000000	00158446	00124598
WS2_32.dll	001570B8	00000000	00000000	00158452	0012458C

ThunkRVA	Thunk 偏移	Thunk 值	提示	API名称
001243C8	001229C8	0015836A	0004	EnumProcessModules
001243CC	001229CC	00158380	0006	EnumProcesses
001243D0	001229D0	00158352	0010	GetModuleFileNameExW

Thunk 数: 3h / 3d (FirstThunk chain) 总是查看 FirstThunk (V)

Figure 25

6. Testing Results

In accordance with the above detection result, the attribute, behavior and recompilation content of ExtSmartWiz.dll File of 360 Secure Browser v5.0.8.7 is consistent with the public letter of @独立调查员. Though the call of 360 Secure Browser, this file download DLL file load it from 360 Server without noticing the users, and there is not definite statements or instructions for the use and functions of ExtSmartWiz.dll file.

In accordance with "360 User Privacy White Book" issued by Qihoo 360 company, (<http://www.360.cn/privacy/v2/360anquanliulanqi.html>) The description of "Instruction for 360 Secure Browser on Protection of Users Privacy" (as the following figure):



当您使用360安全浏览器时 360 会收到的信息

When you are using 360 Safe Browser, 360 will receive information:

为了实现相关的“云安全”和其他特色功能，360安全浏览器会向 360云安全中心发送以下限定的信息：

网址云安全 **Cloud Security of URL**

360安全浏览器的安全红绿灯功能会定期与 360 的服务器进行通信，以便下载存在网络欺诈内容和恶意软件网站的最新黑名单列表，以及被360认证的知名网站的白名单列表。如果您访问的网址不在黑白名单列表中，360安全浏览器会发送到360的服务器，和服务端海量的恶意网址库进行比对，来保证更快速的拦截一些最新出现的恶意网址。

下载云安全 **Cloud Security of Download**

当您使用360安全浏览器内置的安全下载器下载文件时，360安全浏览器会先将下载链接发送给 360 的服务器，和服务端海量的恶意下载链的网址库进行比对，一旦发现问题，会立刻终止下载，保证您的电脑安全。

智能地址栏 **Smart address bar**

当您在地址栏中输入网址或查询时，如果在本地历史记录、收藏夹、以及预置的知名网址库中没有匹配的记录，360安全浏览器会将您键入的文字发送给 360。这样，“建议”功能就能自动向您推荐您可能正要查找的字词或网址。

云备份 **Cloud Backup**

如果您登陆并使用了360安全浏览器的云备份功能，在经过明确提示并由您主动选择确认的情况下，360安全浏览器会将您的浏览器配置文件、登录管家中保存的账号、邮件提醒中保存的账号、微博提醒中保存的账号、游戏小帮手中保存的账号、收藏夹信息等用户个性化内容加密备份到 360 服务器上，并与您的360账户相关联。我们需要存储这些信息，以便将这些信息发送到您选择启用360网络账号功能的其他计算机。360会采取严格的技术措施和管理措施来保障您的个人信息安全，您的360账户中存储的信息受360隐私权政策的保护。

自动升级 **Automatic Update**

360安全浏览器会定期与360的服务器进行通信，查询是否有最新可以升级的版本，发现新版本会提示您安装，让您第一时间使用360安全浏览器最新最稳定的版本。

安装卸载 **Install or Uninstall**

当您安装360安全浏览器，或者卸载360安全浏览器时，360安全浏览器会发送您安装或者卸载的浏览器版本号给360，用于统计不同版本的卸载率，帮助我们发现问题；卸载时还会让您填写卸载原因，如果您填写了，相应信息也会收集到360的服务器，用于改进我们的产品。



崩溃报告 **Crash Report**

当您在使用360安全浏览器时出现崩溃或者其他异常，360安全浏览器会在得到您的确认后，将崩溃报告发送给360。崩溃报告可以帮助我们诊断浏览器所出现的问题。360安全浏览器会尽量避免发送用户个人身份识别信息，但是崩溃报告会包含关于故障发生时正在运行的文件、应用程序和服务的信息。

用户体验改进计划 **Customer Experience Improvement Plan**

您在安装360安全浏览器时，我们会邀请您参加用户体验改进计划，您可以选择不参加。如果您参加了这个计划，我们会收集您的浏览器使用情况数据，仅为举例的目的，比如：某个按钮的点击次数、某些关键配置的选项值，我们不会收集您的浏览历史、cookie以及其他涉及您个人的数据。收集到的数据，我们仅以汇总分析的目的使用，以便改进我们的产品。

