

Cybercriminal Activities Managing a New Android Botnet

Sebastian Garcia

sebastian.garcia@agents.fel.cvut.cz

 @eldracote

Maria Jose Erquiaga

mariajoseerquiaga@gmail.com

 @MaryJo_E

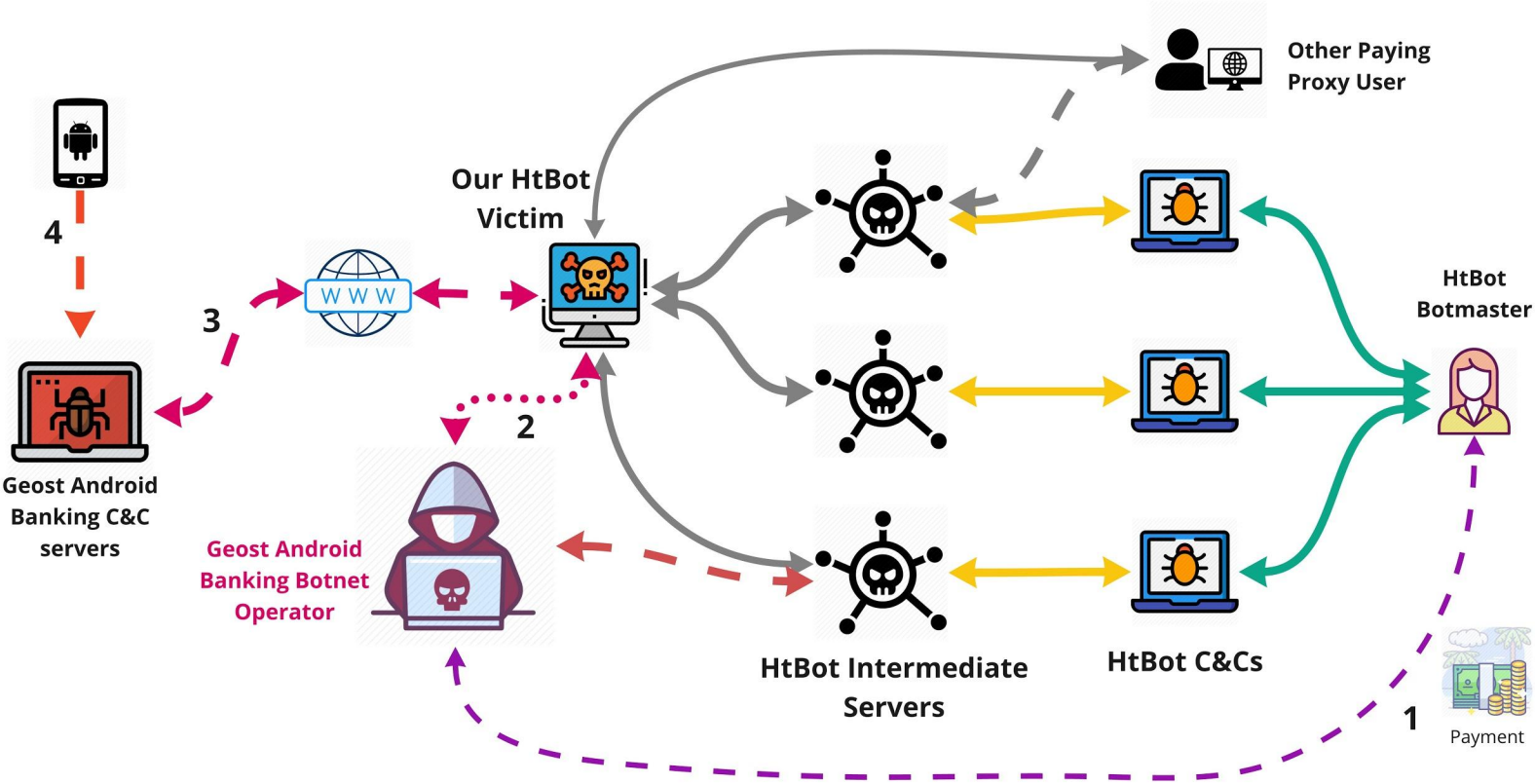
Anna Shirokova

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

| BOTS | | TASKS | | SMS ⁺²⁶¹⁶ | | INJECTS | | SPAM | | STATISTICS | | SETTINGS | |
|----------------------|-----------------|------------|-------------|----------------------|------------------------|---------|-----------------------------|---|-----------------------------------|------------|--|----------|--|
| ID / IMEI / Comments | | Flow | Country | Category | | Inject | | <input checked="" type="radio"/> Online (2 min) | <input type="radio"/> With number | | | | |
| Status | ID | IMEI | The rights | V | Operator | Country | Balance > 0 | Category | Flow | | | | |
| Online | d15f9a46bb907cc | [REDACTED] | Not | 5.1 | Tele2 | RU | bank_old: * 4376 - 852.41r; | Balance | marion1 | +1 | | | |
| Online | 90d9cf5214b8f1c | [REDACTED] | admin / sms | 6.0 | TELE2 [REDACTED]2 | RU | — | Spam | marion1 | +1 | | | |
| Online | d9odd61a0d0195a | [REDACTED] | admin | 5.1 | | RU | — | Uncategorized | give | | | | |
| Online | cf3b3de4a985142 | [REDACTED] | admin | 4.0.4 | | RU | — | Uncategorized | give | | | | |
| Online | ea9e6c880dfcb20 | [REDACTED] | sms | 7.0 | MTS RUS | RU | — | Spam | marion1 | +1 | | | |
