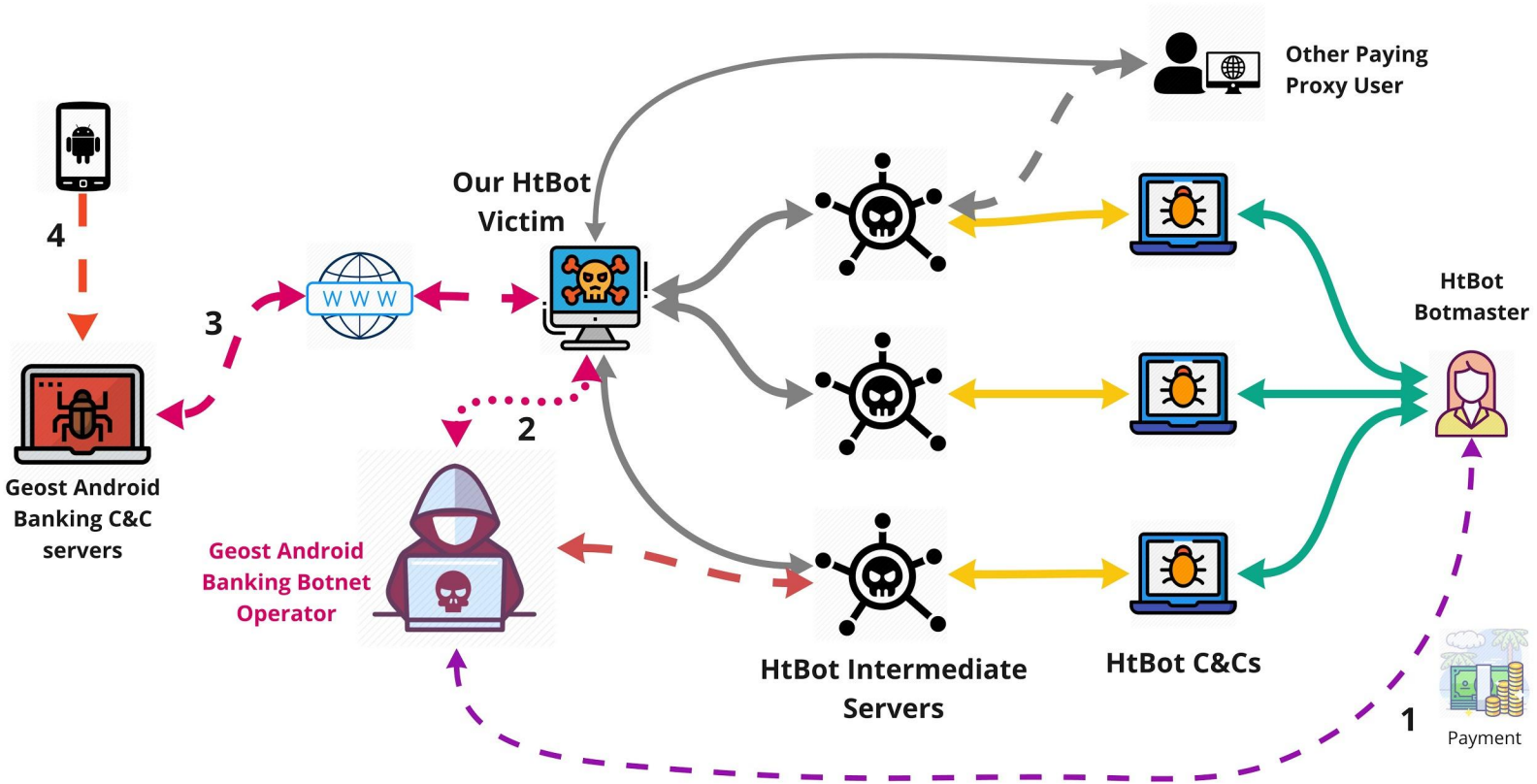
Cybercriminal Activities Managing a New Android Botnet