In this network monitoring, close the functions that can be closed by 360 Security Center, including Cloud Security of the Website, Interception of Advertisement, Second Generation of Anti Feign Death, Protection of Snadbox, under the condition that there is not any operation of the Browser, we ca still grasp the record of ExtSmartWiz.dll’s request of the Server file as well as download the Server file (Figure 26). This shows that ExtSmartWiz.dll’s data request and receive is not contained in “Instruction for 360 Secure Browser’s Protection of Privacy” in “360’s User Privacy Protection White Book”.

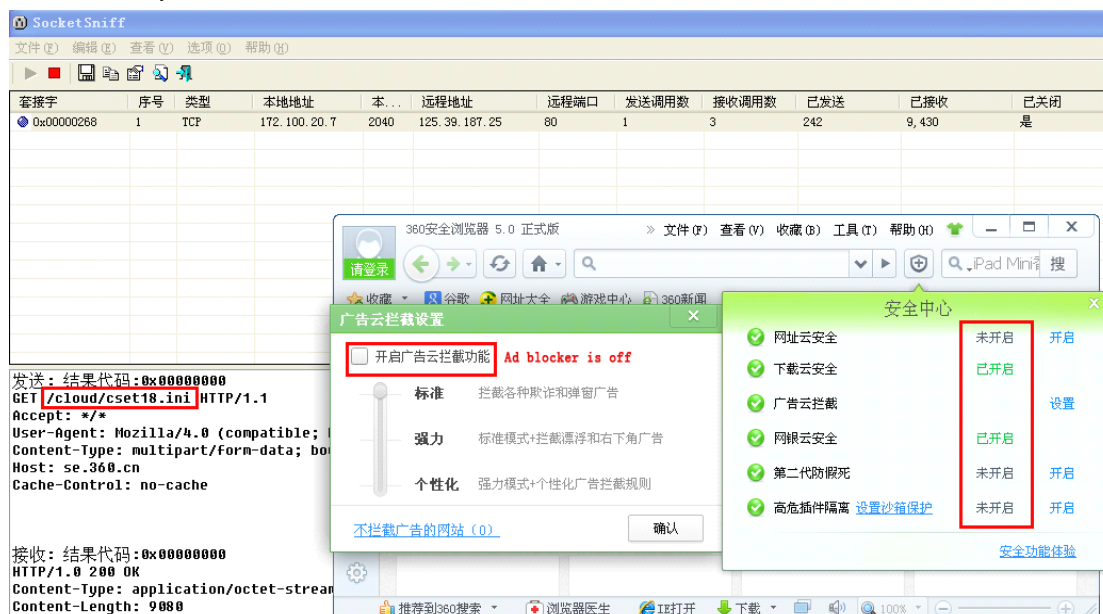


Figure 26

The “Privacy Protection” (as the following figure) in Article 4.9 of “360 Browser Installation Permission Agreement” (<http://www.360.cn/xukexieyi.html>) is included in the “Instruction for 360 Secure Browser’s Protection of Users Privacy” of “360’s Protection of Users Privacy White Book”, therefore the ExtSmartWiz.dll file of 360 Secure Browser also fails to observe “360 Browser Installation Permission Agreement”.



4.9 隐私权保护

4.9.1为了更好地改进软件和服务，当用户安装或者卸载本软件时，本软件会发送用户安装或者卸载的浏览器版本号给奇虎360服务器，用于统计不同本软件版本的卸载率，帮助我们发现问题；卸载本软件时还会让用户填写卸载原因，如果用户选择填写，相应信息也会收集到360的服务器，用于改进我们的产品。

4.9.2帐号加密：用户保存在本地计算机上的微博账号、邮箱账号、人人网账号、登录管家帐号等所有的帐号，都采用本地特征码、AES256、混淆运算等安全加密技术，以最大程度保障这些帐号安全性。

4.9.3网址云安全：本软件的安全红绿灯功能会定期与奇虎360的服务器进行通信，以便下载存在网络欺诈内容和恶意软件网站的最新黑名单列表和被奇虎360认证的知名网站的白名单列表。如果用户访问的网址不在黑白名单列表中，本软件会发送到奇虎360的服务器和服务端海量的恶意网址库进行比对，来保证更快速的拦截一些最新出现的恶意网址。

