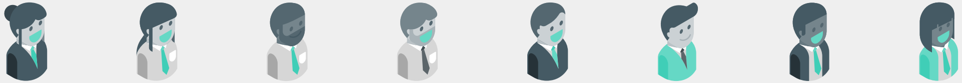
MONEY DOESN'T STINK. CYBERCRIMINAL BUSINESS INSIGHT OF A NEW ANDROID BOTNET

Sebastian Garcia
@eldracote

Anna Shirokova
@anshirokova

Maria Jose Erquiaga
@MaryJo_E

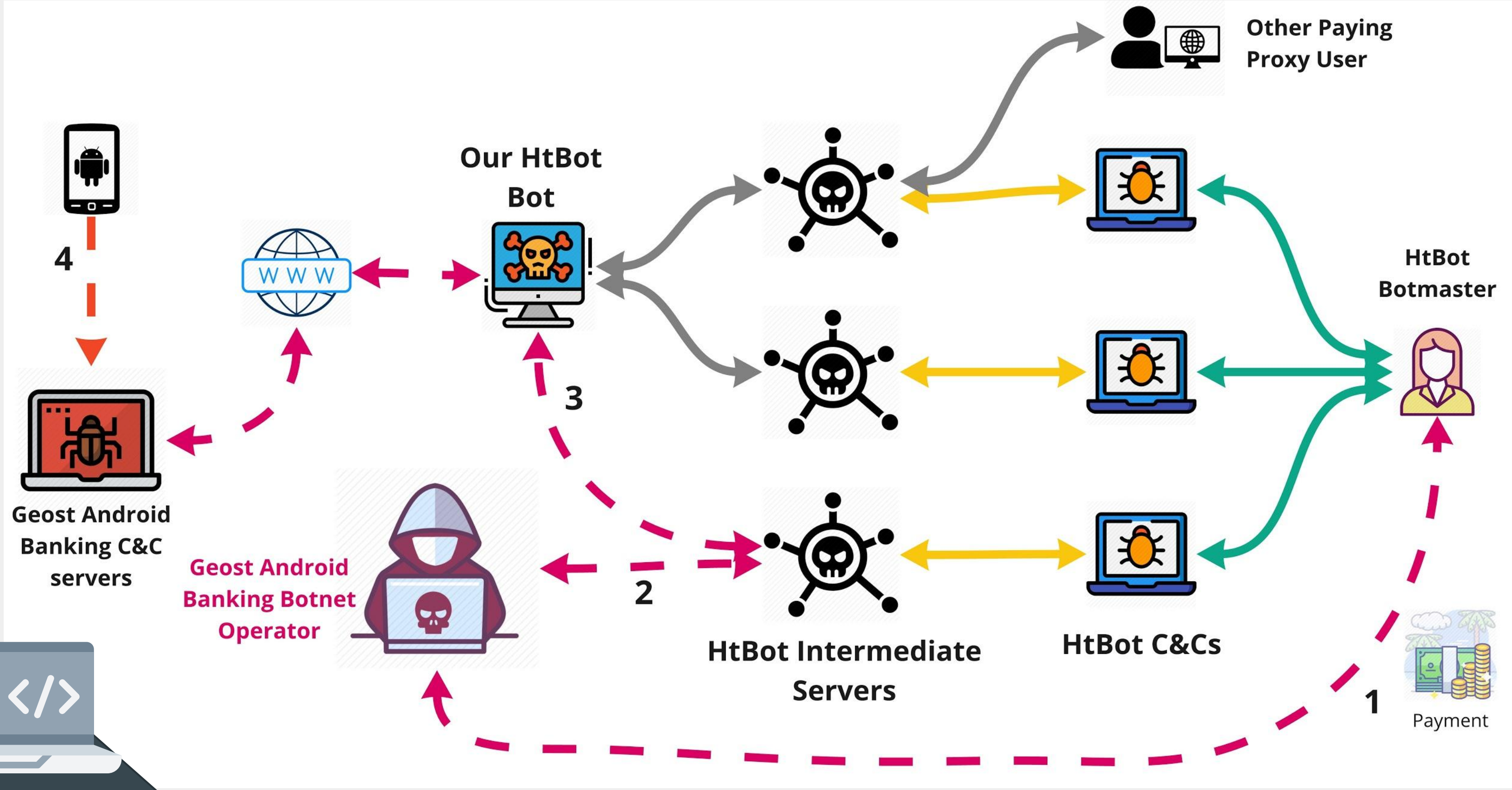
Do attackers care about attacking?