Sebastian Garcia
sebastian.garcia@agents.fel.cvut.cz
@eldracote

Maria Jose Erquiaga
mariajoseerquiaga@gmail.com
@MaryJo_E

Anna Shirokova
shirokova@avast.com
@anshirokova

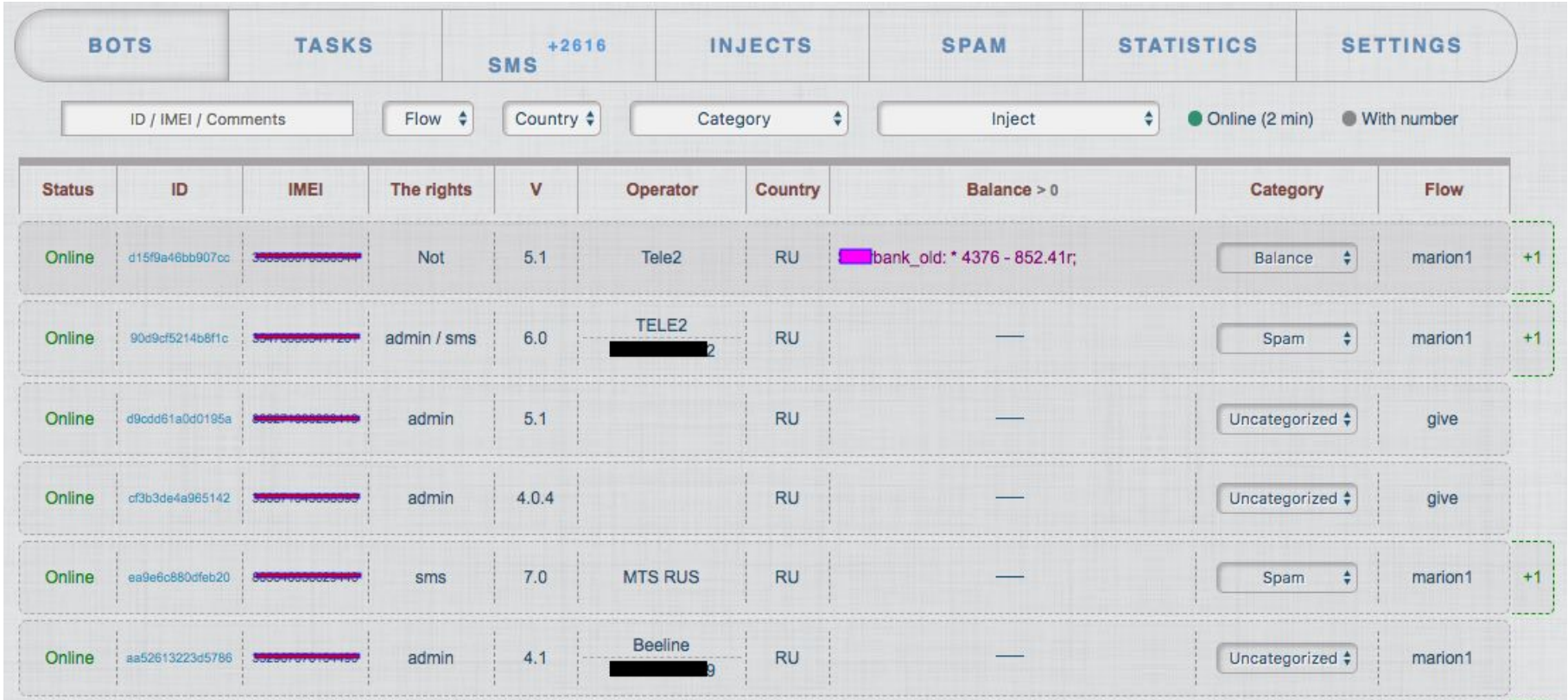
From HtBot to Geost



From 1 Domain to the Geost Infrastructure

- C&C IPs: 13
  - Countries: US, **MU** and RU
  - Each IP hosts 1-100 Geost domains
- ~ 150 Unique Domains
  - DGA style, not quite
- ~150 APKs
  - Identified as **Android Hqwar** or **Banking Trojan**, but there are many others