4.9.4下载云安全：当用户使用本软件内置的安全下载器下载文件时，本软件会先将下载链接发送给奇虎360的服务器和服务端海量的恶意下载链的网址库进行比对，一旦发现问题，会立刻终止下载，保证用户的电脑安全。

4.9.5“无痕浏览”功能，限制本软件在用户的计算机上保存信息。使用无痕浏览功能本软件将不会存储浏览历史记录，也不会记录到地址栏下拉列表中，最近关闭的标签列表和关闭窗口时的未关闭标签列表中都不会有任何痕迹。当用户退出无痕浏览时，本软件会从用户的计算机中删除无痕浏览时收到的新Cookie，以及访问网站时留下的临时文件。在“无痕浏览”时通过内置安全下载器下载的文件记录，以及对浏览器配置的修改仍然会被保存下来。

4.9.6网络收藏夹功能：如果用户登陆并使用了本软件的网络收藏夹功能，本软件会将您的浏览器配置文件和收藏夹数据存储到奇虎360服务器上，并与用户的360帐户相关联。奇虎360存储这些信息，是为了方便用户将这些信息发送到用户选择启用360网络收藏夹功能的其他计算机上。用户360帐户中存储的信息受360隐私权政策的保护。

4.9.7云备份：如果用户开启了云备份功能，用户在360帐号下所保存在本地计算机的用户在第三方网站的帐号信息将会被加密备份到奇虎360云端服务器，并且与用户的360帐号相关联。包括登录管家中的第三方网站的用户名和密码、邮件提醒功能中的邮箱用户名和密码、游戏助手保存的游戏帐号和密码、微博提醒功能中保存的微博帐号和密码。备份帐号信息，可以方便用户将这些信息发送到启用本软件的其他计算机上，用户可以在不同的计算机上通过登录360帐号来使用这些帐号进行登录。奇虎360会采取严格的技术措施和管理措施来保障您的个人信息安全。您360帐号中存储的信息受隐私权政策的保护。

4.9.8本软件会在用户的计算机上记录有关浏览历史记录的实用信息。这些信息包括：浏览历史记录、用户访问过的大部分网页的的屏幕截图（缩略图大小）、Cookie或网络存储数据（由用户所访问的网站存放在用户的计算机上）、访问网站时留下的临时文件、地址栏下拉列表、最近关闭的标签列表、关闭窗口时的未关闭标签列表、使用内置安全下载器的下载记录。用户可以通过“工具”菜单中的“清除浏览器记录”，随时将以上历史记录的全部信息或部分信息删除。

4.9.9程序错误日志上报：当用户在使用本软件时出现崩溃或者其他异常，本软件会在得到用户的确认后，将崩溃报告发送给360。崩溃报告可以帮助我们诊断浏览器所出现的问题。本软件会尽量避免发送用户个人身份识别信息，但是崩溃报告会包含关于故障发生时正在运行的文件、应用程序和服务的信息。

4.9.10用户体验改进计划：用户在安装本软件时，我们会邀请用户参加用户体验改进计划，用户可以选择不参加。如果用户参加了这个计划，我们会发送一些用户的浏览器使用情况数据（比如：某个按钮的点击次数、某些关键配置的选项值）到360，但绝不会发送用户的浏览历史、cookie等隐私数据。收集到的数据，我们会进行汇总分析，以便改进我们的产品。



4.9.11奇虎360制定了严格的用户上传信息处理规则和安全保护措施来确保不超越目的和范围收集用户信息，确保用户上传信息的安全，确保用户上传信息不被滥用。除征得用户明确同意和法律明确规定外，奇虎360不会向任何第三方提供用户上传文件及信息。

4.9.12奇虎360制定了以下四项隐私权保护原则，指导我们如何来处理产品中涉及到用户隐私权和用户信息等方面的问题：

- (1) 利用我们收集的信息为用户提供有价值的产品和服务。
- (2) 开发符合隐私权标准和隐私权惯例的产品。
- (3) 将个人信息的收集透明化，并由权威第三方监督。
- (4) 尽最大的努力保护我们掌握的信息。

您可通过奇虎360安全中心网站查看我们有关隐私保护的详细内容，网址为：
<http://www.360.cn/privacy/index.html>

Special:

The detection of report bases on Qihoo 360 Safe Guard v7.3.0.20031. Welcome enthusiasts and friends detect 360 Safe Guard of this version according to this report by self, including 360 Safe Guard of other version. We hope Qihoo could give an satisfactory reply to every net friends with an open attitude. Welcome your criticism and correction. We sincerely welcome friends from relevant fields, including Qihoo to work together to carry out transparent, professional exchanges and dialogue, and work together to promote the Internet security industry for creating a healthy and good, reliable Internet environment of China.

