Trojan.Win32/Spy.Ranbyus

Archived: 2026-04-05 20:22:21 UTC

Received a mail with an interesting exe
https://www.virustotal.com/file/17a3ee51492b9b2ba155f54be61f2c305b090cee8d604d1df616ca3ba881b372/analysis/135904965
Thanks creep.
This bot is used by one group of Russian carders and is not for sale, they call it 'triton'

IDA Map file imported to Olly, without IDA i got huge problem to understand the exe:

```
0100A65C | DEC ESI                                          | check_for_avp
0100A687 | MOVZX ECX,BYTE PTR DS:[ESI+2]                    | loc_40A687
0100A68D | OR BYTE PTR DS:[EBX],CL                          | check_for_eset_nod
0100A6BB | JLE SHORT 0000A697                               | loc_40A6BB
0100A6D1 | PUSH DWORD PTR SS:[ESP+14]                       | loc_40A6D1
0100A6D8 | CALL 0100A556                                    | check_for_avg
0100A706 | MOV EDX,E800498D                                 | loc_40A706
0100A71C | ADD BYTE PTR DS:[ECX],AL                         | loc_40A71C
0100A723 | CMPS BYTE PTR DS:[ESI],BYTE PTR ES:[EDI          | check_for_avira
0100A791 | STC                                              | loc_40A791
0100A7A7 | INC EAX                                          | loc_40A7A7
0100A7AE | ADD DWORD PTR DS:[ECX],EAX                       | check_for_avast
0100A7FD | JE 0100A8DB                                      | loc_40A7FD
0100A819 | JGE SHORT 0100A79E                               | loc_40A819
0100A837 | MOV DWORD PTR DS:[ECX+EBP*4],EDI                 | loc_40A837
0100A851 | ADD BYTE PTR DS:[EAX],AL                         | loc_40A851
0100A852 | ADD BYTE PTR DS:[EAX],AL                         | loc_40A852
0100A859 | CMP CL,4B                                        | check_for_norton
0100A8A7 | INC DWORD PTR SS:[EBP+FF157SFF]                  | loc_40A8A7
0100A8BD | JE SHORT 0100A8C1                                | loc_40A8BD
0100A8C4 | ADD DWORD PTR DS:[EDI],ECX                       | check_for_mcafee
0100A912 | CMP ESI,DWORD PTR SS:[EBP+C]                     | loc_40A912
0100A928 | DD 1.0100A881                                    | loc_40A928
0100A92F | ADD DWORD PTR DS:[EBX-58],EAX                    | check_for_panda
0100A95E | DB 05                                            | loc_40A95E
0100A964 | DB 00                                            | check_for_comodo
0100A992 | XOR BL,CH                                        | loc_40A992
0100A9A8 | POP EBP                                          | loc_40A9A8
0100A9AF | INTO                                             | check_for_drweb
0100A9DE | CMP DWORD PTR SS:[ESP+10],EAX                    | loc_40A9DE
0100A9E4 | PUSH DWORD PTR SS:[ESP+10]                       | enumerate_processes
0100AA01 | INC ESI                                          | _notify_server_about_installed_av
```

Injects:

```
01007AB7 | SHR CL,0D4                                       | inject_firefox
01007AF5 | INC ESI                                          | inject_BBClient
01007B28 | MOV WORD PTR DS:[ESI+16],AX                      | inject_ContactNG
01007B61 | JE SHORT 01007B8D                                | uninstall_itself
01007B92 | POP EBP                                          | inject_javaw
01007BB9 | PUSH 23                                          | loc_407BB9
01007BF3 | MOV DWORD PTR DS:[ESI+F],EAX                     | inject_info
01007C28 | DEC ESI                                          | loc_407C28
01007C2D | XCHG EAX,ESP                                     | loc_407C2D
01007C43 | ADD EAX,DWORD PTR DS:[EAX]                       | sub_407C43
01007C69 | ???                                              | loc_407C69
01007C6B | PUSH EDI                                         | loc_407C6B
01007C90 | INC EDI                                          | loc_407C90
01007C9D | INT 89                                           | sub_407C9D
01007CE1 | INC EBP                                          | loc_407CE1
01007CED | ADD DWORD PTR DS:[EAX],7                         | inject_cbmain
01007D23 | XCHG DWORD PTR DS:[EDI+4],EBX                    | inject_webmoney
01007D59 | JNZ 01008187                                     | inject_wcInt_rclient_ipclient
01007D97 | ADD EAX,0F023883                                 | inject_browser
01007DD7 | CALL DWORD PTR DS:[EAX+2B0]                      | loc_407DD7
01007DED | ADD EAX,3959036A                                 | inject_putty
01007E28 | CMP DWORD PTR DS:[ECX],EAX                       | inject_java
01007E4F | OR EDI,EDI                                       | loc_407E4F
01007E95 | OR EDI,EDI                                       | sub_407E95
01007EA8 | OR EAX,DWORD PTR DS:[EDX]                        | loc_407EA8
01007EAB | CALL DWORD PTR DS:[EAX+2B4]                      | inject_UniStream
01007EE1 | SUB AL,1                                         | inject_tiny
01007F17 | INC ESP                                          | start_install_thread
01007F2A | ADD EAX,DWORD PTR DS:[EAX]                       | inject_translink
01007F60 | ADD BYTE PTR DS:[EAX],AL                         | main_as_not_injected
```