Geost Command and Control Panel



Randomness as a Feature

Domains

- w24t2t2tfwg.ru
- Wg34gh44t.xyz
- 42r3t24wef.ru
- 34j2lxii24.ru
- Wgg5ggefwg.ru
- 52t34tyt53.xyz

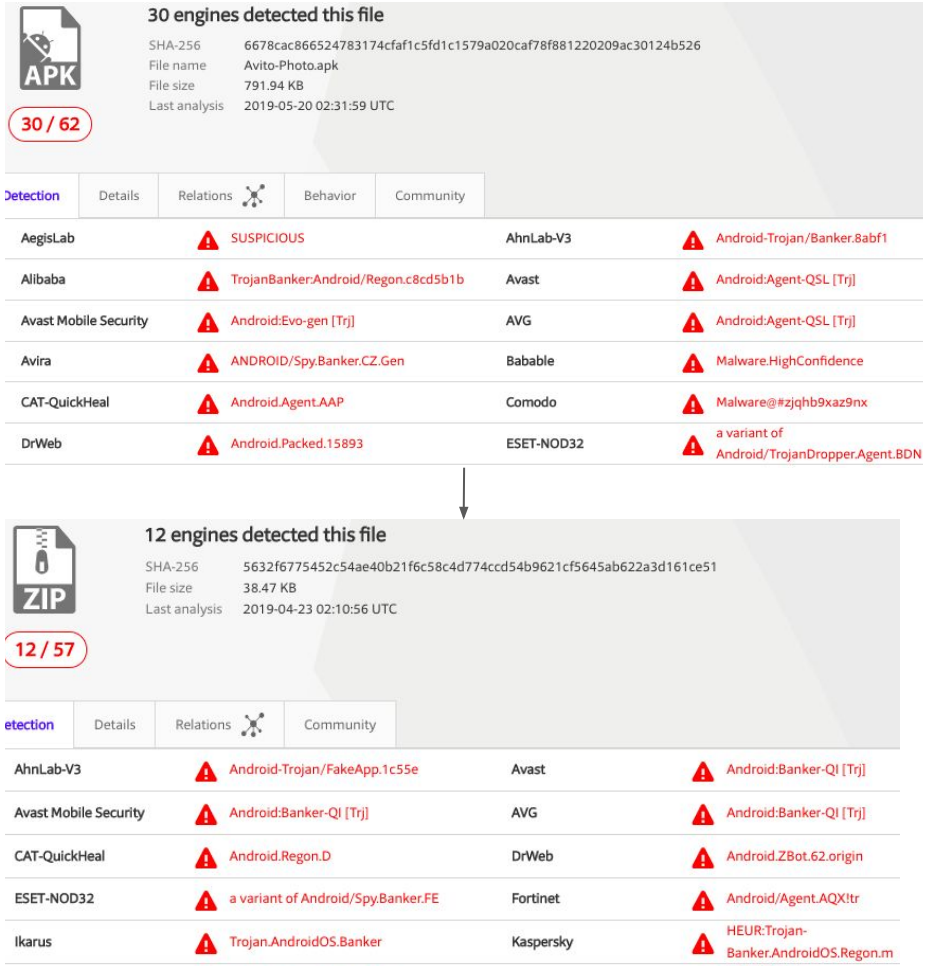
PHP files (one per APK file)

- M99h49wtp1g35b5721d64mfs5p8ese1x.php
- n7co2vpu098x85ctgdn689rf4d18n5jz.php
- fhdkqgyfux4gj2t6zwu434ptw0i0mefu.php
- csbu72ow56i9qq7yg1ufbo3ql1phb1s6.php
- f8t8d5tnqvwwi1l2qf0itr97cdibre6i.php
- hgkvf2riqt49z33isl978pj17aivc0nw.php