7. Appendix I

7.1. Comparing with the Technical Analysis by @独立调查员

According to the detection items of ExtSmartWiz.dll file under the installation path of 360 Secure Browser in the public letter leased by @独立调查员, and the detection items for this file by IDF laboratory, the correlation is as follows:

Detection Item \ Detection Side	@独立调查员	@IDF Laboratory
Monitoring of the Function of the File	√	√
Monitoring of File Operation	×	√
Monitoring of WinSock Expert	×	√
IE Browser Correlation Monitoring	×	√
Detection of Decompilation of the File	√	√
Detection of the Content of STB*.tmp	×	√



File		
Detection of the Input List of the File	×	√
Detection and Demonstration of the File 's Threat	×	×

Detection Correlation Table (√: Yes; ×: No)

7.2. “Public Letter to MITT and the Ministry of Public Security for Public whistle-blowing of Qihoo 360”

The original text came from @独立调查员 in Sina blog (http://blog.sina.com.cn/s/blog_ad048dc101017amd.html). The comments in the original text do not represent the view of IDF Laboratory.



公开举报奇虎360公司——致工信部、公安部公开信 (2012-10-29 12:58:32)

[+ 转载](#) ▾

标签：杂谈

工信部、公安部：

奇虎360公司的“360安全浏览器”暗藏“后门”，是用户系统安全和信息安全的严重潜在威胁，是其竞争对手产品体验和服务体验的严重潜在威胁。“360安全浏览器”暗藏“后门”暴露后一再狡辩、诬赖本人是“枪手”、在“造谣”，企图糊弄公众、蒙混过关。

据称工信部正在调查奇虎360公司，调查对象是奇虎360公司提供的“浏览器样本”。请问工信部，世界上有这样的“调查”吗？你们不要太离谱，世界不只是你们的。在互联网时代，公权力的权威和威信已不可能自证，调查规则与过程必须接受公众严格检验，工信部调查组自行抽查“样本”是底线，否则就别演戏了——看你们演戏不如看苍井空。

本人建议公安部介入，与工信部联合调查。

现向工信部、公安部公开举报互联网秩序的恶意破坏者——奇虎360公司，并提供指令级证据。

是的，本人仍将匿名，仅用事实说话。

部分网友可能看不懂，没关系，请毫不犹豫转发、广播，全国“通缉”奇虎360公司，全部可能的法律责任由本人承担。

工信部、公安部如需进一步的证据或说明，请通过深圳市公安局找到本人，其他人免谈。

举报内容如下：

一、“360安全浏览器”实为C/S架构木马系统的客户端，服务器群是se.360.cn(云架构，IP地址不定)。浏览器每隔5分钟即自动向服务器请求新的“指示”，新的指示伪装成Ini(纯文本文件类型)发出，实际上是Dll文件(Windows可执行程序库或资源库)。

二、“360安全浏览器”“后门”程序文件是%AppData%\360SE\Apps\ExtSmartWiz\ExtSmartWiz.dll。其中%AppData%在WindowsXP下是C:\Documents and Settings\用户名\Application Data\，在Windows7下是C:\Users\用户名\AppData\Roaming\。这是系统隐藏的数据文件夹。

三、ExtSmartWiz.dll的加载者是“360安全浏览器”安装路径下的pluginbar.dll，可配置，配置文件是%AppData%\360SE\Apps\Appslocal.ini。



四、“扩展中心”见不到该组件，用户不知道它的存在，即使看到文件也不知道其用途。现提供禁用方法：首先进入文件管理选项设置“隐藏文件夹可见”，然后进入所在文件夹删除文件ExtSmartWiz.dll，或删除配置文件Applocal.ini中的部分内容“[ExtSmartWiz]AppItem=1,0,ExtSmartWiz,ExtSmartWiz,9,1,8,0”，或删除pluginbar.dll禁用所有扩展功能。请还在使用“360安全浏览器”的网友务必根据上述方法删除或禁用。