Let’s look at the attackers

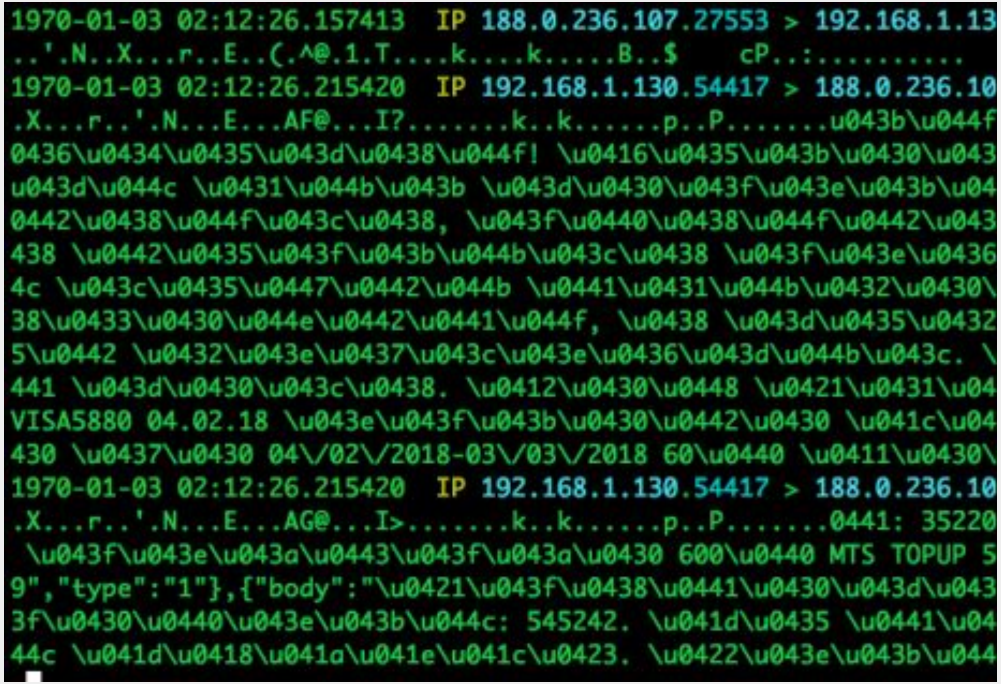
FINDING GEOST

THE DISCOVERY. FROM HTBOT TO GEOST


Other Paying Proxy User
Our HtBot Bot
W W W
4
3
HtBot Botmaster
Geost Android Banking C&C servers
Geost Android Banking Botnet Operator
2
HtBot Intermediate Servers
HtBot C&Cs
1
Payment

CAPTURED THE UNENCRYPTED PATTERN IN HTBOT

- Unencrypted traffic pattern
- Unicode encoding
- Russian language
- List of SMS from a victim



```
1970-01-03 02:12:26.157413  IP 188.0.236.107.27553 > 192.168.1.13
..'.N..X...r..E..(.^@.1.T....k....k.....B..$    cP..:.........
1970-01-03 02:12:26.215420  IP 192.168.1.130.54417 > 188.0.236.10
.X...r..'.N...E...AF@...I?.......k..k......p..P.......u043b\u044f
0436\u0434\u0435\u043d\u0438\u044f! \u0416\u0435\u043b\u0430\u043
u043d\u044c \u0431\u044b\u043b \u043d\u0430\u043f\u043e\u043b\u04
0442\u0438\u044f\u043c\u0438, \u043f\u0440\u0438\u044f\u0442\u043
438 \u0442\u0435\u043f\u043b\u044b\u043c\u0438 \u043f\u043e\u0436
4c \u043c\u0435\u0447\u0442\u044b \u0441\u0431\u044b\u0432\u0430\
38\u0433\u0430\u044e\u0442\u0441\u044f, \u0438 \u043d\u0435\u0432
5\u0442 \u0432\u043e\u0437\u043c\u043e\u0436\u043d\u044b\u043c. \
441 \u043d\u0430\u043c\u0438. \u0412\u0430\u0448 \u0421\u0431\u04
VISA5880 04.02.18 \u043e\u043f\u043b\u0430\u0442\u0430 \u041c\u04
430 \u0437\u0430 04\/02\/2018-03\/03\/2018 60\u0440 \u0411\u0430\
1970-01-03 02:12:26.215420  IP 192.168.1.130.54417 > 188.0.236.10
.X...r..'.N...E...AG@...I>.......k..k......p..P.......0441: 35220
 \u043f\u043e\u043a\u0443\u043f\u043a\u0430 600\u0440 MTS TOPUP 5
9","type":"1"},{"body":"\u0421\u043f\u0438\u0441\u0430\u043d\u043
3f\u0430\u0440\u043e\u043b\u044c: 545242. \u041d\u0435 \u0441\u04
44c \u041d\u0418\u041a\u041e\u041c\u0423. \u0422\u043e\u043b\u044
```

