МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

Анализ дампа памяти в REMnux при помощи Volatility

Отчет по лабораторной работе 2

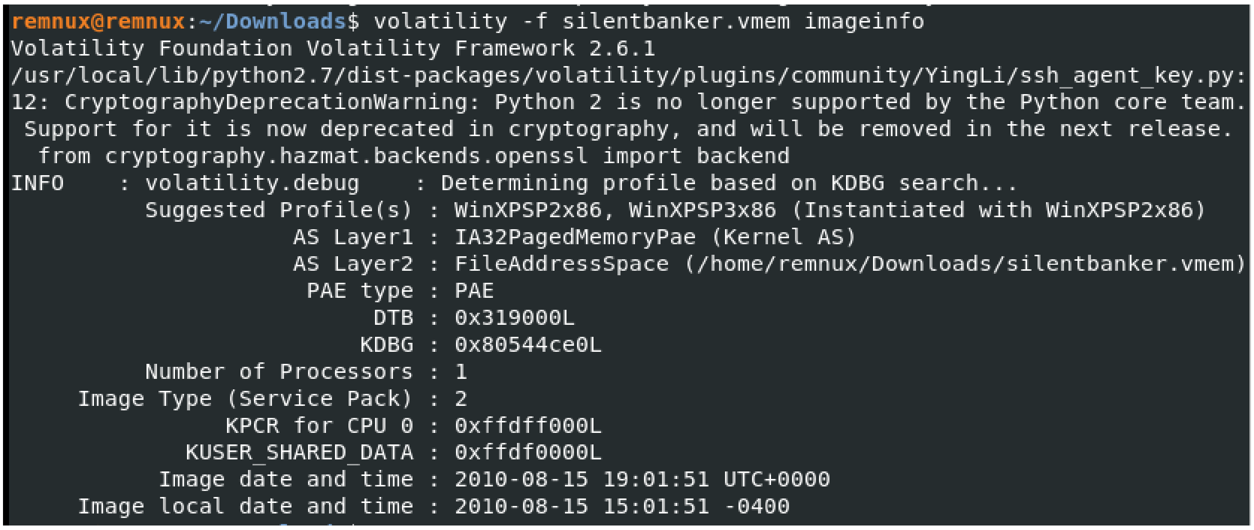
по дисциплине «**Информационная безопасность**»

студента 3 курса группы ИВТ-б-о-202
Шор Константина Александровича

Направления подготовки 09.03.01«Информатика и вычислительная техника»

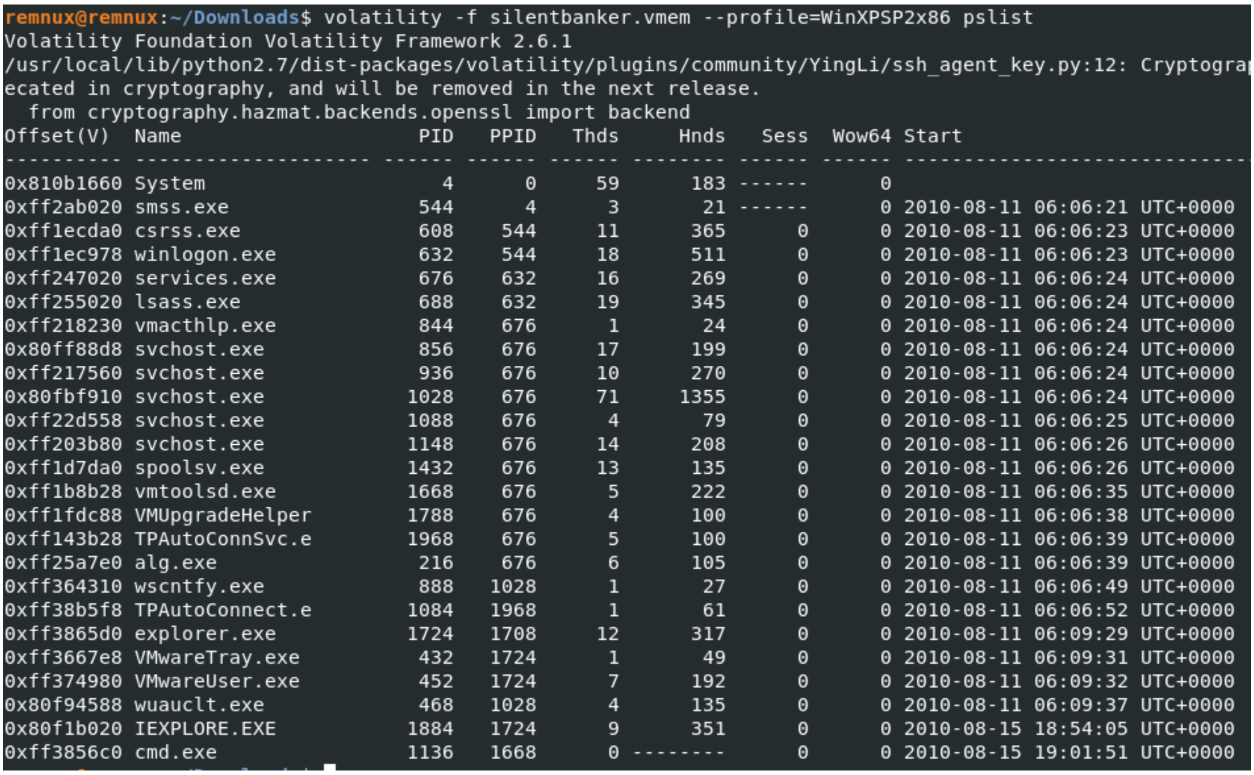
Симферополь, 2023

Imageinfo (Информация о дампе)