Decoded strings (some, not everything):

&pp=1
reg add "
&files=1

nabagent.exe
putty.exe
[MOUSE R %dx%d]
POST
SeShutdownPrivilege
UniStream.exe
cbsmain.exe
HKLM\
jawt.dll
&net=1
disk%u.xml
&scrn=1
&cmd=1
UZ.DB3
GET
iexplore.exe
ThunderRT6FormDC
com.bifit.harver.core.DocumentBrowserFrame
drweb.exe
nabwatcher.exe
WINNT
bc_loader.exe
avfwsvc.exe
[VK_END]
.iBank*
aswupdsv.exe
%s\tmp%xa%04d.$$$
\/servlets\/ibc
bclient.exe
EnableLUA
secring
client7.exe
Western Union® Translink™
Tiny Client-Bank
/bsi.dll
Content-type: multipart/form-data, boundary=%s
Edit
java.exe
sign.key
\\.\PhysicalDrive0
inbank-start-ff.exe
http://([^:/]+):*([^/]*)(.+)
Content-Disposition: form-data; name="data"; filename="1"
clbank.exe
BBClient.exe
WS2_32.DLL
ComSpec

iscc.exe
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
avengine.exe
https:\/\/ibank.alfabank.ru
WebMoney Keeper Classic » Âõîä
a:\keys.dat
https:\/\/ibank.prbb.ru
oncbcli.exe
logs
nortonantibot.exe
ContactNG.exe
BUTTON
wclnt.exe
ashwebsv.exe
mj=%u&mi=%u&pt=%u&b=%u&dc=%u
sgbclient.exe
cbsmain.dll
avmailc.exe
Software\Microsoft\Windows NT\CurrentVersion\
winlogon.exe
webmoney.exe
egui.exe
/c del
--%s--
auth-attr-\d+-param1=.*&auth-attr-\d+-param2=.*
intpro.exe
vshwin32.exe
firefox.exe
mcshield.exe
Password:
nabmonitor.exe
UNIStream®. Àóòåíòèôèêàöèÿ.
Software\Microsoft\Windows\CurrentVersion\Policies\System
&file=2
http://e71koapi.org/lc5dx/index.php
rclient.exe
.jks
cfp.exe
translink.exe
http://pulden376-seven3.in/doEst71beG/index.php

Content-Transfer-Encoding: binary
ntvdm.exe
SysDebug32
%s?id=%s&session=%u&v=%u&name=%s
&av=

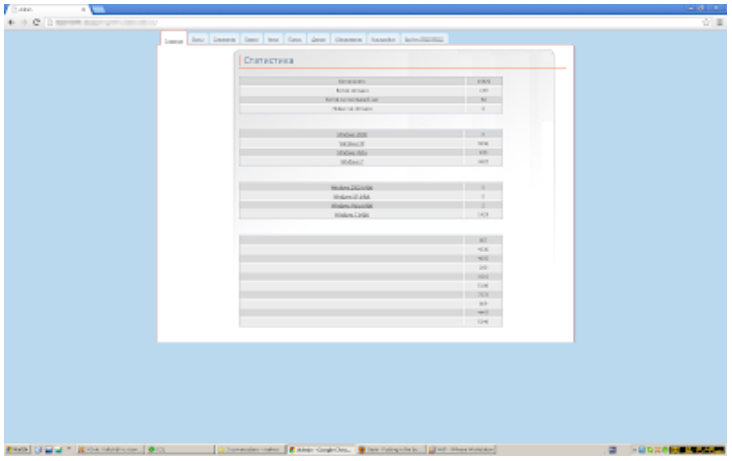
avp.exe
System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
cmdagent.exe
WINSCARD.DLL
" /v EnableLUA /t REG_DWORD /d 0 /f
bankcl.exe
Software\Microsoft\Windows\CurrentVersion
safari.exe
avconsol.exe
elbank.exe
username=.*&password=.*
pubring=(.*)
javax.swing.JFrame
secring=(.*)
javaw.exe
ISClient.exe
JVM.DLL
bk.exe
http://([^:/]+)/.+
auth-attr-\d+-param1=(.*)&auth-attr-\d+-param2=([^&]*)
ekrn.exe
sched.exe
avgnt.exe
avwebgrd.exe
startclient7.exe
master.key
avsynmgr.exe
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Aleksandr Matrosov know better than me this threat go have a look his article: http://blog.eset.com/2012/12/19/win32spy-ranbyus-modifying-java-code-in-rbs