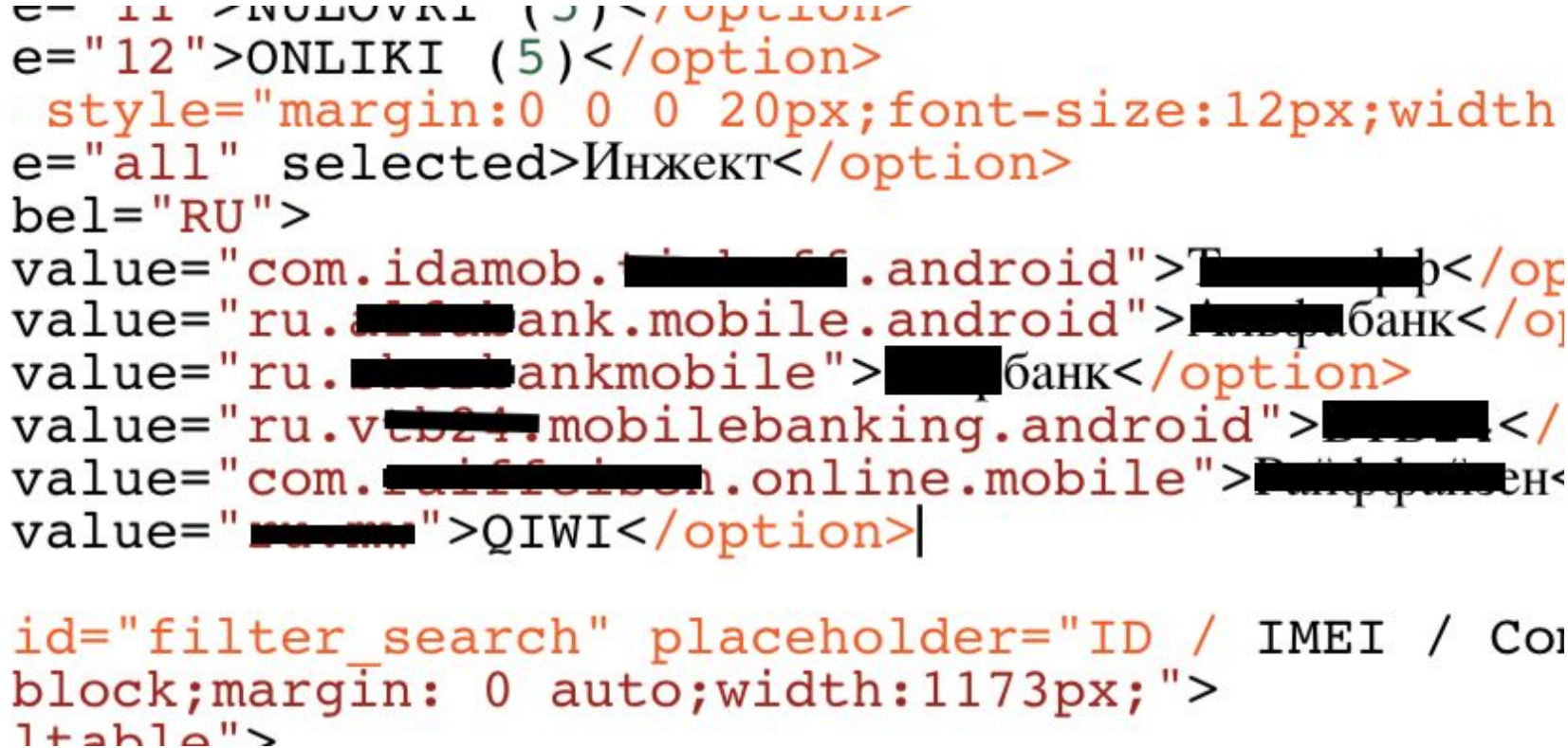
Why?

Geost APKs

Detections	Name
33/62	Yandeks.Navigator.apk
34/61	adobe_reader.apk
24/62	Odnoklassniki.apk
21/62	youtube.apk
21/62	Avito-Photo.apk
19/62	sberbank_onlayn.apk
33/61	visa_qiwi.apk
23/62	book.apk
33/61	Perevodchik.apk
32/62	navitel.apk
33/59	thirtydayfitnesschallenge.apk
32/62	word.apk
31/61	MMS.apk
16/59	Avito-Photo.apk
22/59	banker.apk
11/59	word.apk
28/61	Pokemon_GO.apk



