black hat®

EUROPE 2019

DECEMBER 2-5, 2019

EXCEL LONDON, UK

Money Doesn't Stink Cybercriminal Business Insight of A New Android Botnet

Who We Are

avast

Sebastian Garcia
Aposemat Group
AIC, CTU University

Anna Shirokova
Avast Software
www.avast.com

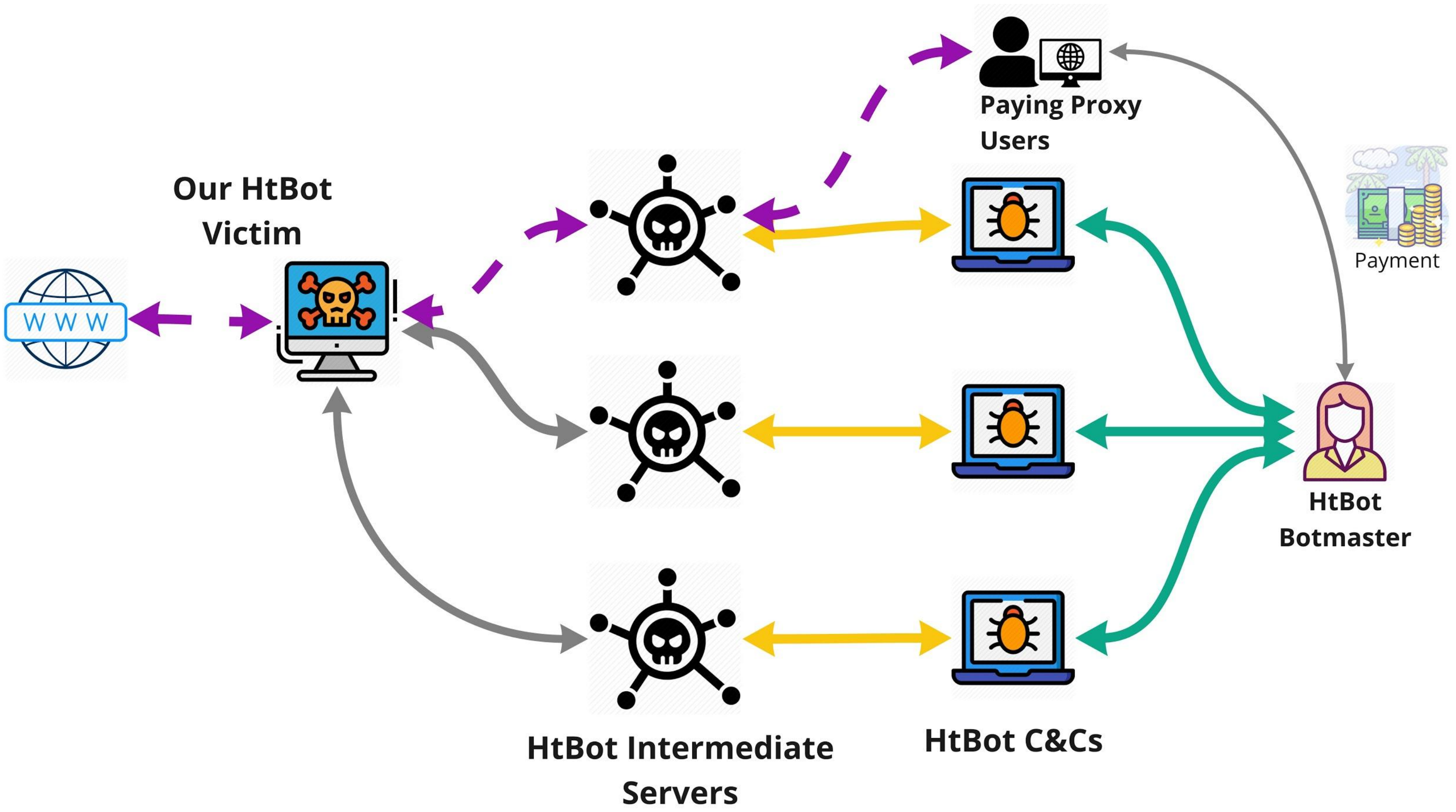
Maria Jose Erquiaga
Aposemat Group
AIC, CTU University

Agenda

- Find Geost (15 mins)
  - Htbot
  - Geost CC
  - Geost Infrastructure
  - APKs
  - Opsec
- Cyber group (20 mins)
  - Finding a chatlog (3mins)
  - Map the group (2mins)
  - Profiles (one slide, 2 profiles?) Check that Anna
- Conclusion - take away (5mins)