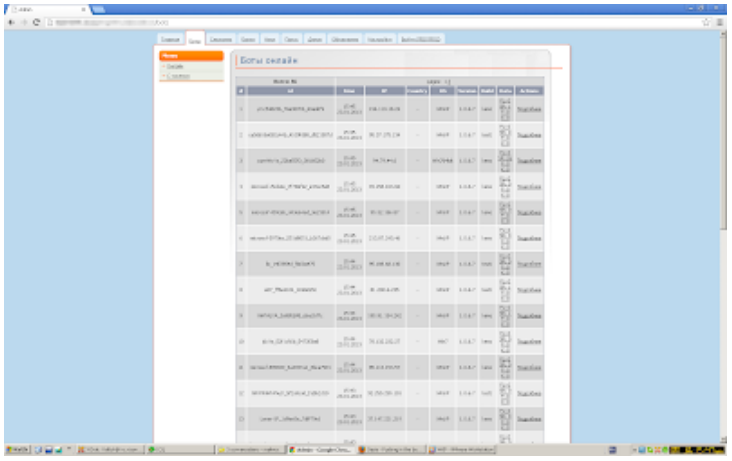
Let's do directly to the panel...

Login:

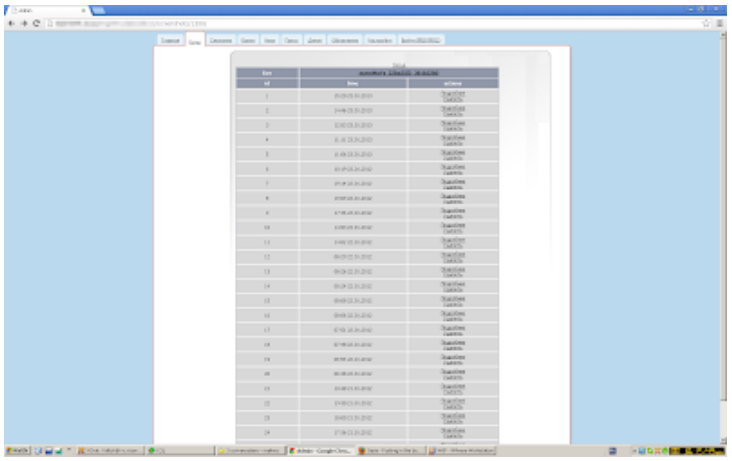
Statistics:



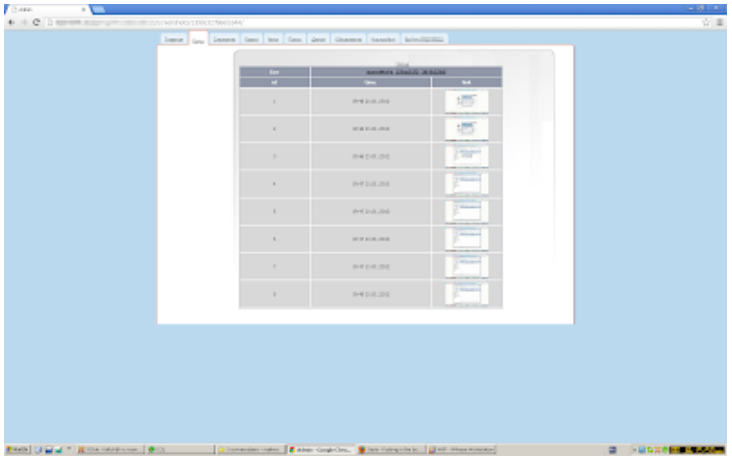
Active bots with smartcard:



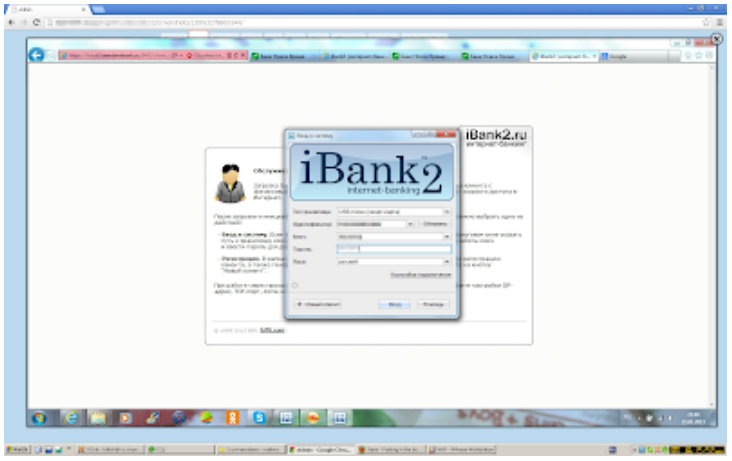
Screenshots (SR):