五、ExtSmartWiz.dll内部流程(局部；sub_XXXXXXXX后面的数字是相应函数入口地址)：

1. 加载初始化时设置定时器

```
public Ext_Init
call sub_100B44B0
push 493E0h // 16进制 0x493E0 = 300000毫秒 = 5分钟
...
call eax // =sub_100BB970
call ds:SetTimer // 设置定时器，触发间隔固定5分钟
```

2. 请求服务器提供新的程序指令与/或配置数据

```
sub_100B4A90
call sub_100B4DB0
call sub_100B4EF0
push edx; int
push offset sub_100B4F90; int
push eax; wchar_t *
...
call sub_100C23C0 // 设置处理函数(=sub_100B4F90)，数据区地址
call sub_100C2800
call sub_100C2D90 // 从服务器se.360.cn下载伪装为Ini文本的Dll文件
call ds:InternetOpenW
... // 下载过程
call ds:InternetCloseHandle
```

3. 执行程序指令与/或应用配置参数，并销毁证据

```
sub_100B4F90
call sub_100B8500 // 生成以 STB 为前缀的临时文件名：STBxxx.tmp
call ds:CreateFileW // 临时存储Dll文件
call ds:WriteFile
call ds:CloseHandle
call sub_100B4DD0
call sub_100B8970
call ds:LoadLibraryW // 加载Dll并调用其入口函数DllEntryPoint(用户从这里开始成了木马被控端——肉鸡)
call ds:LoadResource // 加载并分析Dll中的配置数据，这些数据控制浏览器预置的可编程行为
call ds:FreeResource
call ds:FreeLibraryW
call ds>DeleteFileW // 删除临时文件，销毁证据
```

六、ExtSmartWiz.dll内部流程的白话翻译：“360总部，请指示！”“A计划！”“收到！A计划执行完毕！证据销毁完毕！”……(睡眠5分钟)……“360总部，请指示！”“B计划！”“收到！B计划执行完毕！证据销毁完毕！”……(睡眠5分钟)……“360总部，请指示！”“C计划！”“收到！C计划执行完毕！证据销毁完毕！”……(睡眠5分钟)……

七、反向分析版本是5.0.8.4，ExtSmartWiz.dll文件签名时间戳是“2012年10月3日 21:28:50”。

八、截至目前，本人已捕获3种“指示”，其中2种资源库(配置数据，干扰百度等竞争对手网站运行)、1种可执行程序库。本人已对后者做初步分析，该程序库仅一个加载即被自动调用的入口DllEntryPoint，无其它可编程接口(API)，代码量超过9000，其函数流程见本文附图(仅框架，暂不提供详图)，欢迎工信部、公安部取证。



九、做为社会一分子，本人已经超额承担义务，现在请工信部、公安部的同志们切实负起责任，尽快查封奇虎360公司代码管理服务器，全面检查10月3日前的最新基线版本。你们的调查报告内容必须比本人知道和披露的更多，否则就是失职，部长应该鞠躬下台。

十、再次要求中国信息安全测评中心公开奇虎360公司所谓“代码托管”细节，包括但不限于其托管范围(核心还是全部)、托管更新周期(实时跟进还是一次性)、托管申请审查流程(是否完整审查及测试)等。

8. Appendix II

8.1. Revision History

Version	Revised Contents	Revision Date	Record	Notes
1.0	Create Document	2012/11/4	Create Document	" <i>Public whistle-blowing of Qihoo 360---Public Letter to MIIT and the Ministry of Public Security</i> "
1.1	Re-typesetting, and add the detection result	2012/11/8	Revise the Document	
1.2	Add 360 White Book, the Correlation of Permission Agreement and Detection Result	2012/11/20	Revise the Document	Refer to "Investigation Process of Privacy Invasion"
1.3	Revise the wording and sentence of the detection result	2012/11/21	Revise the Document	
1.4	Add the analysis on STB*.tmp File Resource	2012/11/23	Revise the Document	Refer to " <i>Technical Research Report on the Risk of Disclosure of Individual Privacy</i> "

8.2. Acknowledgement

We received the review and reference views from multiple technicians, security experts and consultants from the Security Industry during the composition of this report, based on their suggestions and advices, the report has been revised and perfected continuously.

We want to thank @做个好人, @lylspector, @渥村万涛, @黑客老鹰 for their suggestions, advices and assistance during the tetsing and the writing of this report. We also want to thank other people who provided comments and suggestions on this work. Without their help, this report will not be possible.