Finding Geost

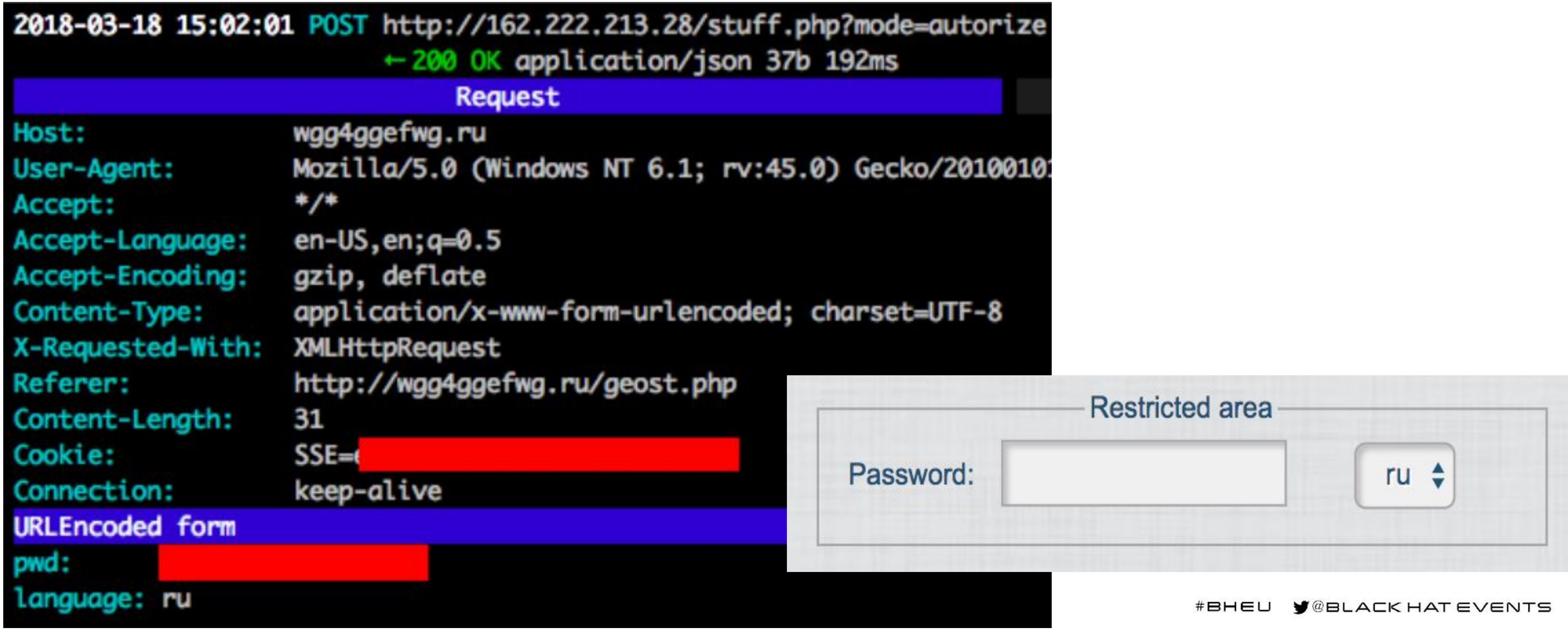
The discovery of Geost



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
```

The CC panel



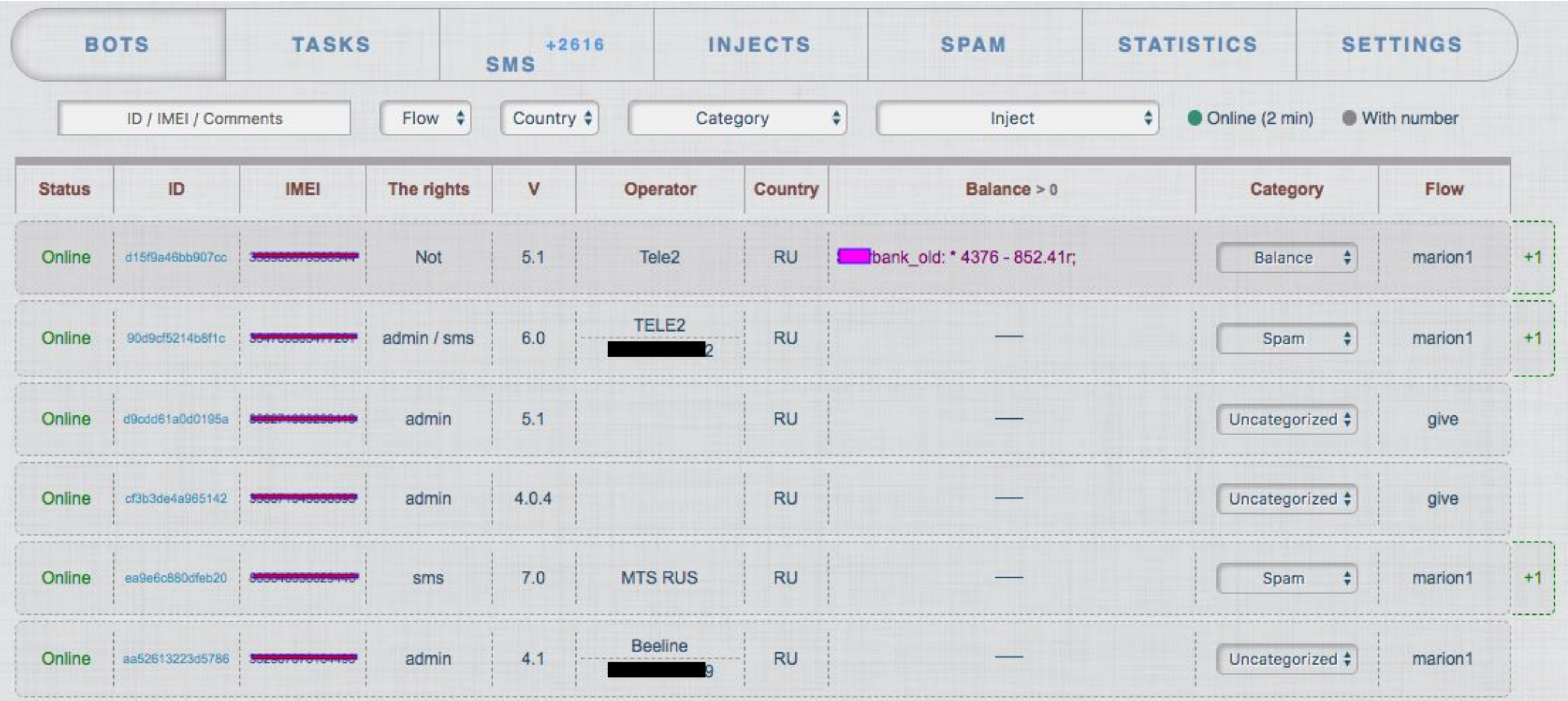
```
2018-03-18 15:02:01 POST http://162.222.213.28/stuff.php?mode=autorize
                          ←200 OK application/json 37b 192ms
                              Request
Host:               wgg4ggefwg.ru
User-Agent:         Mozilla/5.0 (Windows NT 6.1; rv:45.0) Gecko/2010010
Accept:             */*
Accept-Language:    en-US,en;q=0.5
Accept-Encoding:    gzip, deflate
Content-Type:       application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With:   XMLHttpRequest
Referer:            http://wgg4ggefwg.ru/geost.php
Content-Length:     31
Cookie:             SSE=[redacted]
Connection:         keep-alive
URLEncoded form
pwd:     [redacted]
language: ru
```

Restricted area

Password:

ru

Geost 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: 15
    - 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

APKs

- Fake aplicacions
- Code obfuscated
- Permissions:
  - Send and receive sms and mms
  - Read contacts
  - Phone calls
  - Control the system alert window
  - Write external storage