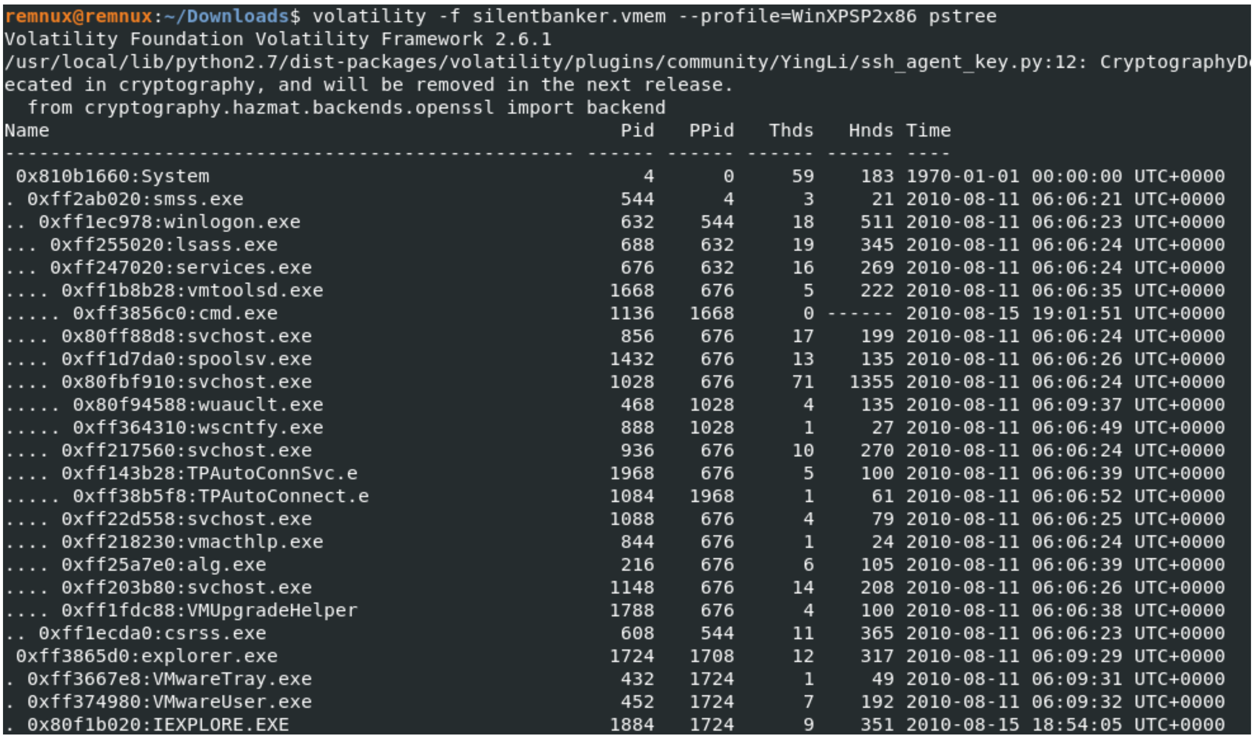
```
remnux@remnux:~/Downloads$ volatility -f silentbanker.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:
12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team.
 Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/remnux/Downloads/silentbanker.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-08-15 19:01:51 UTC+0000
     Image local date and time : 2010-08-15 15:01:51 -0400
```

Pslist (Список процессов в момент дампа)