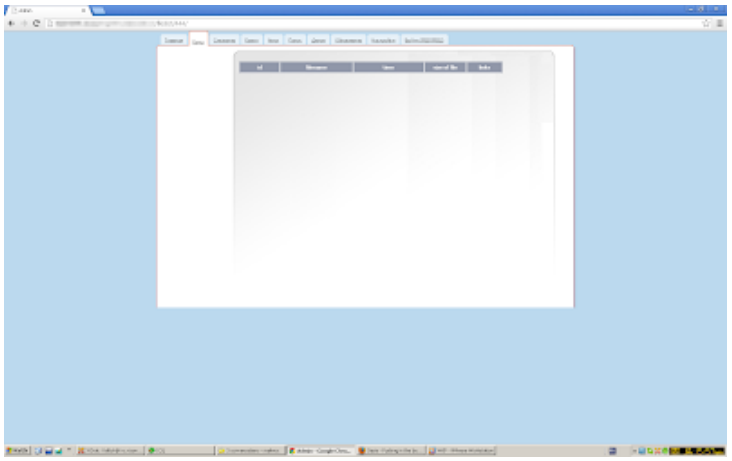
Clicking on a random day:



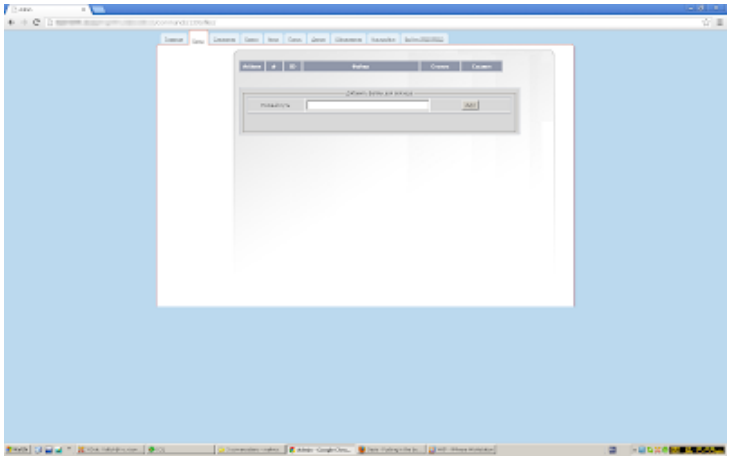
A screenshot took by the bot:



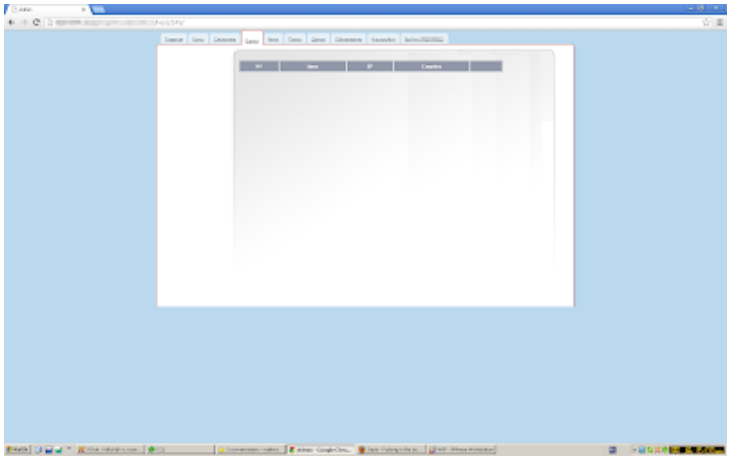
Filelist (FL):



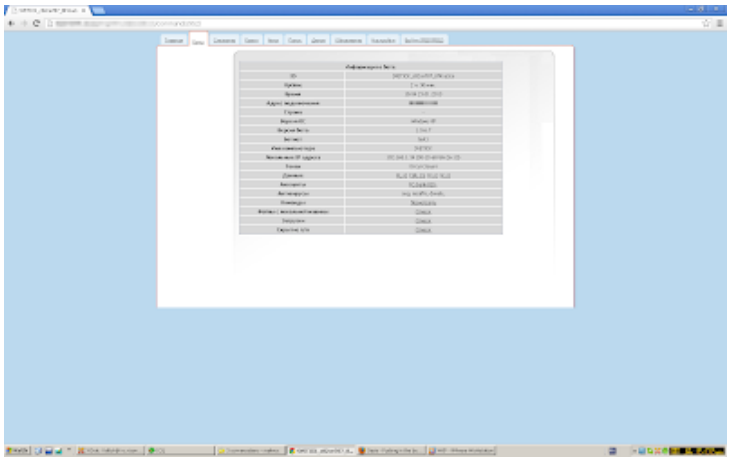
File (F):