Banks Targeted

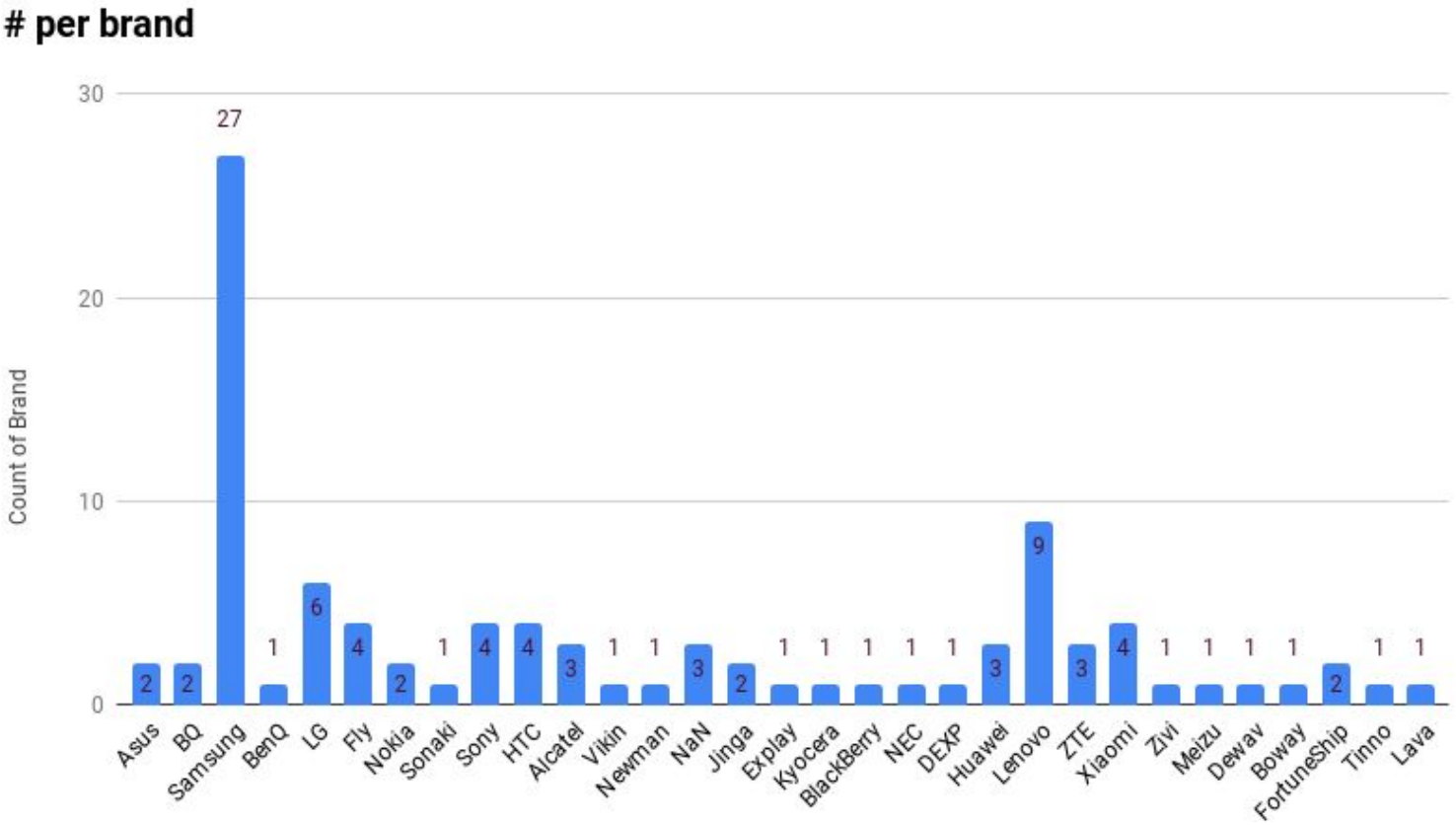


Geost Victims and SMS

- ~800,000 victims. ~65,000 per CC.
- Per victim, >700 SMS per year

29/07/17 12:19 VISA5880 purchase 324r MAG[redacted]J Balance: 27598.58r
Charges: YM * (RUB 400.00); password: 1[redacted]5. Do not give your password to anyone. Only scammers ask for passwords.
29/07/17 19:14 VISA5880 purchase 400r YM * Balance: 27198.58r
Your verification code 141
30/07/17 10:40 VISA5880 purchase 469r \ SPORTMASTER \ "SHOP Balance: 26729.58r"
VISA5880 30/07/17 13:56 ATM cash withdrawal 4000r 224228 Balance: 22729.58r
Charges: PSCB * PHONE (RUB 200.00); password: [redacted]. Do not give your password to anyone. Only scammers ask for passwords.
30/07/17 12:58 VISA5880 purchase 200r PSCB.RU Balance: 22529.58r
VISA5880 30/07/17 12:58 canceling purchases 200r Balance: 22729.58r
Charges: PSCB * PHONE (RUB 200.00); password: [redacted]. Do not give your password to anyone. Only scammers ask for passwords.