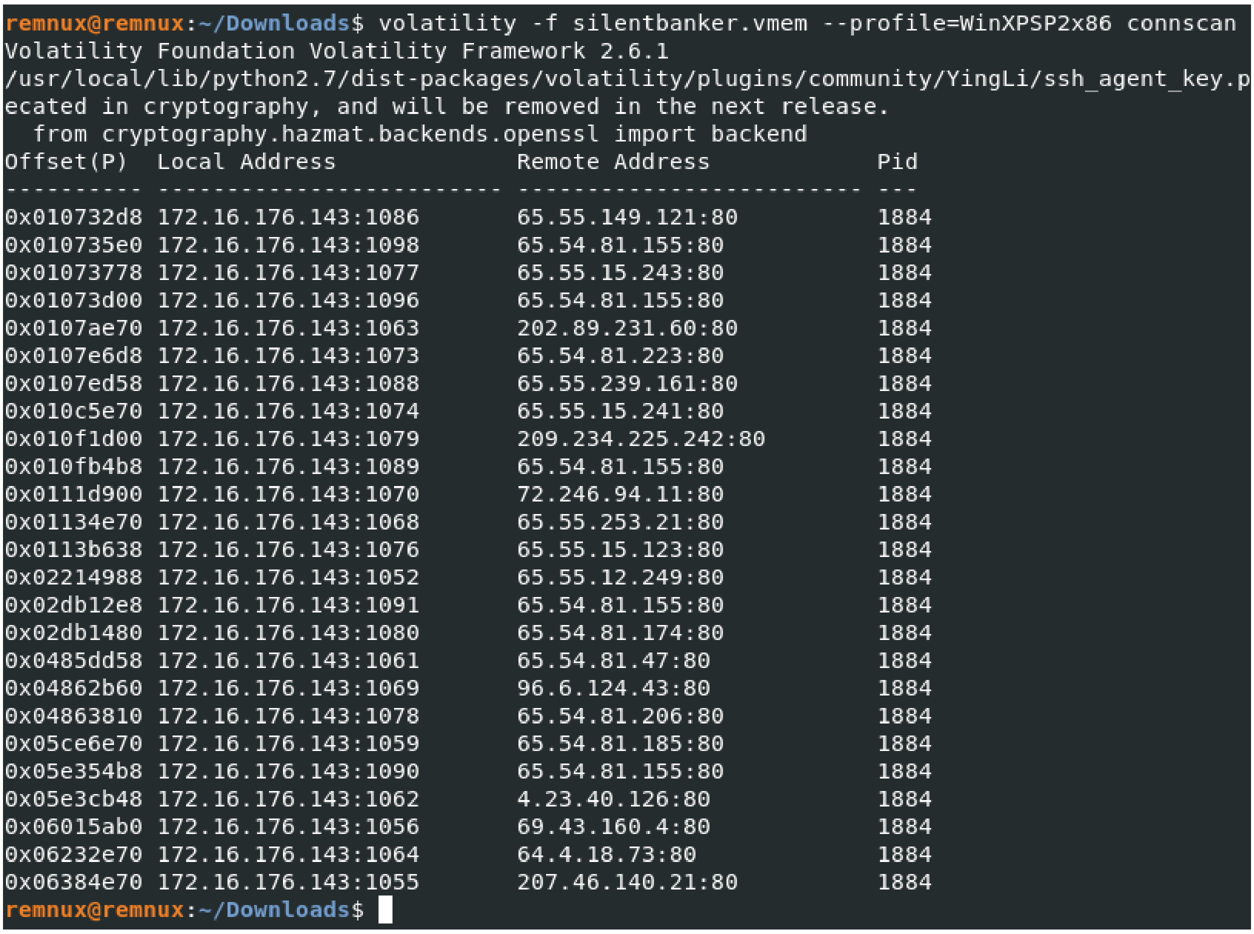
```
remnux@remnux:~/Downloads$ volatility -f silentbanker.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: Cryptograp
ecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
0x810b1660 System                    4      0     59      183 ------      0
0xff2ab020 smss.exe                544      4      3       21 ------      0 2010-08-11 06:06:21 UTC+0000
0xff1ecda0 csrss.exe               608    544     11      365      0      0 2010-08-11 06:06:23 UTC+0000
0xff1ec978 winlogon.exe            632    544     18      511      0      0 2010-08-11 06:06:23 UTC+0000
0xff247020 services.exe            676    632     16      269      0      0 2010-08-11 06:06:24 UTC+0000
0xff255020 lsass.exe               688    632     19      345      0      0 2010-08-11 06:06:24 UTC+0000
0xff218230 vmacthlp.exe            844    676      1       24      0      0 2010-08-11 06:06:24 UTC+0000
0x80ff88d8 svchost.exe             856    676     17      199      0      0 2010-08-11 06:06:24 UTC+0000
0xff217560 svchost.exe             936    676     10      270      0      0 2010-08-11 06:06:24 UTC+0000
0x80fbf910 svchost.exe            1028    676     71     1355      0      0 2010-08-11 06:06:24 UTC+0000
0xff22d558 svchost.exe            1088    676      4       79      0      0 2010-08-11 06:06:25 UTC+0000
0xff203b80 svchost.exe            1148    676     14      208      0      0 2010-08-11 06:06:26 UTC+0000
0xff1d7da0 spoolsv.exe            1432    676     13      135      0      0 2010-08-11 06:06:26 UTC+0000
0xff1b8b28 vmtoolsd.exe           1668    676      5      222      0      0 2010-08-11 06:06:35 UTC+0000
0xff1fdc88 VMUpgradeHelper        1788    676      4      100      0      0 2010-08-11 06:06:38 UTC+0000
0xff143b28 TPAutoConnSvc.e        1968    676      5      100      0      0 2010-08-11 06:06:39 UTC+0000
0xff25a7e0 alg.exe                 216    676      6      105      0      0 2010-08-11 06:06:39 UTC+0000
0xff364310 wscntfy.exe             888   1028      1       27      0      0 2010-08-11 06:06:49 UTC+0000
0xff38b5f8 TPAutoConnect.e        1084   1968      1       61      0      0 2010-08-11 06:06:52 UTC+0000
0xff3865d0 explorer.exe           1724   1708     12      317      0      0 2010-08-11 06:09:29 UTC+0000
0xff3667e8 VMwareTray.exe          432   1724      1       49      0      0 2010-08-11 06:09:31 UTC+0000
0xff374980 VMwareUser.exe          452   1724      7      192      0      0 2010-08-11 06:09:32 UTC+0000
0x80f94588 wuauclt.exe             468   1028      4      135      0      0 2010-08-11 06:09:37 UTC+0000
0x80f1b020 IEXPLORE.EXE           1884   1724      9      351      0      0 2010-08-15 18:54:05 UTC+0000
0xff3856c0 cmd.exe                1136   1668      0 --------      0      0 2010-08-15 19:01:51 UTC+0000
```