THE UNENCRYPTED PATTERN IN HTBOT

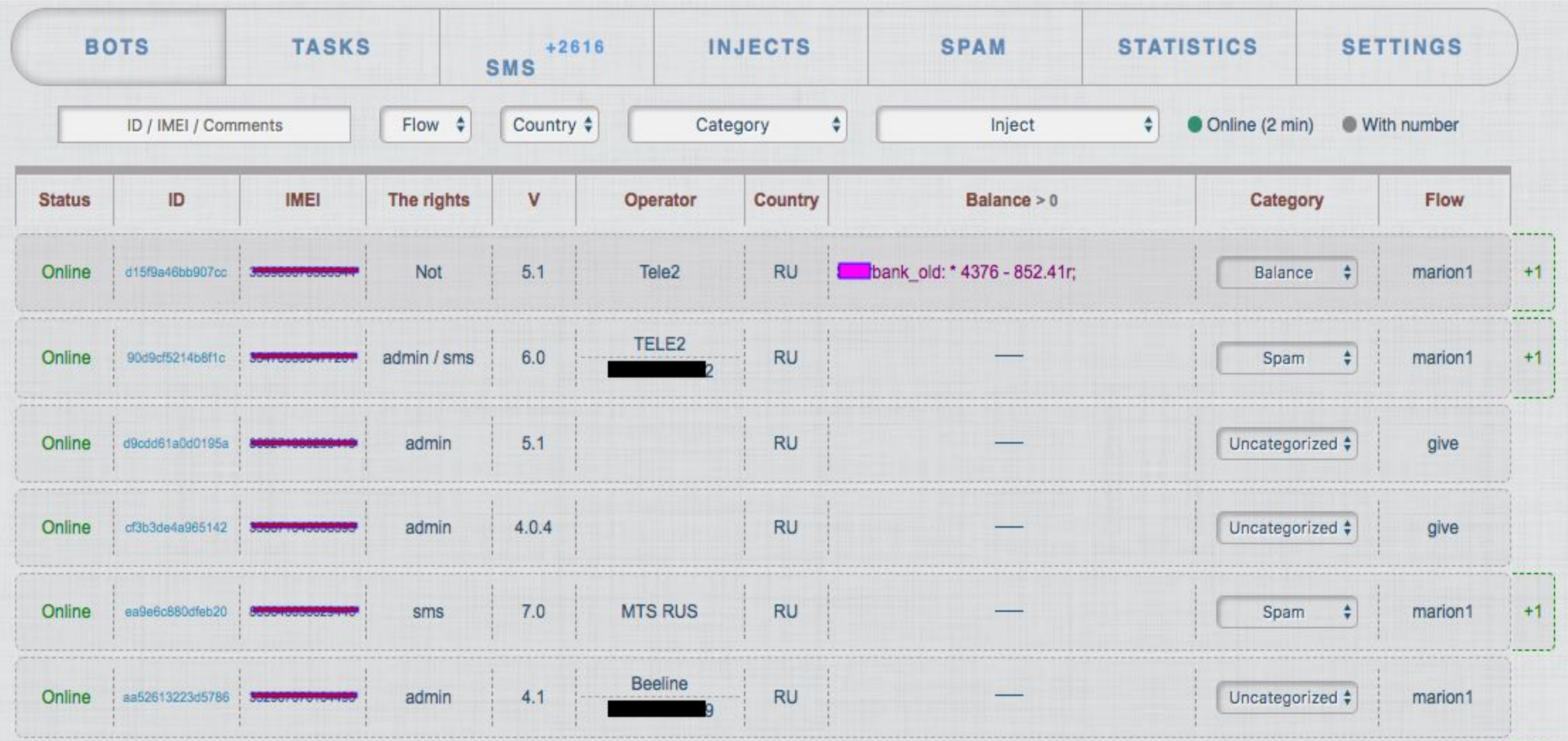
The complete **decoded text** was in **Russian,** the translation from the message is:

“Withdrawal of funds: Platbox (RUB 120.00); password: 321435. Do not disclose the password to ANYONE. Only fraudsters request passwords.”

ACCESS TO THE PANEL

```
GET /geost.php?bid=c5d72910bd8a97aeb2ce

7336fbd78a1f  HTTP/1.1

Host: wgg4ggefwg.ru

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:48.0) Gecko/20100101
Firefox/48.0

Accept-Language: en-US,en;q=0.5

Referrer: http://wgg4ggefwg.ru/geost.php

Cookie: SSE=p6ee96ki2knqrtsahdv84cuj04; __lnkrntdmcvrd=-1
```

GEOST CC PANEL



Status	ID	IMEI	The rights	V	Operator	Country	Balance > 0	Category	Flow	
Online	d15f9a46bb907cc	[redacted]	Not	5.1	Tele2	RU	[redacted] bank_old: * 4376 - 852.41r;	Balance	marion1	+1
Online	90d9cf5214b8f1c	[redacted]	admin / sms	6.0	TELE2 [redacted]	RU	—	Spam	marion1	+1
Online	d9cdd61a0d0195a	[redacted]	admin	5.1		RU	—	Uncategorized	give	
Online	cf3b3de4a965142	[redacted]	admin	4.0.4		RU	—	Uncategorized	give	
Online	ea9e6c880dfeb20	[redacted]	sms	7.0	MTS RUS	RU	—	Spam	marion1	+1
Online	aa52613223d5786	[redacted]	admin	4.1	Beeline [redacted]	RU	—	Uncategorized	marion1	