30/07/17 13:06 VISA5880 purchase 200r PSCB.RU Balance: 22529.58r
VISA5880 07/30/17 13:06 canceling purchases 200r Balance: 22729.58r
Night Sale! Additional 12% NIGHT3007 code. Term to 10:00 on 30 July. A discount of not more than 5000 rubles. https: \ / \ / goo.gl \ / E

Victims Phones in 1 page only



Breakthrough

From some “information” about Geost, Veronica Valeros “found” a file in a public webpage that was a Skype chat log

Breakthrough

From some “information” about Geost, Veronica V[illegible]und” a file in a public web[illegible] was a Skype chat log

Geost Leads to a New Discovery

Chat Log

6,250 lines

11 month long

28 people involved

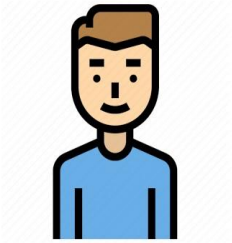
Lost in Translation

- When Google translate is not enough
- English words written in Cyrillic
- Misspelling and slang words

Brain Teaser

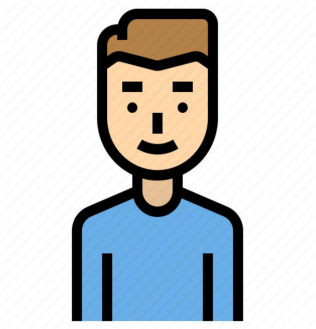
“belka” (“белка” in Cyrillic) stands for …?