- Detects emulators
- Still analyze them

Games

UpdatePlayer

Installing

Avito Photo

OpSec

- The use of htbot as insecure network
- No traffic encryption
- Hire Developers with low Opsec
- Leaked chat log
- No chat encryption
- No separated personas

Finding the Cyber Group

Discovery of a Chat Log

Our OSINT work discovered a Skype Chat Log in a semi-public web site

The publication circumstances of the log are unclear. Who created it? Why?

Why it was published?

Are there other trackers of these threat? Is the group having an internal

issue?

6,200

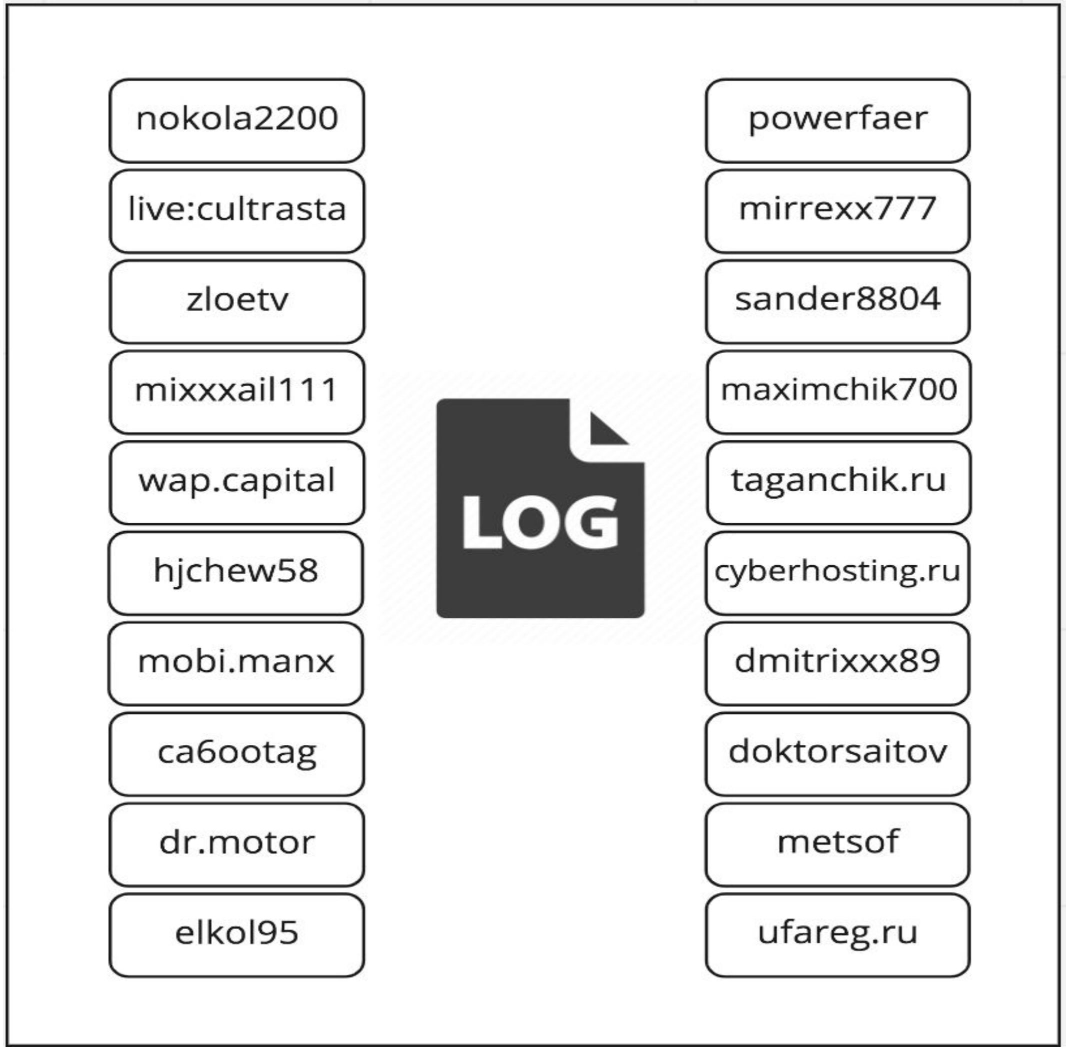
Lines of text

11 Months Long

From June 2017 to April 2018

20 people

Not all of them related to Geost



nokola2200

live:cultrasta

zloetv

mixxxail111

wap.capital

hjchew58

mobi.manx

ca6ootag

dr.motor

elkol95

powerfaer

mirrexx777

sander8804

maximchik700

taganchik.ru

cyberhosting.ru

dmitrixxx89

doktorsaitov

metsof

ufareg.ru

Translation Chat Log

Slang

Misspelling

Transliteration

Translation Chat Log

BELKA

In Cyrillic "**БЕЛКА**"
stands for **squirrel**

TP

In Cyrillic "**ТП**"

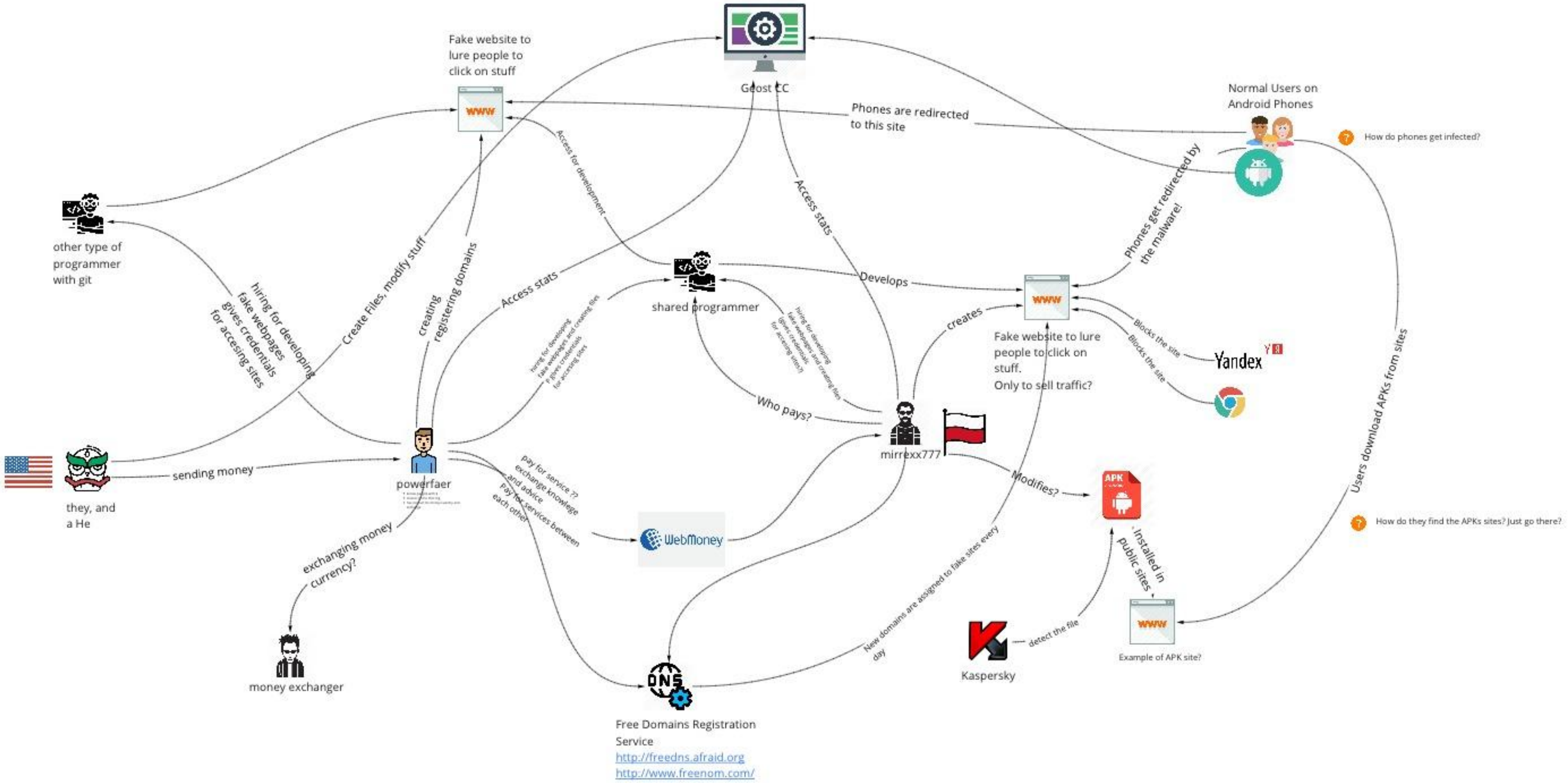
TELEGA

In Cyrillic "**ТЕЛЕГА**"
stands for **cart**