Pstree



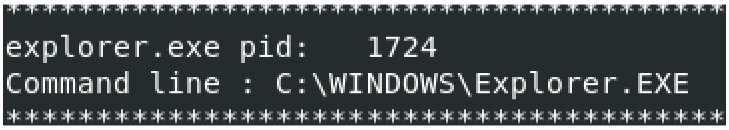
```
remnux@remnux:~/Downloads$ volatility -f silentbanker.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyD
ecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x810b1660:System                                      4      0     59    183 1970-01-01 00:00:00 UTC+0000
. 0xff2ab020:smss.exe                                 544      4      3     21 2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe                            632    544     18    511 2010-08-11 06:06:23 UTC+0000
... 0xff255020:lsass.exe                              688    632     19    345 2010-08-11 06:06:24 UTC+0000
... 0xff247020:services.exe                           676    632     16    269 2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe                         1668    676      5    222 2010-08-11 06:06:35 UTC+0000
..... 0xff3856c0:cmd.exe                             1136   1668      0 ------ 2010-08-15 19:01:51 UTC+0000
.... 0x80ff88d8:svchost.exe                           856    676     17    199 2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe                          1432    676     13    135 2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe                          1028    676     71   1355 2010-08-11 06:06:24 UTC+0000
..... 0x80f94588:wuauclt.exe                          468   1028      4    135 2010-08-11 06:09:37 UTC+0000
..... 0xff364310:wscntfy.exe                          888   1028      1     27 2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe                           936    676     10    270 2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e                      1968    676      5    100 2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e                     1084   1968      1     61 2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe                          1088    676      4     79 2010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe                          844    676      1     24 2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe                               216    676      6    105 2010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe                          1148    676     14    208 2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper                      1788    676      4    100 2010-08-11 06:06:38 UTC+0000
.. 0xff1ecda0:csrss.exe                               608    544     11    365 2010-08-11 06:06:23 UTC+0000
 0xff3865d0:explorer.exe                             1724   1708     12    317 2010-08-11 06:09:29 UTC+0000
. 0xff3667e8:VMwareTray.exe                           432   1724      1     49 2010-08-11 06:09:31 UTC+0000
. 0xff374980:VMwareUser.exe                           452   1724      7    192 2010-08-11 06:09:32 UTC+0000
. 0x80f1b020:IEXPLORE.EXE                            1884   1724      9    351 2010-08-15 18:54:05 UTC+0000
```

Connscan (Внешние подключения)

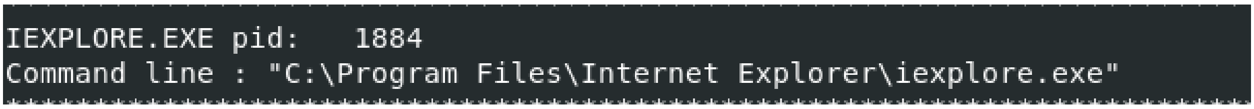


```
remnux@remnux:~/Downloads$ volatility -f silentbanker.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.p
ecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x010732d8 172.16.176.143:1086       65.55.149.121:80          1884
0x010735e0 172.16.176.143:1098       65.54.81.155:80           1884
0x01073778 172.16.176.143:1077       65.55.15.243:80           1884
0x01073d00 172.16.176.143:1096       65.54.81.155:80           1884
0x0107ae70 172.16.176.143:1063       202.89.231.60:80          1884
0x0107e6d8 172.16.176.143:1073       65.54.81.223:80           1884
0x0107ed58 172.16.176.143:1088       65.55.239.161:80          1884
0x010c5e70 172.16.176.143:1074       65.55.15.241:80           1884
0x010f1d00 172.16.176.143:1079       209.234.225.242:80        1884
0x010fb4b8 172.16.176.143:1089       65.54.81.155:80           1884
0x0111d900 172.16.176.143:1070       72.246.94.11:80           1884
0x01134e70 172.16.176.143:1068       65.55.253.21:80           1884
0x0113b638 172.16.176.143:1076       65.55.15.123:80           1884
0x02214988 172.16.176.143:1052       65.55.12.249:80           1884
0x02db12e8 172.16.176.143:1091       65.54.81.155:80           1884
0x02db1480 172.16.176.143:1080       65.54.81.174:80           1884
0x0485dd58 172.16.176.143:1061       65.54.81.47:80            1884
0x04862b60 172.16.176.143:1069       96.6.124.43:80            1884
0x04863810 172.16.176.143:1078       65.54.81.206:80           1884
0x05ce6e70 172.16.176.143:1059       65.54.81.185:80           1884
0x05e354b8 172.16.176.143:1090       65.54.81.155:80           1884
0x05e3cb48 172.16.176.143:1062       4.23.40.126:80            1884
0x06015ab0 172.16.176.143:1056       69.43.160.4:80            1884
0x06232e70 172.16.176.143:1064       64.4.18.73:80             1884
0x06384e70 172.16.176.143:1055       207.46.140.21:80          1884
remnux@remnux:~/Downloads$
```

Подозреваемые файлы

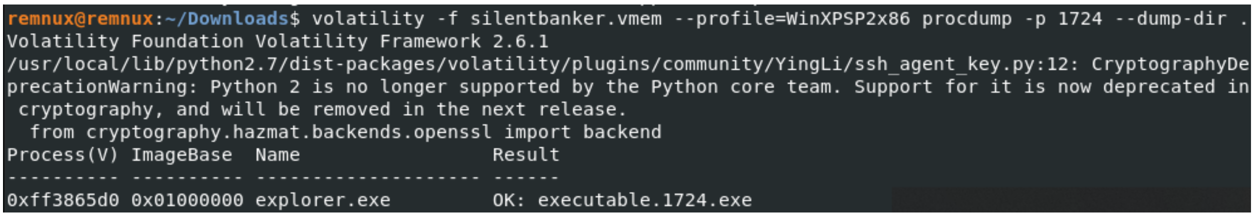


```
*****************************************
explorer.exe pid:   1724
Command line : C:\WINDOWS\Explorer.EXE
*****************************************
```