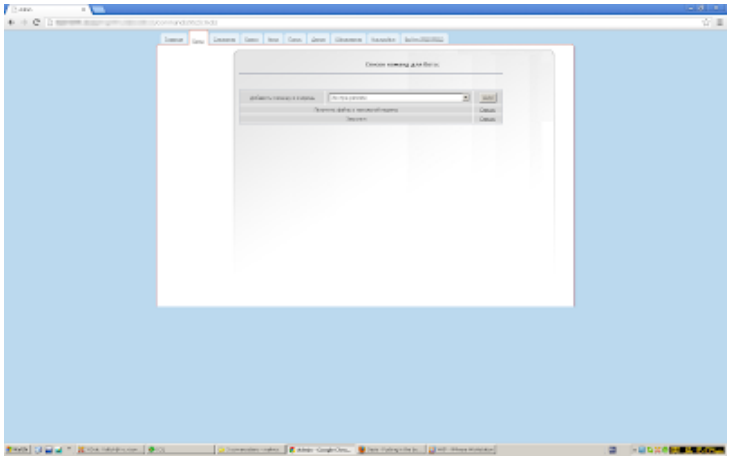
Keys (K):

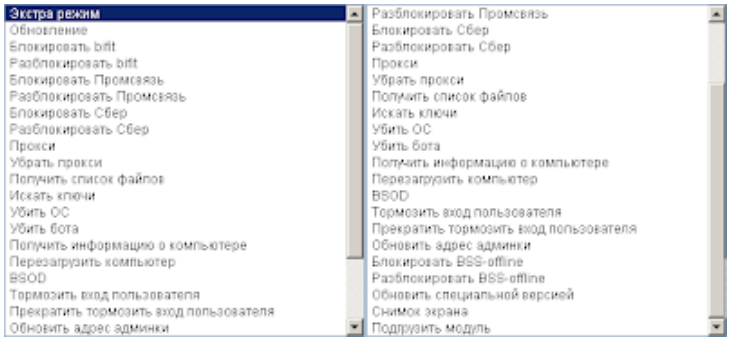


Bot informations:

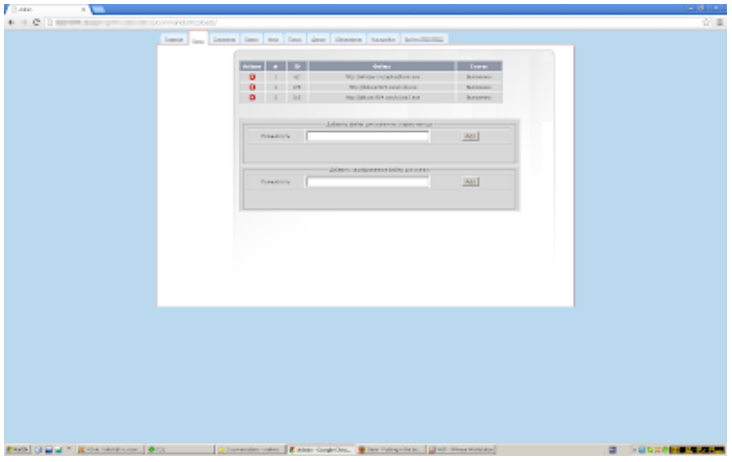


Orders to send:





Download list:



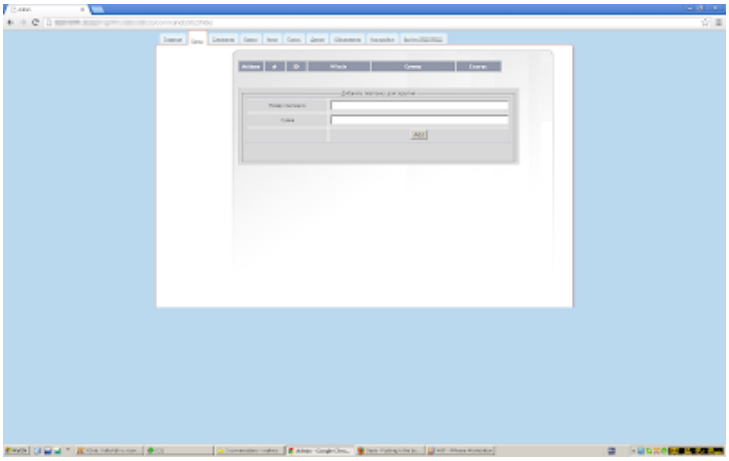
Some task urls:

hxxp://whispers.ru/upload/term.exe
hxxp://178.18.249.11/cono.exe
hxxp://hoombauls.com/cono.exe
hxxp://deluxe1924.com/cc/d.exe
hxxp://deluxe1924.com/cc/car2.exe
hxxp://hoombauls.com/cono.exe
hxxp://gramma.pro/update.exe
hxxp://girgrozn.narod2.ru/01/CONO.exe
hxxp://deluxe1924.com/cc/picpic.exe
hxxp://gramma.pro/update.exe