Comrades



powerfaer

mirrexx777



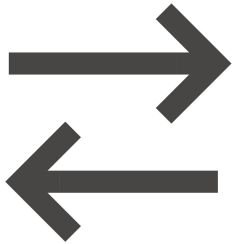
powerfaer

Paying to Mirrexx777

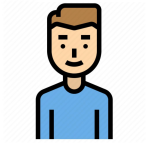
Knows people with money

Exchange money

Online Payment System



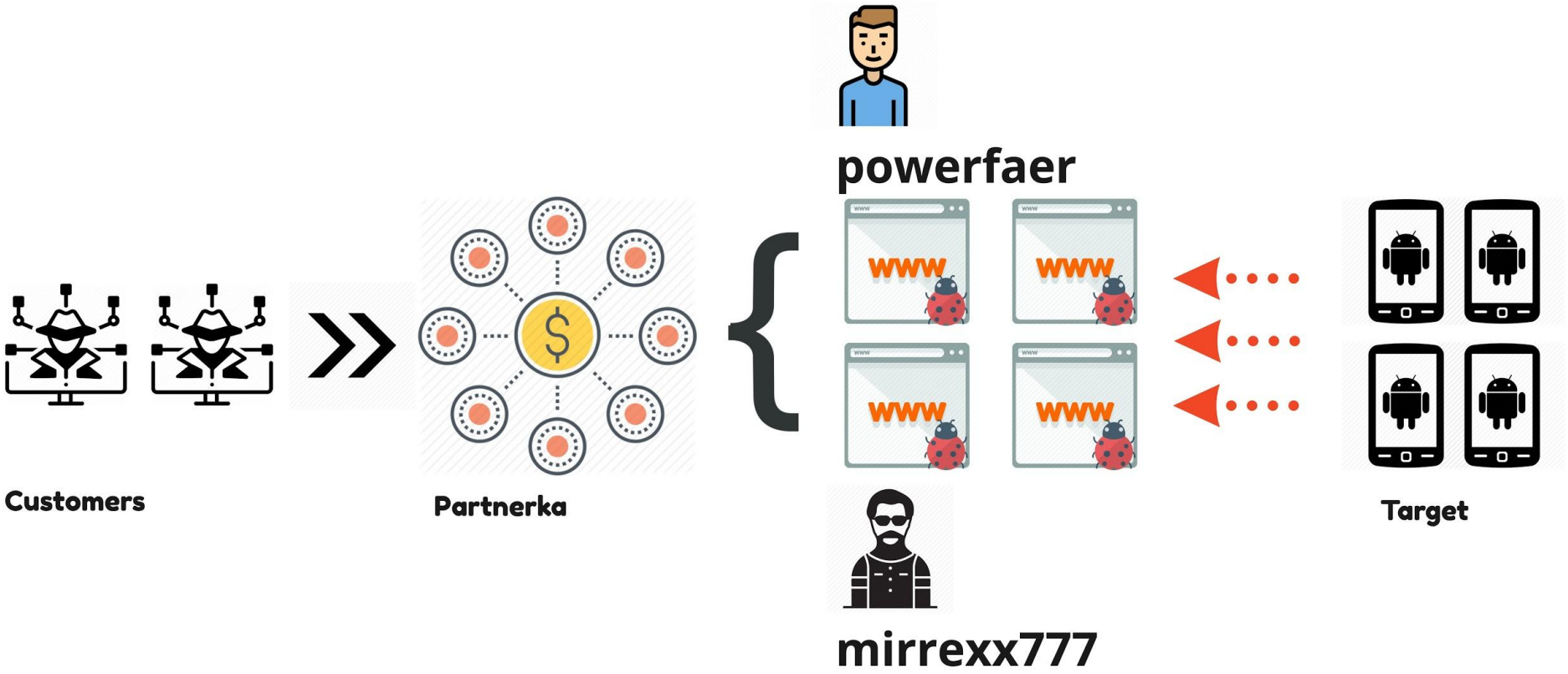
Business model



powerfaer

mirrexx777

Partnerka



How Much Money?

Price per **1 installation** is 20 rubles (**7 CZK / 0.3 USD**)

Price per **250 installations** 5,000 rubles* (**1,788 CZK / 77 USD**)

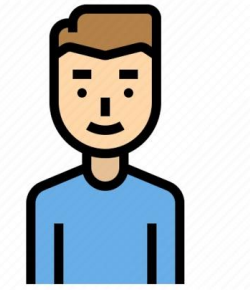
Price per **1,000 installations** 20,000 rubles* (**7,152 CZK / 310 USD**)

*** Minus fees**

**** Check your local black market contracts for more information**

Installations in Geost

694dea5.apk



powerfaer

mirrexx777

Relation to Geost

mirrexx777

694dea5.apk

Get your Money! Stats Page is Ready in Geost

http://fif33tG2dsutj.ru/stats.php?sid=boX9SzoQzU6CDpc

Conclusions?

- We are fx@#d
- Don’t use Android
- Don’t use the Internet
- Don’t

Real Conclusions

- OpSec is important. Cumbersome but important.
- Geost is large, but not *that* large. On purpose.
- Anecdotal evidence is still evidence. A glimpse on their daily life.
- The life of an attacker is…, well boring.
- Ongoing, so keep tuned for updates. (WACCO, VB, Defcon?, Blackhat?)

Questions?

Sebastian Garcia
sebastian.garcia@agents.fel.cvut.cz
@eldracote

Maria Jose Erquiaga
mariajoseerquiaga@gmail.com
@MaryJo_E

Anna Shirokova
shirokova@avast.com
@anshirokova