INFRASTRUCTURE

C&C IPs: 17

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

APKS

Fake applications

Detect emulators

Grant permissions

Obfuscated Code

Fishdom

Update Player

Installing

Avito Photo

VICTIMS

Estimated ~1,000,000 victims in 17 CC
~72,000 per CC

Per victim, >700 SMS per year

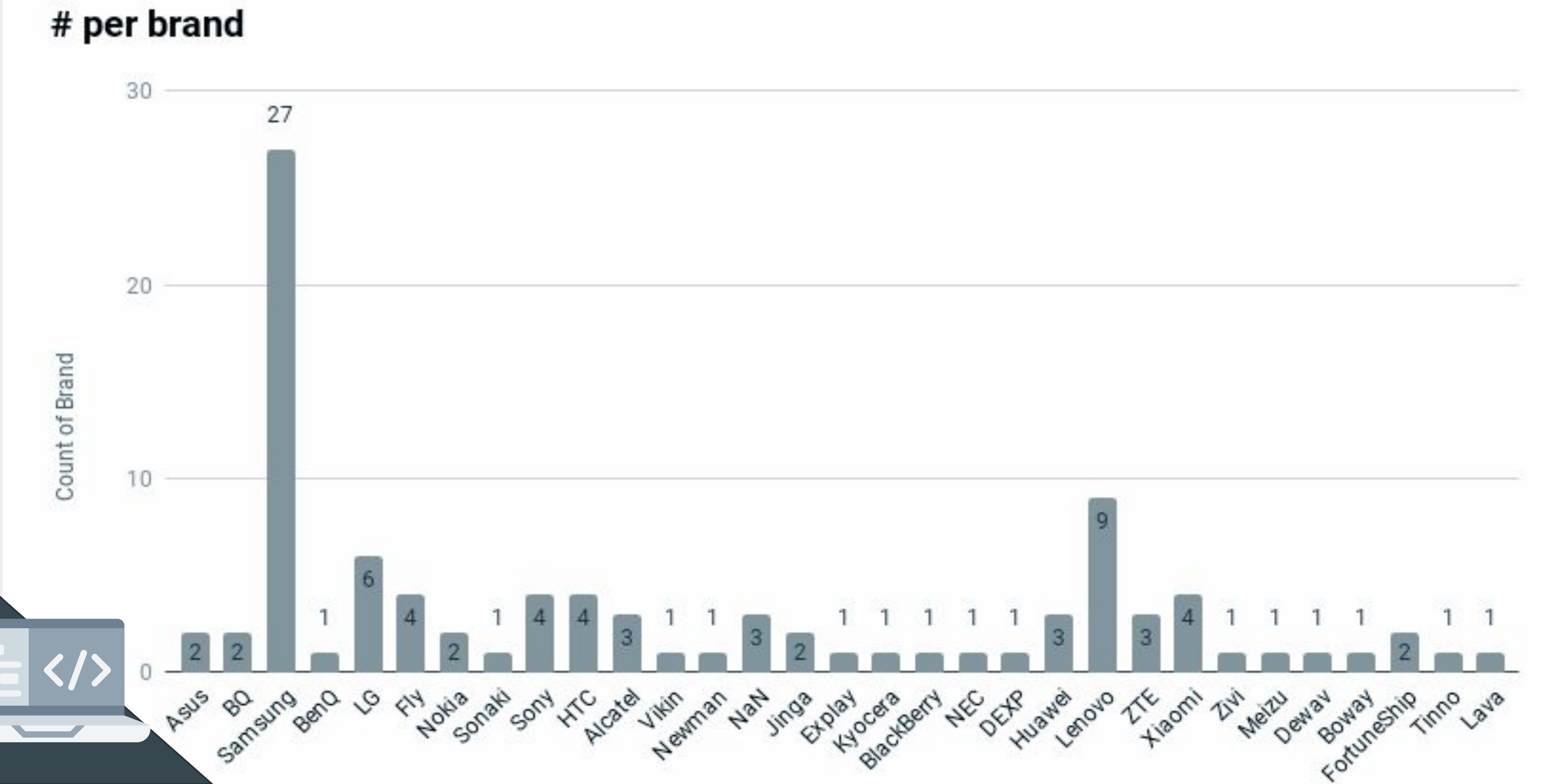
“[redacted]bank[redacted] Online. L[redacted]A SE[redacted]NA Sh translated (a) You 2500.00 RUB”

”Log in [redacted]bank[redacted] Online for Android 07:33 04.03.18.”

”Al[redacted]e R[redacted]ova, pay your mobile one SMS and without commission! To replenish your balance at 100 p. your card, send an SMS to the number 900 with the text 100. [redacted]Bank [redacted] ”

“[redacted] [redacted], we congratulate you on your birthday! Thank you for being with us. your Savings. 2018-02-05”

PHONES SAMPLE FROM VICTIMS



DISCOVERY OF A CYBER GROUP

ONCE UPON A LOG . . .