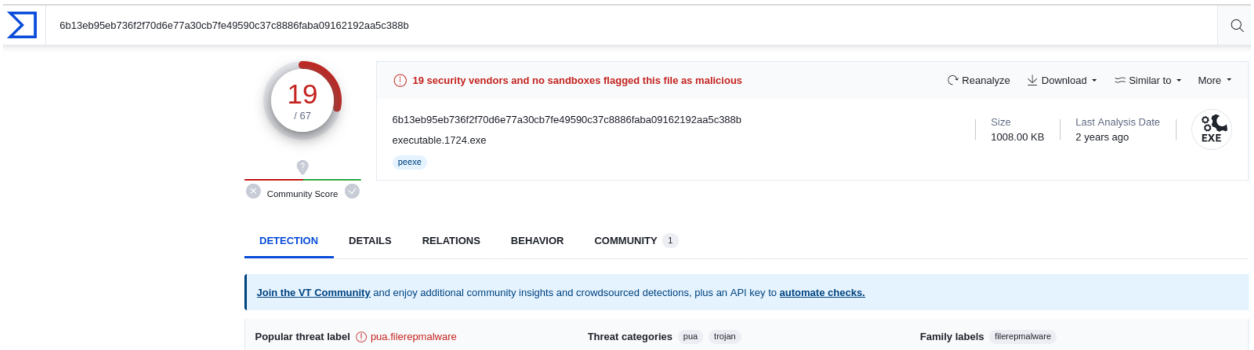


```
IEXPLORE.EXE pid:   1884
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"
************************************************************************
```

Восстановление исполняемых файлов



```
remnux@remnux:~/Downloads$ volatility -f silentbanker.vmem --profile=WinXPSP2x86 procdump -p 1724 --dump-dir .
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDe
precationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in
 cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0xff3865d0 0x01000000 explorer.exe         OK: executable.1724.exe
```



6b13eb95eb736f2f70d6e77a30cb7fe49590c37c8886faba09162192aa5c388b

19 / 67

19 security vendors and no sandboxes flagged this file as malicious

6b13eb95eb736f2f70d6e77a30cb7fe49590c37c8886faba09162192aa5c388b
executable.1724.exe
peexe

Size 1008.00 KB

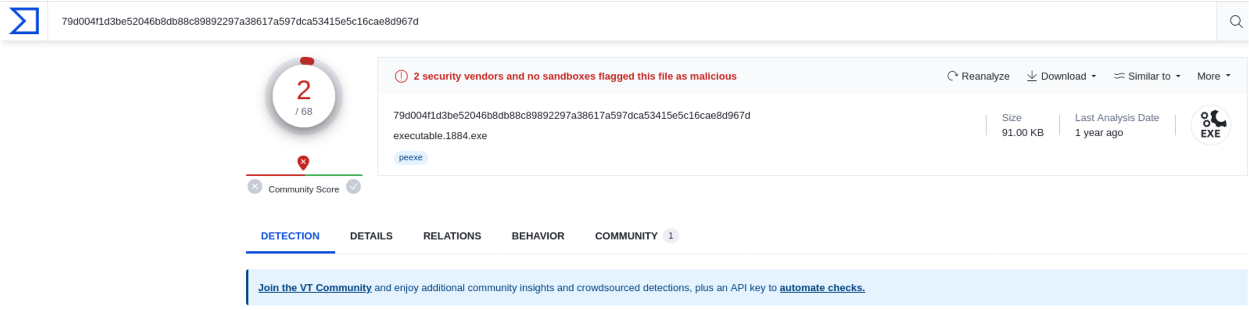
Last Analysis Date 2 years ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label pua.filerepmalware

Threat categories pua trojan

Family labels filerepmalware



79d004f1d3be52046b8db88c89892297a38617a597dca53415e5c16cae8d967d

2 / 68

2 security vendors and no sandboxes flagged this file as malicious

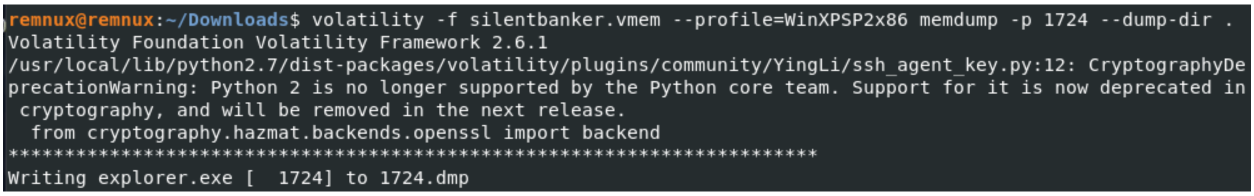
79d004f1d3be52046b8db88c89892297a38617a597dca53415e5c16cae8d967d
executable.1884.exe
peexe