| Online | aa52613223d5786 | [REDACTED] | admin | 4.1 | Beeline [REDACTED]9 | RU | — | Uncategorized | marion1 | | | | |

Randomness as a Feature

Domains

- w24t2t2tfwg.ru
- Wg34gh44t.xyz
- 42r3t24wef.ru
- 34j2lxii24.ru
- Wgg5ggefwwg.ru
- 52t34tyt53.xyz

PHP files (one per APK file)


- M99h49wtp1g35b5721d64mfs5p8ese1x.php
- n7co2vpu098x85ctgdn689rf4d18n5jz.php
- fhdkqgyfux4gj2t6zww434ptw0i0mefu.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 |


 **30 engines detected this file**

SHA-256 6678cac866524783174cfaf1c5fd1c1579a020caf78f881220209ac30124b526
File name Avito-Photo.apk
File size 791.94 KB
Last analysis 2019-05-20 02:31:59 UTC

30 / 62

Detection Details Relations Behavior Community











| | | | |
|-----------------------|---|------------|--|
| AegisLab |  SUSPICIOUS | AhnLab-V3 |  Android-Trojan/Banker.Babf1 |
| Alibaba |  TrojanBanker:Android/Regon.c8cd5b1b | Avast |  Android:Agent-QSL [Trj] |
| Avast Mobile Security |  Android:Evo-gen [Trj] | AVG |  Android:Agent-QSL [Trj] |
| Avira |  ANDROID/Spy.Banker.CZ.Gen | Babable |  Malware.HighConfidence |
| CAT-QuickHeal |  Android.Agent.LAAP | Comodo |  Malware@#zjqhb9xaz9nx |
| DrWeb |  Android.Packed.15893 | ESET-NOD32 |  a variant of Android/TrojanDropper.Agent.BDN |

 **12 engines detected this file**

SHA-256 5632f6775452c54ae40b21f6c58c4d774ccd54b9621cf5645ab622a3d161ce51
File size 38.47 KB
Last analysis 2019-04-23 02:10:56 UTC