CHAT LOG

6,200
Lines of text

11 MONTHS
June 2017 to April 2018

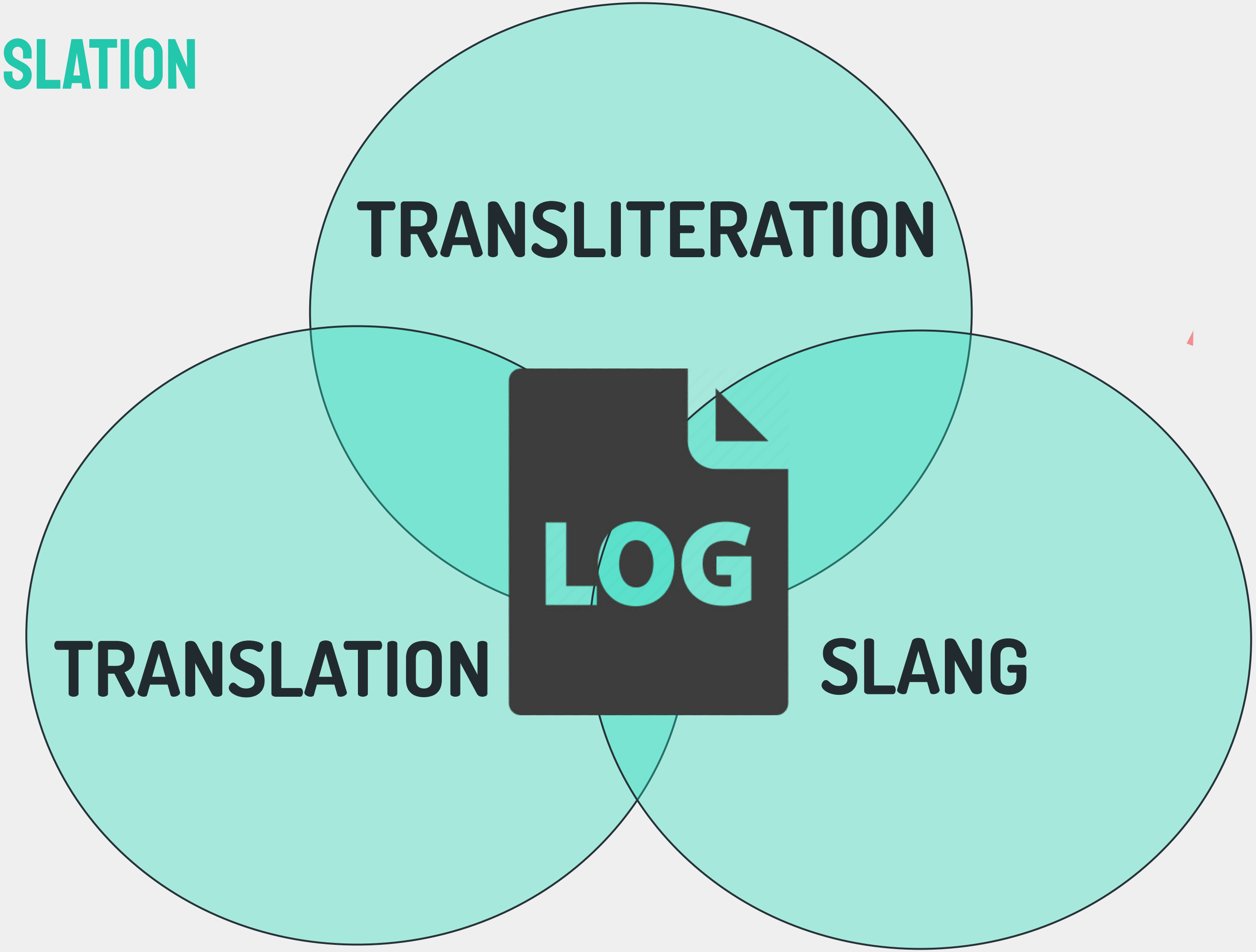
10 PEOPLE
Conversations

- nokola2200
- live:cultrasta
- zloetv
- mixxxail111
- wap.capital
- hjchew58
- mobi.manx
- ca6ootag
- dr.motor
- elkol95

LOG

- powerfaer
- mirrexx777
- sander8804
- maximchik700
- taganchik.ru
- cyberhosting.ru
- dmitrixxx89
- doktorsaitov
- metsof
- ufareg.ru