Size 91.00 KB

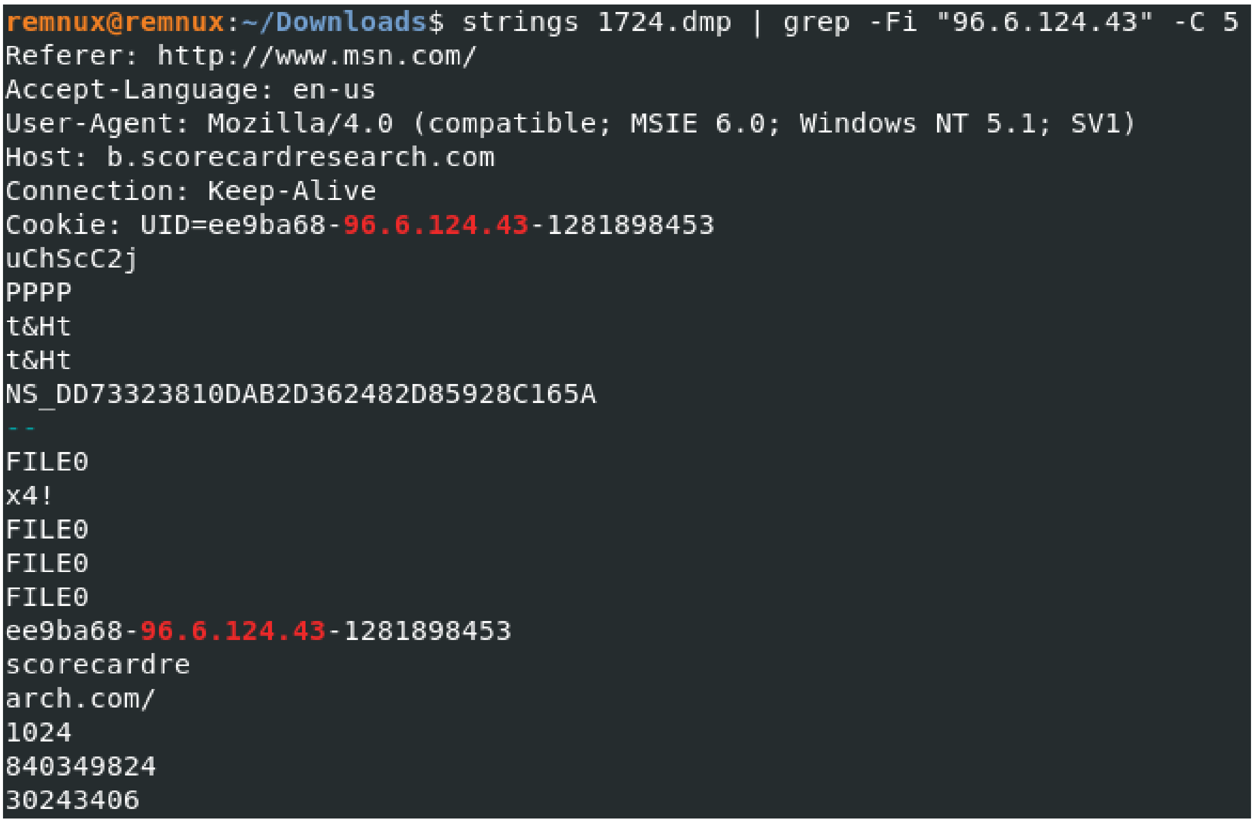
Last Analysis Date 1 year ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