SSH

In Cyrillic "**ССШ**"

Map of the Group



Geost CC

Fake website to lure people to click on stuff

Phones are redirected to this site

Normal Users on Android Phones

How do phones get infected?

Access for development

Access stats

Phones get redirected by the malware!

other type of programmer with git

Create Files, modify stuff

creating registering domains

hiring for developing fake webpages gives credentials for accesing sites

Access stats

shared programmer

Develops

hiring for developing fake webpages and creating files p gives credentials for accesing sites

hiring for developing fake webpages and creating files (gives credentials for accesing sites?)

Who pays?

creates

Fake website to lure people to click on stuff. Only to sell traffic?

Blocks the site

Blocks the site

Yandex

Users download APKs from sites

mirrexx777

Modifies?

they, and a He

sending money

powerfaer

pay for service ?? exchange knowlege and advice

pay for services between each other

WebMoney

exchanging money currency?

money exchanger

New domains are assigned to fake sites every day

Installed in public sites

How do they find the APKs sites? Just go there?

detect the file

Kaspersky

Example of APK site?

Free Domains Registration Service
http://freedns.afraid.org
http://www.freenom.com/

Map of the group: Profiles

Powerfaer

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

Mirrexx777

- Used to subcontract others
- Installing files when Powerfaer asks
- Tracking for what they are getting payed

Social Communications: Powerfaer & Mirexx777

- Main actors in the log
- Both create websites. Mirexx777 also prepares APK
- Powerfaer gives work to Mirexx777 and then pays
- Both use programmers to help them
- They don't believe what they do is much illegal. ***"maybe you have infected files?"***
- They ignore who pays them, and the discuss where are they from: USA?
- They chat from their phones too. (How was log collected?)
- Change APKs every 2days.

Map of the group: Profiles

Taganchick.ru

- Offers php and javascript development
- Has motivation issues to work

Cyberhosting

- Money mule
- Offers bitcoin exchange

Social Communications: Taganchick.ru & Cyberhosting

Taganchick.ru

- Doing developer tasks for Powerfaer
- Often missing deadlines
- Unmotivated to work

Cyberhosting

- Offers money exchange
- Supports legal and illegal accounting

Map of the group: Profiles