12 / 57

etecction Details Relations Community

| | | | |
|-----------------------|--|-----------|--|
| AhnLab-V3 |  Android-Trojan/FakeApp.1c55e | Avast |  Android:Banker-QI [Trj] |
| Avast Mobile Security |  Android:Banker-QI [Trj] | AVG |  Android:Banker-QI [Trj] |
| CAT-QuickHeal |  Android.Regon.D | DrWeb |  Android.ZBot.62.origin |
| ESET-NOD32 |  a variant of Android/Spy.Banker.FE | Fortinet |  Android/Agent.AQX!tr |
| Ikarus |  Trojan.AndroidOS.Banker | Kaspersky |  HEUR:Trojan-Banker.AndroidOS.Regon.m |


Banks Targeted

```
e="12">ONLIKI (5)</option>
style="margin:0 0 0 20px;font-size:12px;width
e="all" selected>ИНЖЕКТ</option>
bel="RU">
value="com.idamob.████████.android">████████</option>
value="ru.████████bank.mobile.android">████████банк</option>
value="ru.████████bankmobile">████████банк</option>
value="ru.vcb24.mobilebanking.android">████████</option>
value="com.████████.online.mobile">████████банк</option>
value="████████">QIWI</option>
```

```
id="filter_search" placeholder="ID / IMEI / Co
block;margin: 0 auto;width:1173px;">
table">
```

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 MAGI [REDACTED] 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.

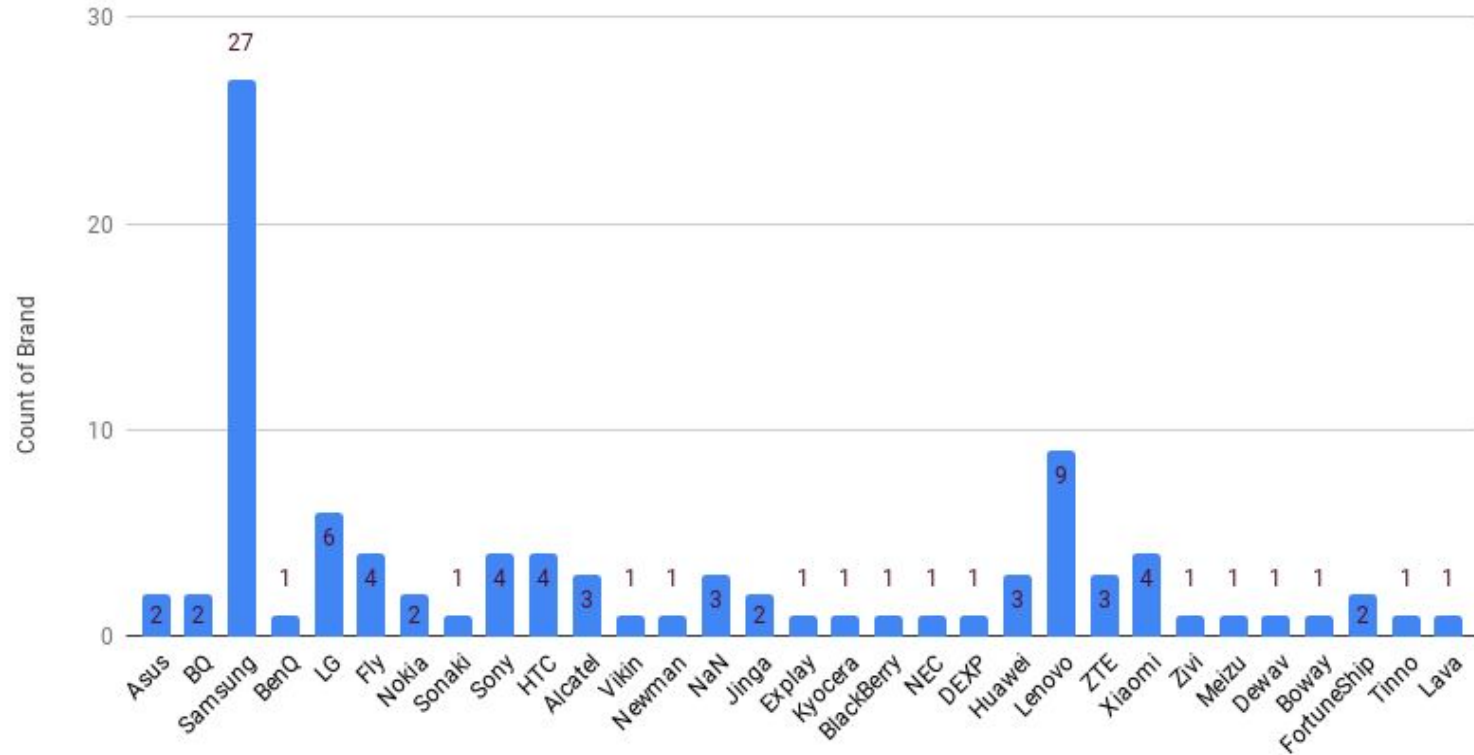
30/07/17 13:06 VISA5880 purchase 200r PSCB.RU Balance: 22529.58r