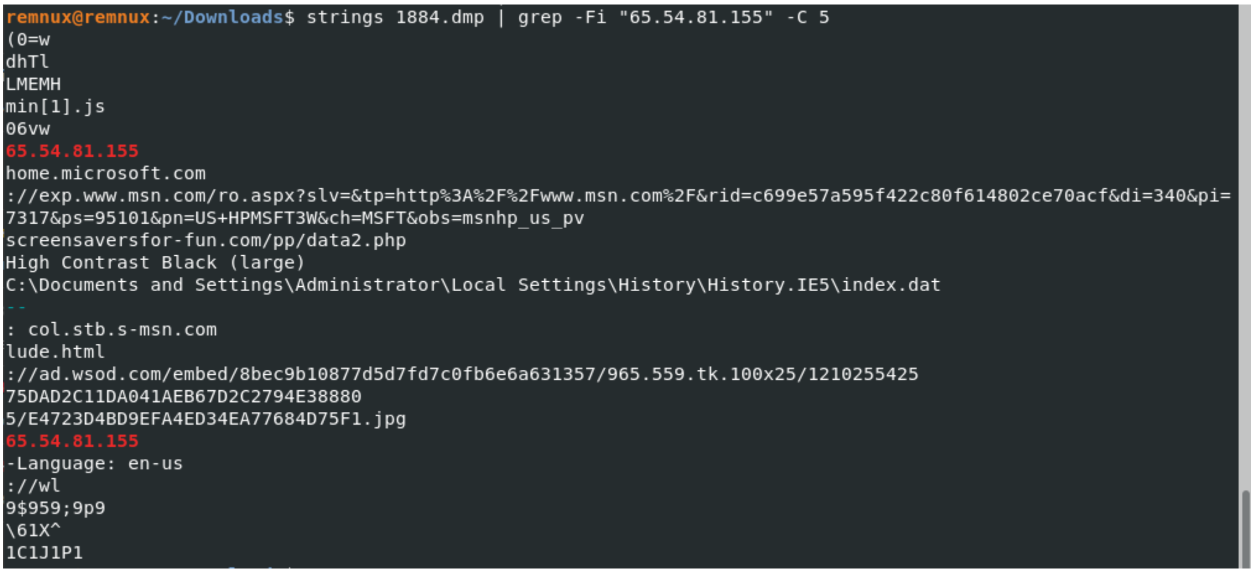
Восстановления дампа оперативной памяти



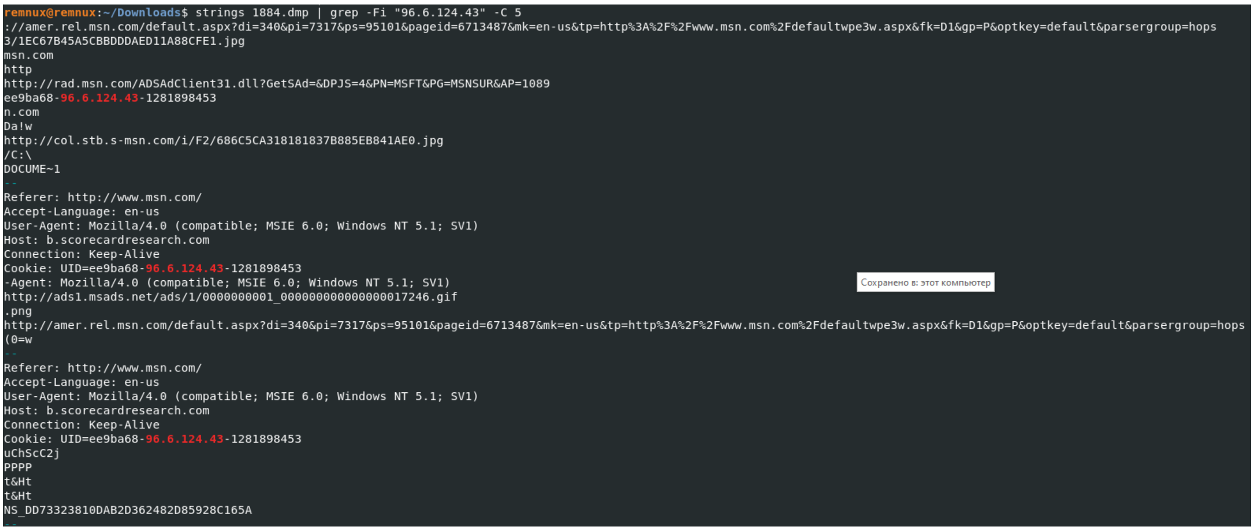
```
remnux@remnux:~/Downloads$ volatility -f silentbanker.vmem --profile=WinXPSP2x86 memdump -p 1724 --dump-dir .
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDe
precationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in
 cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
************************************************************************
Writing explorer.exe [  1724] to 1724.dmp
```



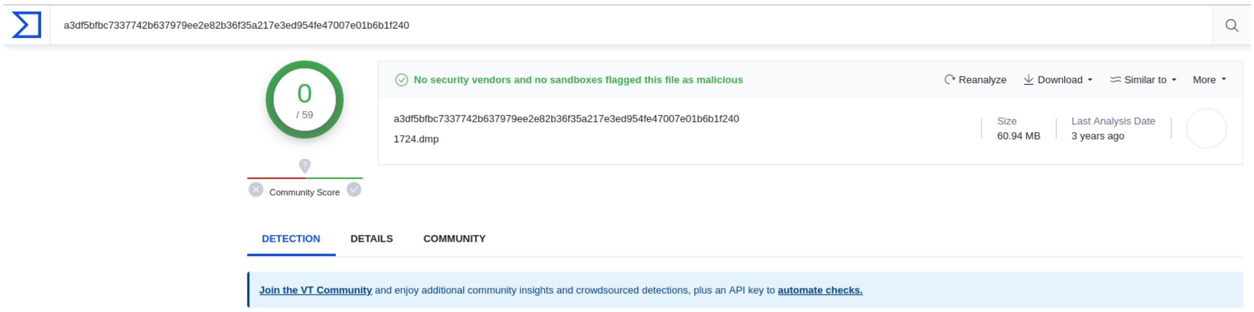
```
remnux@remnux:~/Downloads$ strings 1724.dmp | grep -Fi "96.6.124.43" -C 5
Referer: http://www.msn.com/
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: b.scorecardresearch.com
Connection: Keep-Alive
Cookie: UID=ee9ba68-96.6.124.43-1281898453
uChScC2j
PPPP
t&Ht
t&Ht
NS_DD73323810DAB2D362482D85928C165A
--
FILE0
x4!
FILE0
FILE0
FILE0
ee9ba68-96.6.124.43-1281898453
scorecardre
arch.com/
1024
840349824
30243406
```



```
remnux@remnux:~/Downloads$ strings 1884.dmp | grep -Fi "65.54.81.155" -C 5
(0=w
dhTl
LMEMH
min[1].js
06vw
65.54.81.155
home.microsoft.com
://exp.www.msn.com/ro.aspx?slv=&tp=http%3A%2F%2Fwww.msn.com%2F&rid=c699e57a595f422c80f614802ce70acf&di=340&pi=
7317&ps=95101&pn=US+HPMSFT3W&ch=MSFT&obs=msnhp_us_pv
screensaversfor-fun.com/pp/data2.php
High Contrast Black (large)
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat
--
: col.stb.s-msn.com
lude.html
://ad.wsod.com/embed/8bec9b10877d5d7fd7c0fb6e6a631357/965.559.tk.100x25/1210255425
75DAD2C11DA041AEB67D2C2794E38880
5/E4723D4BD9EFA4ED34EA77684D75F1.jpg
65.54.81.155
-Language: en-us
://wl
9$959;9p9
\61X^
1C1J1P1
```



```
remnux@remnux:~/Downloads$ strings 1884.dmp | grep -Fi "96.6.124.43" -C 5
://amer.rel.msn.com/default.aspx?di=340&pi=7317&ps=95101&pageid=6713487&mk=en-us&tp=http%3A%2F%2Fwww.msn.com%2Fdefaultwpe3w.aspx&fk=D1&gp=P&optkey=default&parsergroup=hops
3/1EC67B45A5CBBDDDAED11A88CFE1.jpg
msn.com
http
http://rad.msn.com/ADSAdClient31.dll?GetSAd=&DPJS=4&PN=MSFT&PG=MSNSUR&AP=1089
ee9ba68-96.6.124.43-1281898453
n.com
Da!w
http://col.stb.s-msn.com/i/F2/686C5CA318181837B885EB841AE0.jpg
/C:\
DOCUME~1
--
Referer: http://www.msn.com/
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: b.scorecardresearch.com
Connection: Keep-Alive
Cookie: UID=ee9ba68-96.6.124.43-1281898453
-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
http://ads1.msads.net/ads/1/0000000001_000000000000000017246.gif
.png
http://amer.rel.msn.com/default.aspx?di=340&pi=7317&ps=95101&pageid=6713487&mk=en-us&tp=http%3A%2F%2Fwww.msn.com%2Fdefaultwpe3w.aspx&fk=D1&gp=P&optkey=default&parsergroup=hops
(0=w
--
Referer: http://www.msn.com/
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: b.scorecardresearch.com
Connection: Keep-Alive
Cookie: UID=ee9ba68-96.6.124.43-1281898453
uChScC2j
PPPP
t&Ht
t&Ht
NS_DD73323810DAB2D362482D85928C165A
--
```