maximchik700

- Offers php and javascript development
- Has motivation issues to work

dimitrixxx89

- Offers php and javascript development
- Has motivation issues to work

Map of the group: Profiles

elko95

- Offer Android auto-installs

nokola2020

- Money exchange

Social Communications: powerfaer & taganchick.ru. A motivational Tale

- Taganchick: *“While i was getting ready i have got an idea. what if we tale popular games ehich have more than 1 000 000 downloads, for exmample there would be 100-500 of them. Hire authors and let them re-write or copywrite game descriptions.We will create for them easy text editing.”*
- *Powerfaer: “Ok, it doesnt go this way. You need to pull yourself together and work. Otherwise, we would continue to work for someone else. And make money for other people. Seriously, you need to gather your strenght and start to work, moreover i already started buying links for domain.”*
- *Powerfaer: “Shame, we had such great plans. Ok, i will inform that money for links would be hand over to another person. I think we would not make a website for a week”*
- *Powerfaer: “Hi, maybe we can still do what we agreed on? A few web sites would be enough for the begining. And it is not that much to do. At the end of the month when we finish i will get a good payment.”*
- *Powerfaer: “Tell me so i dont have to keep people for nothing“*
- *Powerfaer: “So think it over one more time. Look at all pros and cons. The motivation we have is not working for other boss (not to work for someone else). At the end of the month i will pay you a good amount of money. Also a motivation. Honestly, lets do it, create a few websites and thats it, then you can relax and the rest of work would be on me. Please undertsand it is important. Ansd its not an option to look for another programmer.”*

Social Communications: powerfaer & taganchick.ru. A motivational Tale

- *Powerfaer: “Hi, can you just tell me if we are going to continue or not. SO i dont have to bother you every day”*
- *T: “Hi, i think no. I cant do it”*
- *Powerfaer: “i got it, shame, the money would come in handy. Think it over till 20th maybe you will change your mind”*
- *Powerfaer: “we just need to finish and thats it. Maybe we can try double payment?. You just need to understand, for these 2 websites we would through away 100k for links and will not have any trouble with money at all. I will ask you tomorrow once again, and if it is affirmative no i will have to look for another programmer. Shame“*