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

per brand

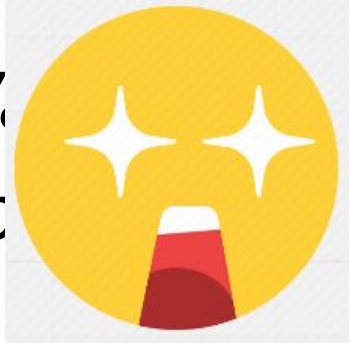


Breakthrough

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

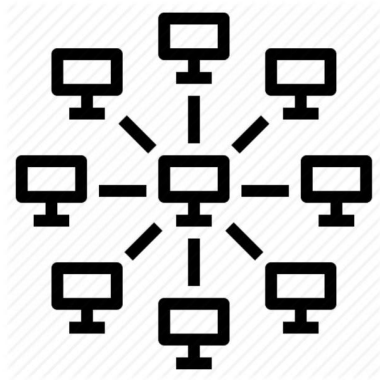
Breakthrough

*From some “information” about Geost,
Veronica V. [redacted] found” a file in
a public web [redacted] was a Skype*



strategy

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

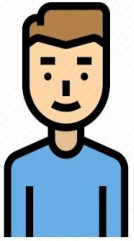


Misspelling and slang words

Brain Teaser

“belka” (“**белка**” in Cyrillic)
stands for ...?

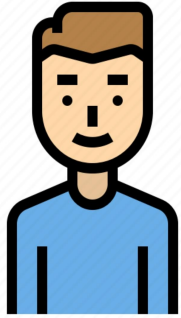
Comrades



powerfaer



mirrexx777



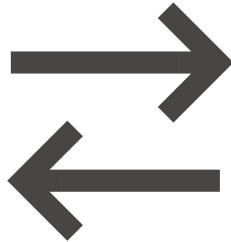
powerfaer

Paying to Mirrexx777

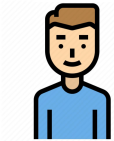
Knows people with money

Exchange money

Online Payment System



Business model

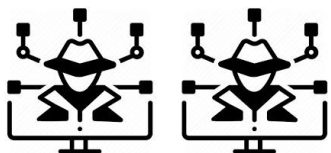


powerfaer



mirrexx777

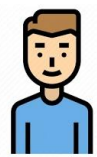
Partnerka



Customers



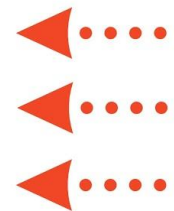
Partnerka



powerfaer



mirrexx777



Target

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**)

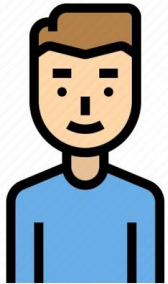
Price per **1,000 installations** 20,000 rubles* (**7,152 CZK / 310 USD**)

* Minus fees

** Check your local black market contracts for more information

Installations in Geost

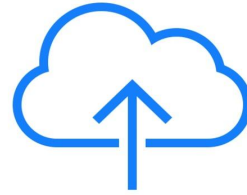
694dea5.apk



powerfaer

mirrexx777

Relation to Geost



694dea5.apk



mirrexx777



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

 @anshiroкова