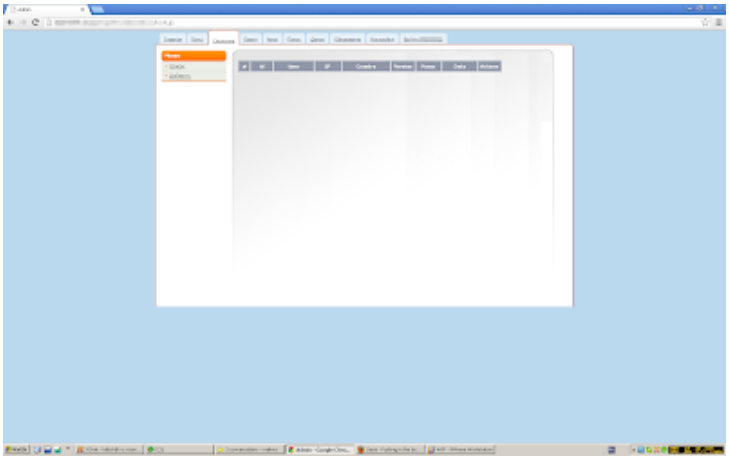
hxxp://deluxe1924.com/cc/fun2101.exe
hxxp://www.mobi-sys.ru/en/lox.exe
hxxp://likeme.pro/update.exe
hxxp://ejdovberk.org/MRD.exe
hxxp://www.enmtp.com/admin/lunt30.exe
hxxp://178.18.249.10/exel.exe
hxxp://deluxe1924.com/cc/picpic.exe
hxxp://orlik.pro/update1.exe
hxxp://whispers.ru/upload/MLN1.exe
hxxp://www.enmtp.com/admin/termclean.exe
hxxp://www.enmtp.com/admin/IMRD.exe

Some files can be found here: http://vxvault.siri-urz.net/ViriList.php?IP=209.61.202.242

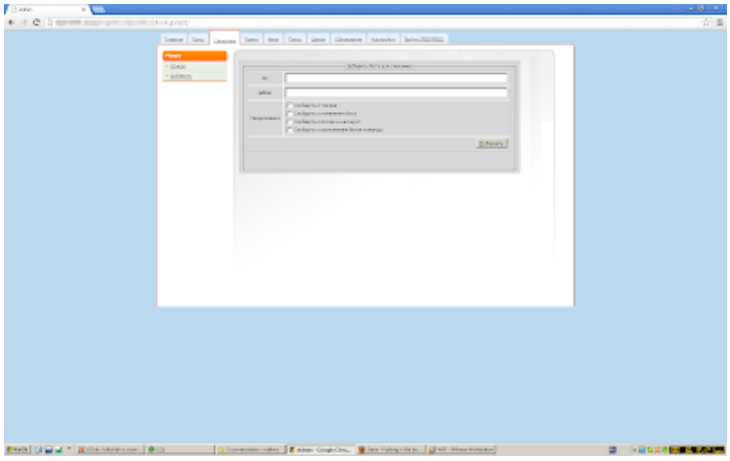
Hide:



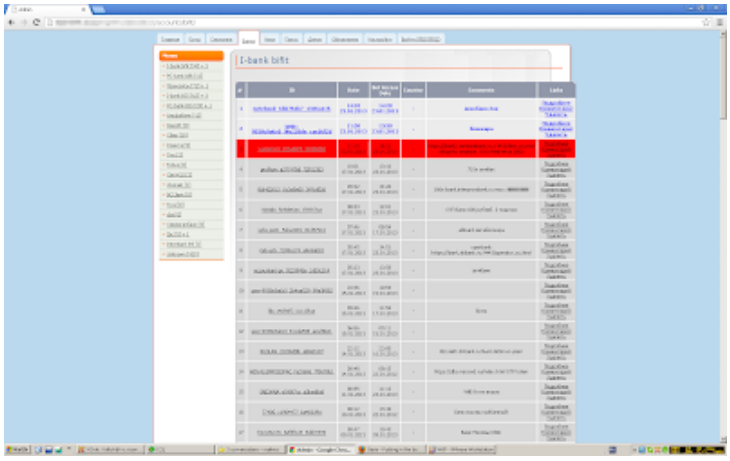
Lookup:



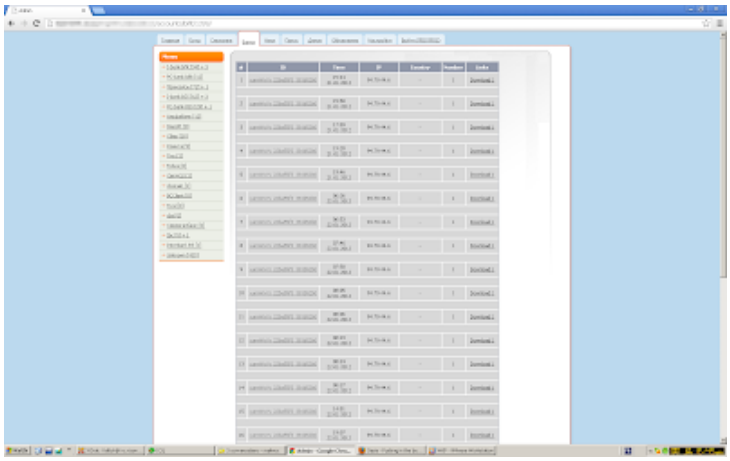
add:



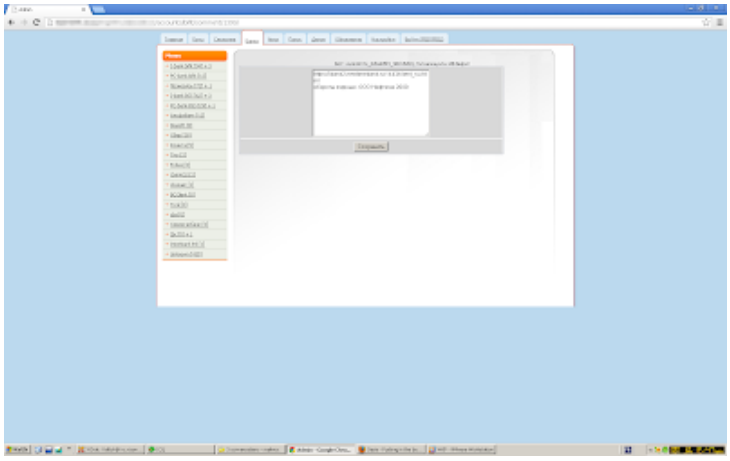
Banks:



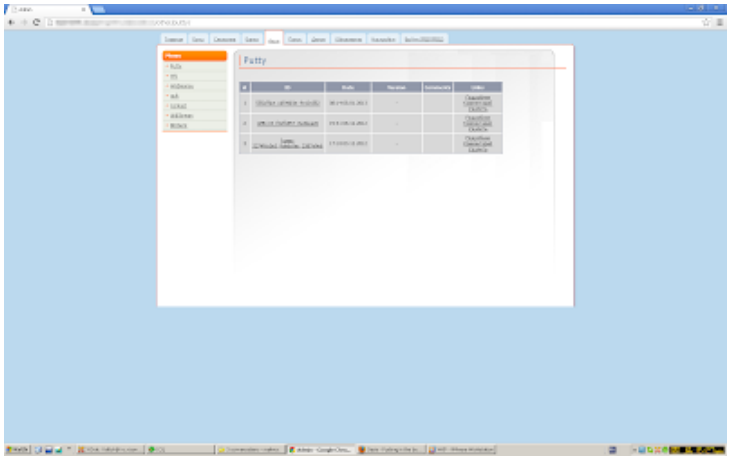
Download:



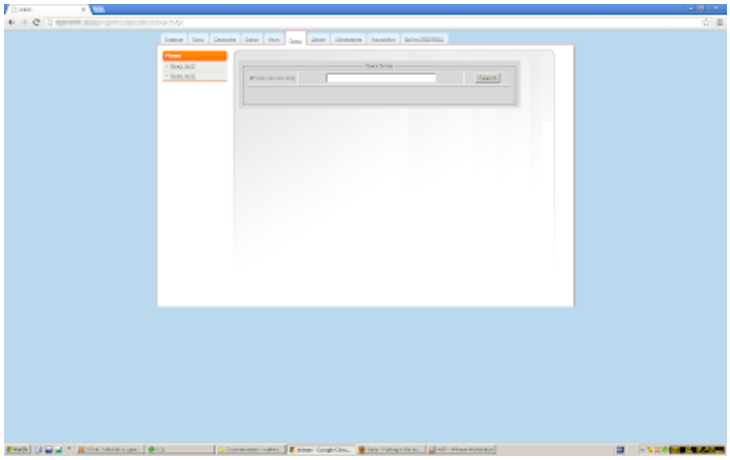
Comments:



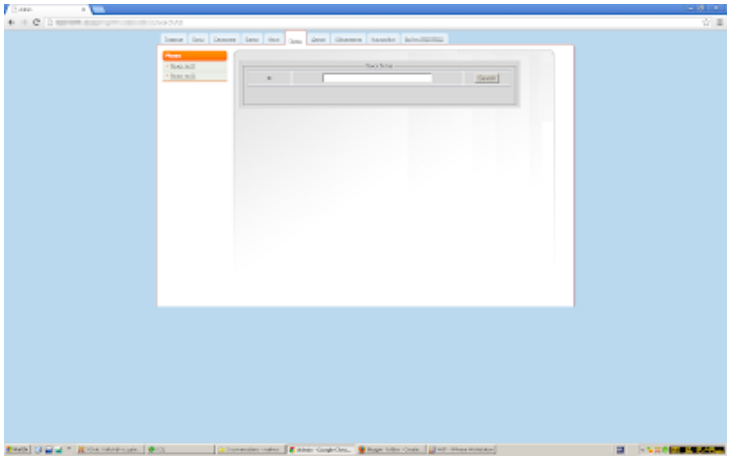
Others:



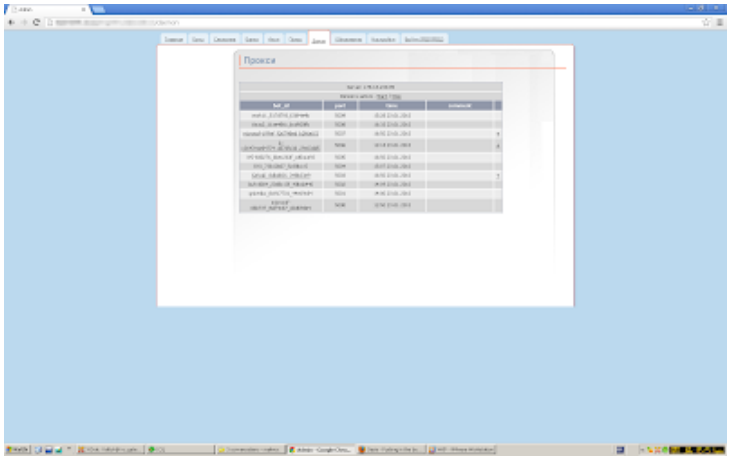
Search via IP:



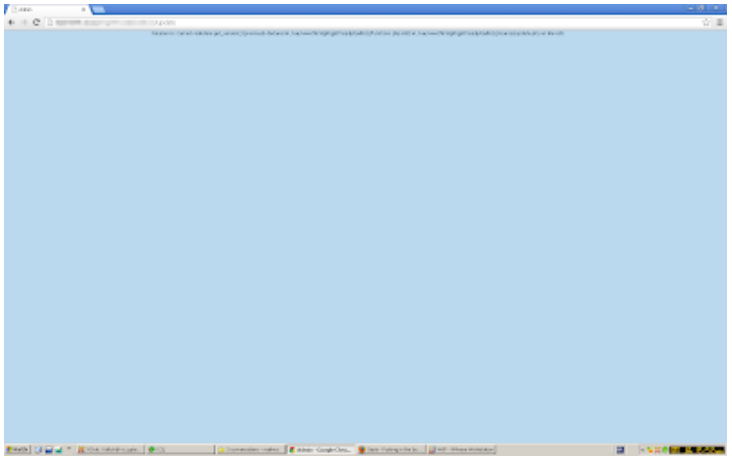
Search via ID:



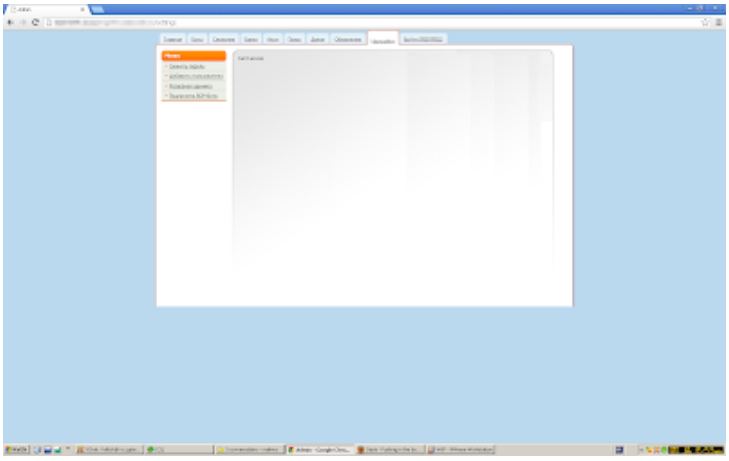
Daemon:



Update:



Settings:



Source: http://www.xylibox.com/2013/01/trojanwin32spyranbyus.html