LOST IN TRANSLATION



TRANSLITERATION

TRANSLATION

SLANG

LOG

CHAT LOG

BELKA

In Cyrillic “**БЕЛКА**” stands for **squirrel**

TELEGA

In Cyrillic “**ТЕЛЕГА**” stands for **cart**

BLIN

In Cyrillic ‘**БЛИН**” stands for **pancake**

SHAVE

In Cyrillic “**Шейв**” stands for

to pay less money for traffic

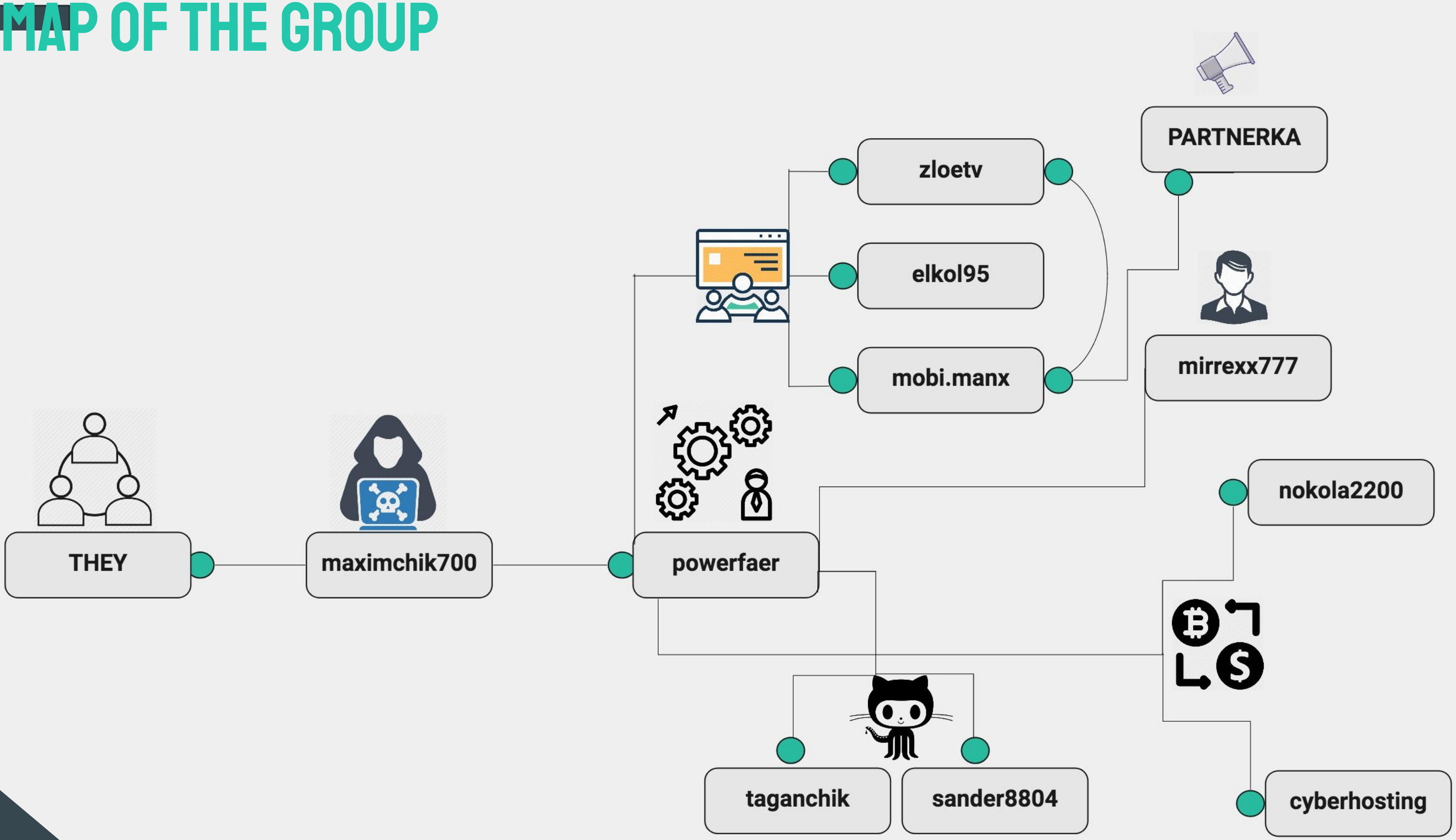
ABON

In Cyrillic “**АБОН**” stands for **subscriber**

PRILA

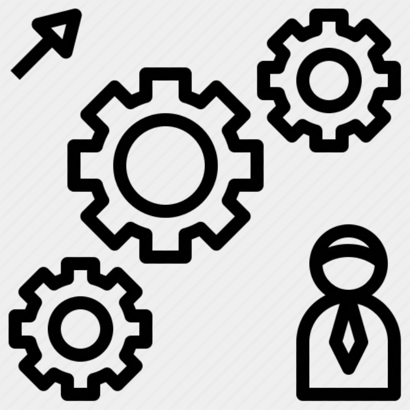
In Cyrillic “**ПРИЛА**” stands for **app**

MAP OF THE GROUP



PUPPETEER

POWERFAER



- Owner of the chat log
- Knows people with money
- Knows money launders and exchangers
- Creates websites

MIRREXX777

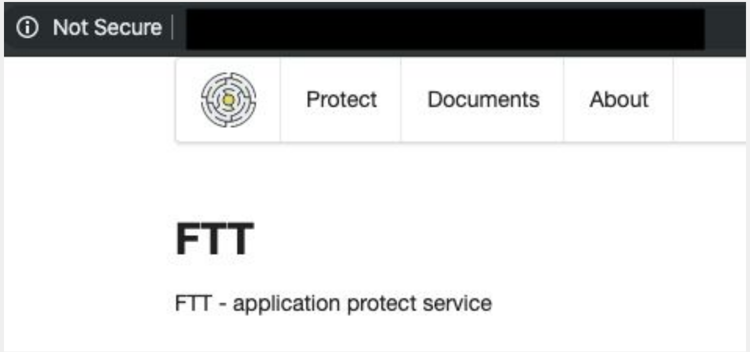
- Used to subcontract others
- Tracking payments
- Prepares APKs
- Creates websites