a3df5bfbc7337742b637979ee2e82b36f35a217e3ed954fe47007e01b6b1f240

0 / 59

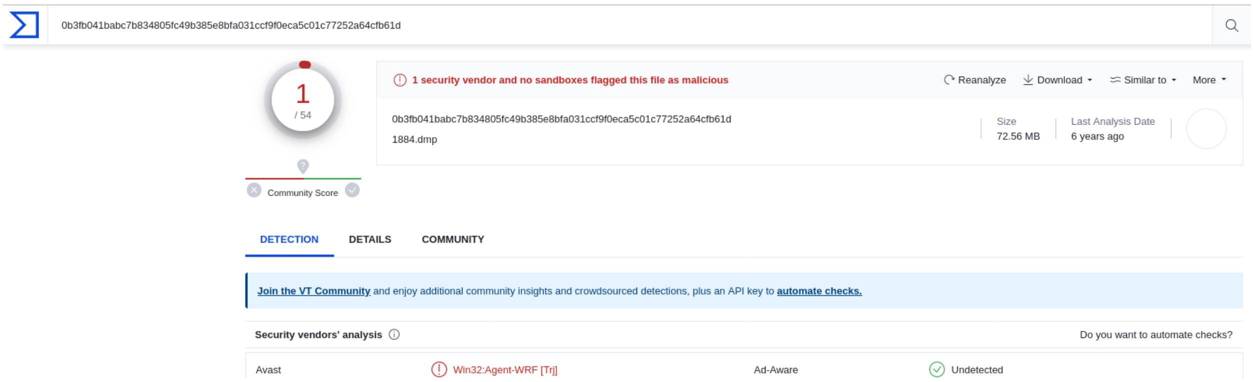
No security vendors and no sandboxes flagged this file as malicious

a3df5bfbc7337742b637979ee2e82b36f35a217e3ed954fe47007e01b6b1f240
1724.dmp

Size 60.94 MB

Last Analysis Date 3 years ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.



0b3fb041babc7b834805fc49b385e8bfa031ccf9f0eca5c01c77252a64cfb61d

1 / 54

1 security vendor and no sandboxes flagged this file as malicious

0b3fb041babc7b834805fc49b385e8bfa031ccf9f0eca5c01c77252a64cfb61d
1884.dmp

Size 72.56 MB

Last Analysis Date 6 years ago

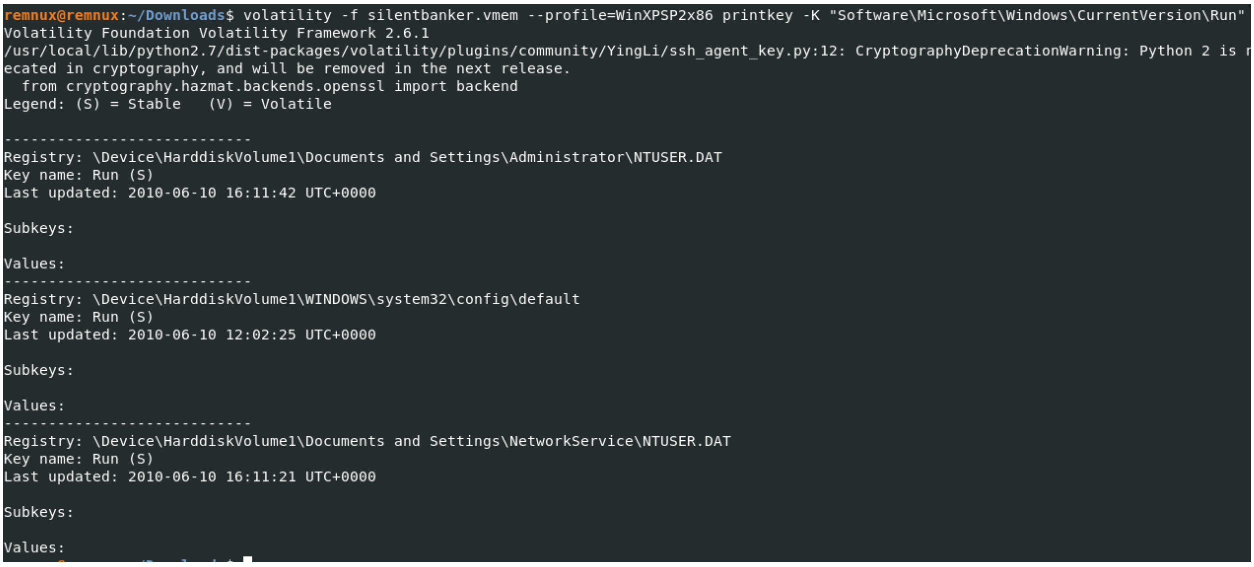
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Avast	Win32:Agent-WRF [Trj]	Ad-Aware	Undetected

Проверка автозагрузки



```
remnux@remnux:~/Downloads$ volatility -f silentbanker.vmem --profile=WinXPSP2x86 printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDeprecationWarning: Python 2 is n
ecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Key name: Run (S)
Last updated: 2010-06-10 16:11:42 UTC+0000

Subkeys:

Values:
----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: Run (S)
Last updated: 2010-06-10 12:02:25 UTC+0000

Subkeys:

Values:
----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
Key name: Run (S)
Last updated: 2010-06-10 16:11:21 UTC+0000

Subkeys:

Values:
```