POWERFAER & MIRREXX777

- Powerfaer is in control of the business. Mirrexx777 also has access to Geost CC
- They both setup domains, and pay developers to create sites
- Mirrexx777 creates APKs, reencrypt APKs (kaspersky detected them)
- Powerfaer: "it seems that the money is coming from the phones credit. Not sure what is going on with the balances."
- Mirrexx777 shared his WebMoney wallet with Powerfaer
- They discuss the people paying as "they". And discuss possible countries of origin

POWERFAER & MIRREXX777

- Time between updates of the APK: 2 days in average
- Domains get blocked by Yandex Browser and Chrome. They do official complains
- New domains for websites created every day (freedns.afraid.org)
- APKs are 'recrypted' in FTT hidden service
- Powerfaer server was hacked

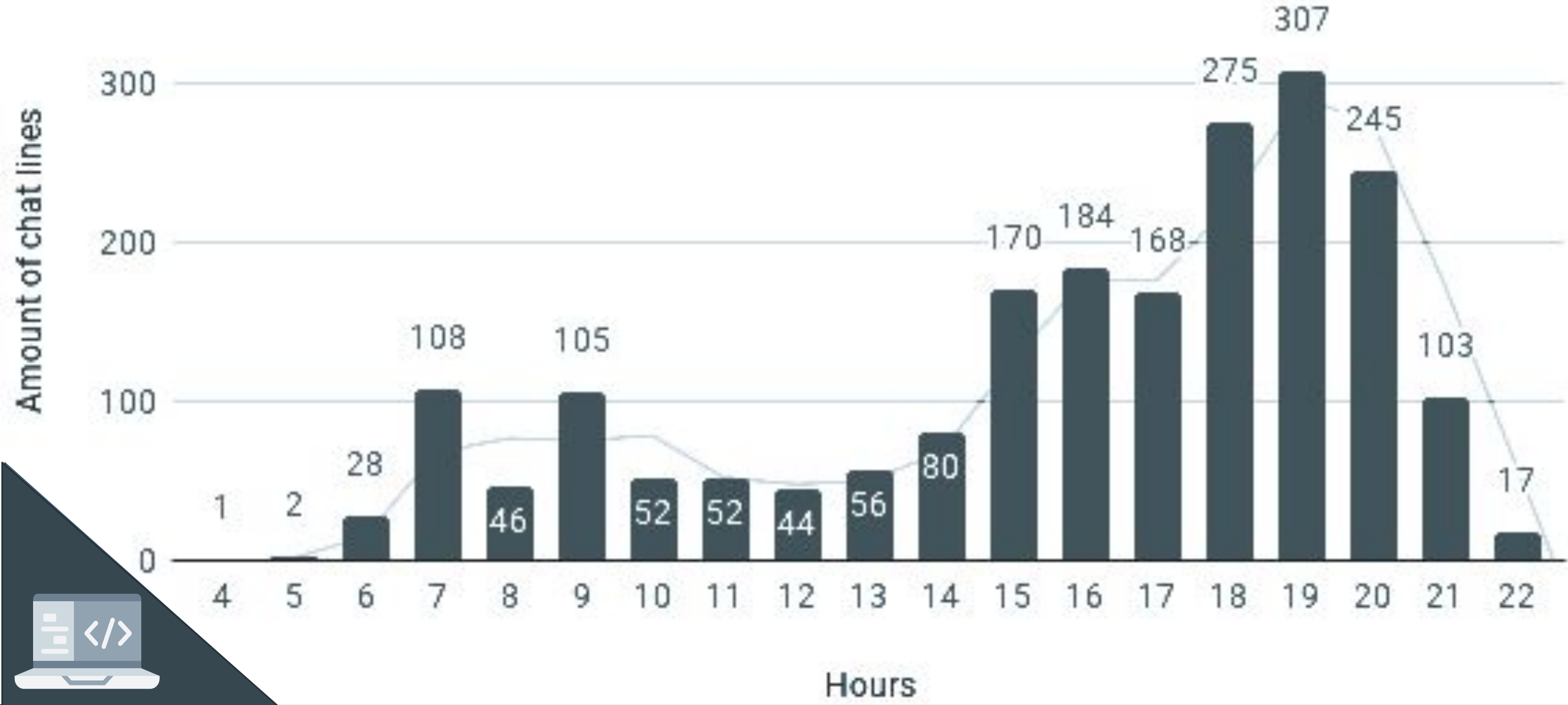


[redacted]

FTT

FTT - application protect service

MOST COMMON CHAT TIME. POWERFAER-MIREXX777



MAXIMCHIK700

Providing encrypted APKs

Hires freelancers for different job types

Searching for advertising in an Android apps

WEB TRAFFIC, PPI

Sends traffic to web subscriptions

Sends traffic to wap click

Works with Partnerka

POWERFAER & MOBI.MANX

- Powerfaer needs traffic from mobi.manx. The calls worked!
- Previous redirections didn’t work.
- Mobi.manx has access to Geost panels too
- From Powerfaer: *“An offer. Their programmer needs a consultation, they want to add click into midlet. The programmer needs to be explained how to do auto-click, how to download these landing pages, or insert some script. So you can get a share from user clicks, plus from the calls and SMS”*

ZLOETV

- Owner of online movie sites
- Has platform for traffic
- Interested in Pay Per Call traffic
- Part of a larger group

“Regarding the app it is going via [name redacted], those people are shady :-(“

ELKOL95

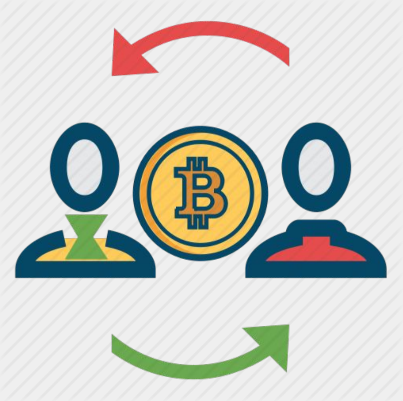
Recruiting webmasters with their websites

Active on russian hacker forum Antichat.ru

Buys Android installs

MONEY EXCHANGERS

NOKOLA2200

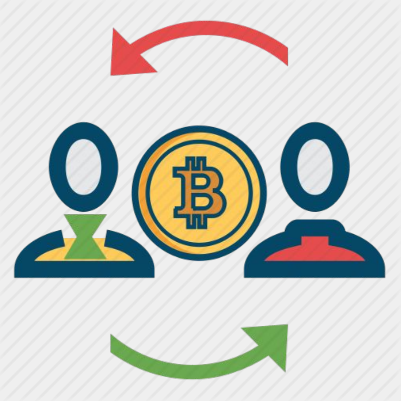


Doesn’t work with banks or legal entities

Active on darkmoney.sg forum for money mules

Charge up to 3% fee for exchange

CYBERHOSTING.RU



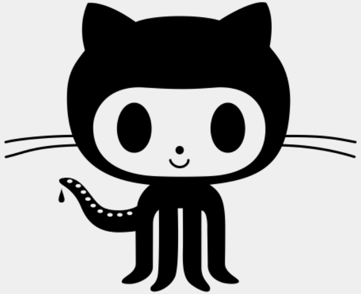
Charges 3-5% more for legal accountant papers

Exchanges cash to BTC

Doesn’t gives loans

DEVELOPERS

TAGANCHIK



PHP and Java developer

CMS datalife engine

Lacks of motivation

POWERFAER & TAGANCHIK. A MOTIVATIONAL TALE

P: “maybe you can still try to pull yourself together?”

“No”

P: “Shame, we had such great plans. Ok, i will inform that money for links would be hand over to another person.”

“No”

P: “ok think it over one more time. Look at all pros and cons. The motivation we have is not working for other boss. At the end of the month i will pay you a good amount of money. Please understand it is important”

“No, i don't want”

P: “Hi, can you just tell me if we are going to continue or not. SO i dont have to bother you every day

“No”

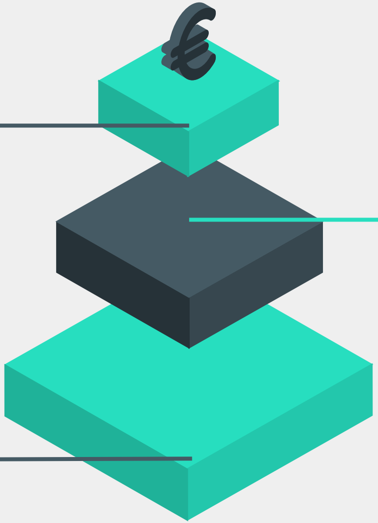
P: “i got it, shame, the money would come in handy. Think it over till 20th,you will change your mind”

“I cant do it“

P: “Of course, you have to force yourself to do it! nothing will happen if you are not going to make an effort. I judge from my experience. i will pay you double”

FINAL THOUGHTS

ATTACKERS PERCEPTION ABOUT ATTACKING



ILLEGAL

INFECTIONS

Malware development
Infection of phones
Attacking others
No tax paying?

PROBABLY NOT ILLEGAL

INFRASTRUCTURE

Fake organizations websites
Mirror a 3rd party website
Premium SMS
Redirection of traffic

NOT ILLEGAL

DEVELOPING

Website creation
Backend development

CONCLUSIONS

Cybercrime is like another business
There is an infrastructure and different people with different roles involved

Hacking is a routine daily job

No response from RuCERT nor Russian Police

5 banks affected. More than 1,000,000 victims

THANKS!

QUESTIONS?

Sebastián García
🐦 @eldracote
sebastian.garcia@agents.fel.cvut.cz
AIC, CTU University

Anna Shirokova
🐦 @anshirokova
shirokova@avast.com
Avast Software

Maria Jose Erquiaga
🐦 @MaryJo_E
maria.erquiaga@aic.fel.cvut.cz
AIC, CTU University