- *T: “Really 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 experiance.”*
- *P: “Alexander, really, if we started together we need to finish it. Because for now this is working and we can earn money. Not every day we are getting around 100k (100 000 rubles) for promotion. If nothing to do it ownt turn out good. Or you have some concerns?“*

Team communications

On 2017-10-18 07:24:07

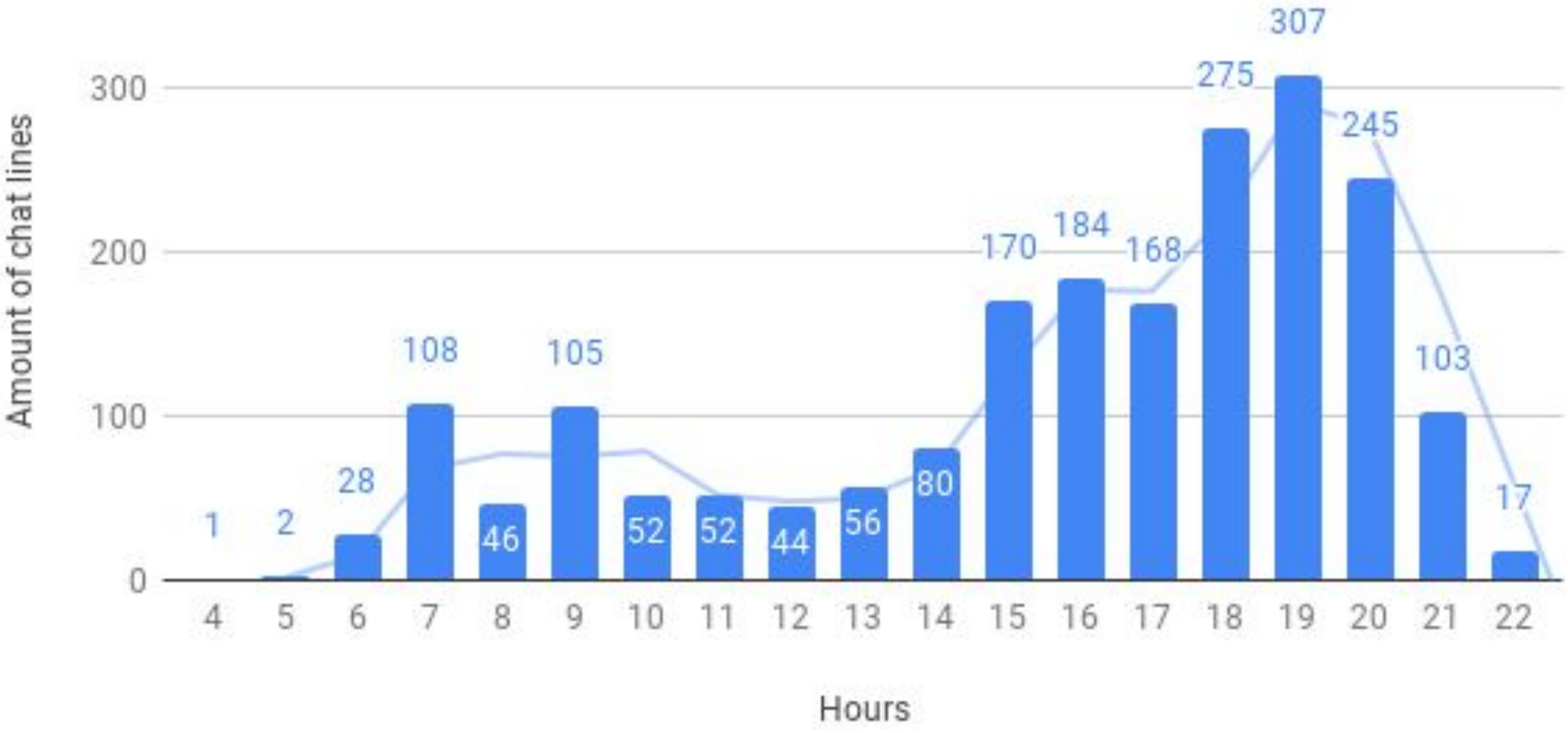
From **powerfaer** to **mirrexx777**:

Title: Statistics

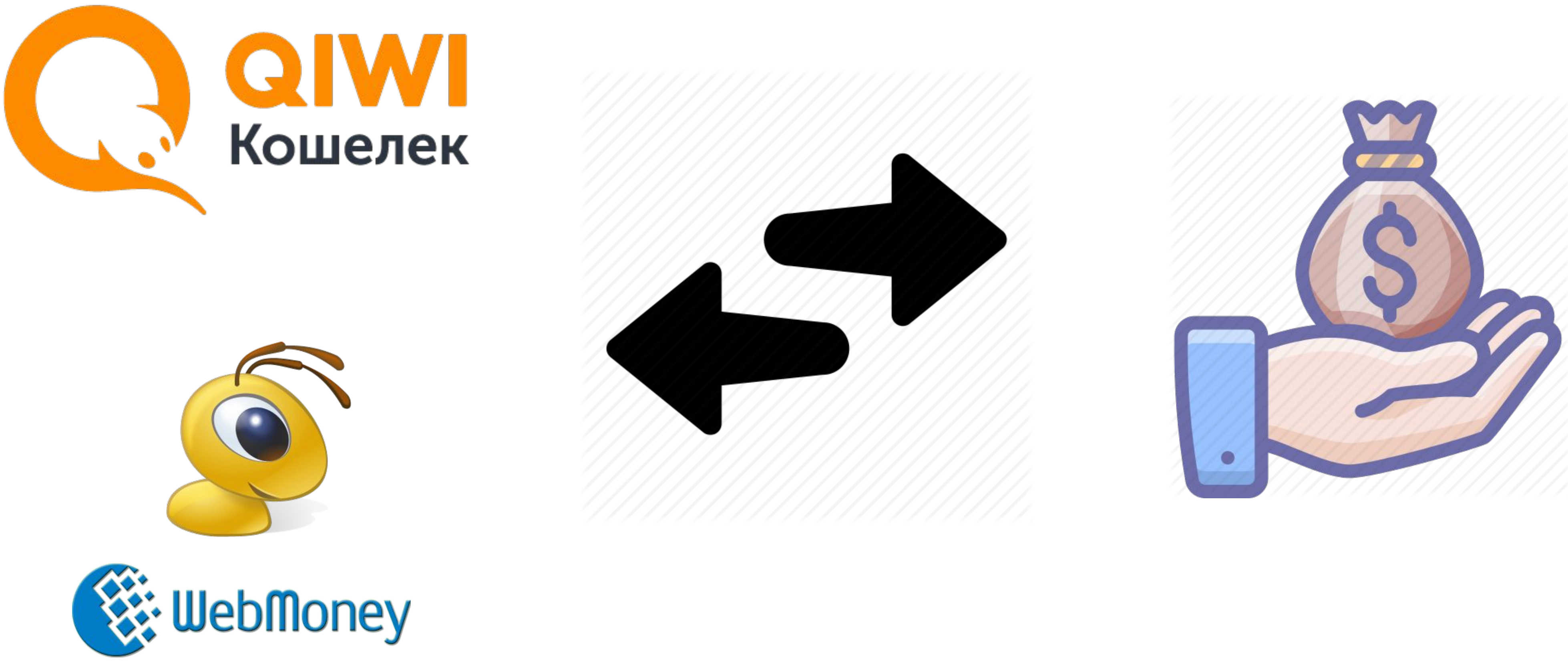
http://2[redacted]e.xyz/stats.php?sid=7NDNI0aercTtwPA

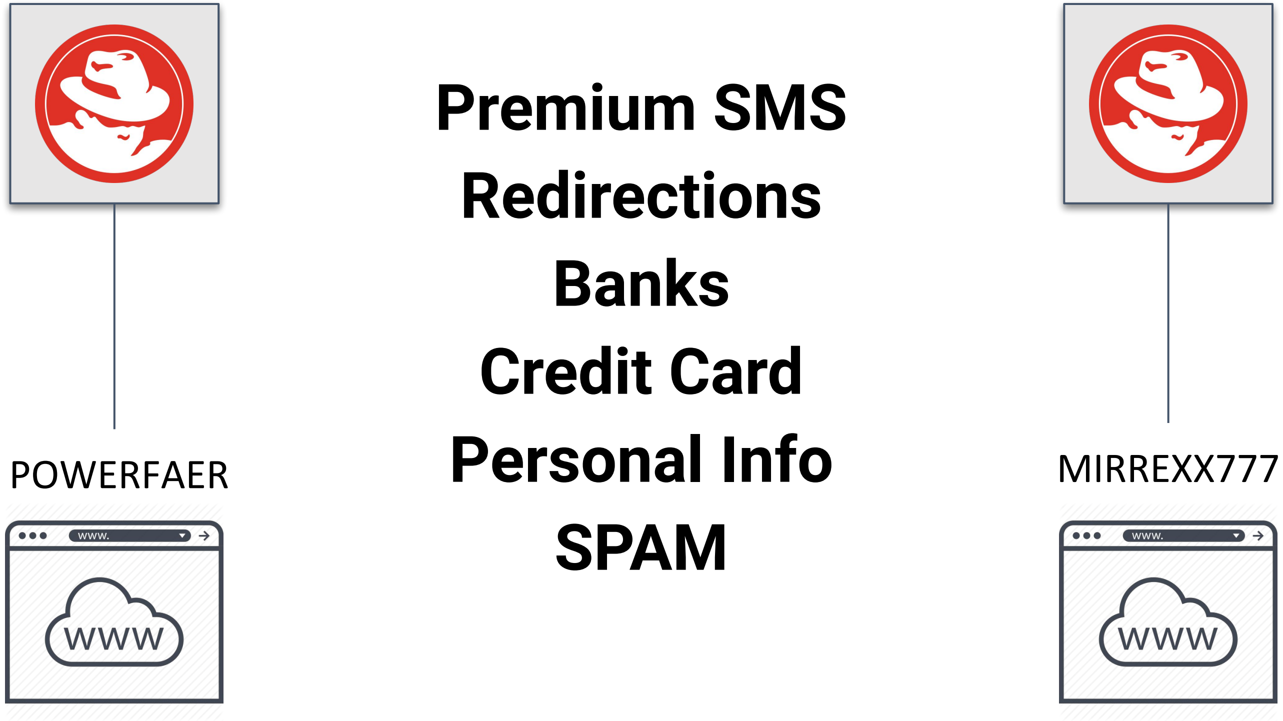
Message: *“Re-crypt, Kaspersky got cleaned”*

Most common chat times



Online Payment system





Premium SMS

Redirections

Banks

Credit Card

Personal Info

SPAM

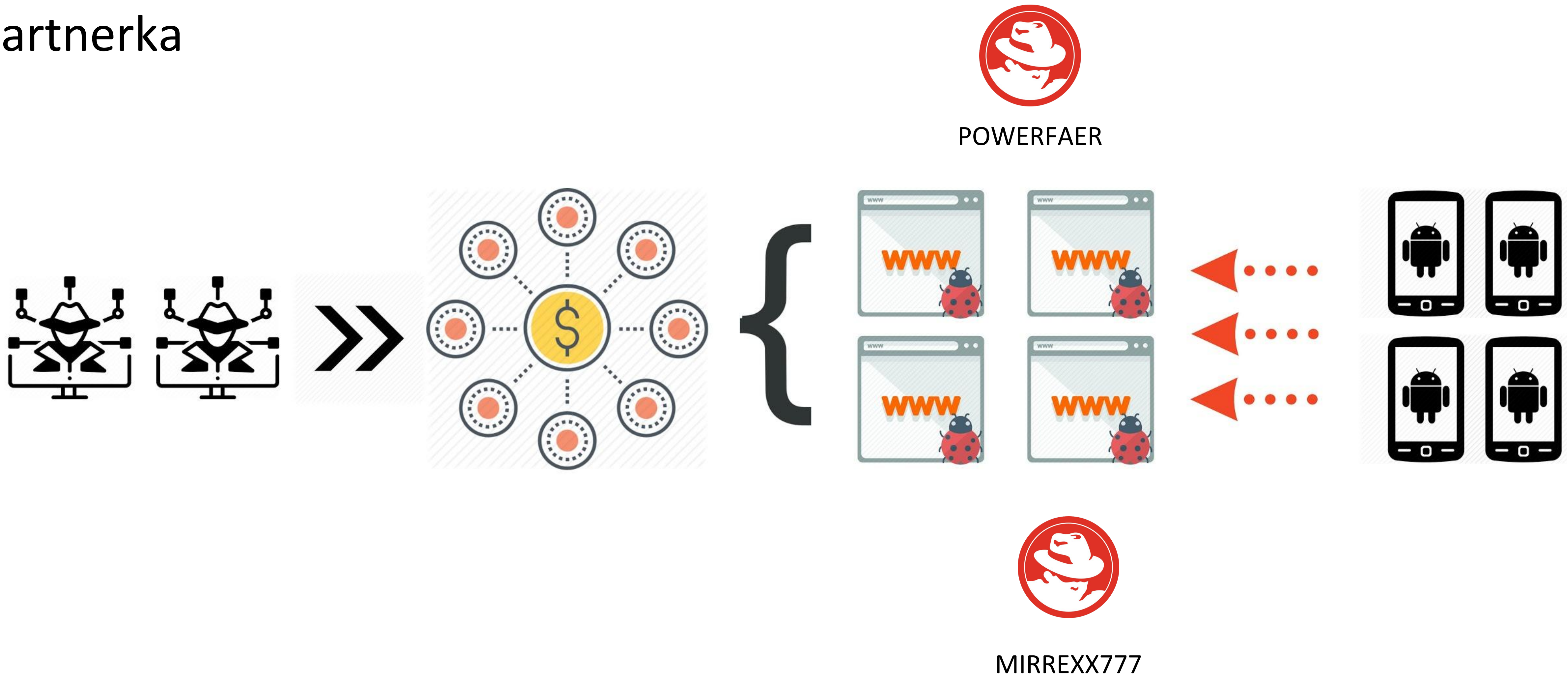
Business Models: APKs

To make purchases on Google Play, you need a ***Google Wallet account****. Google Wallet stores your payment information, transaction history, and is free to use.*

Please fill in all the necessary data to continue.

```
    <string name="name_on_card">"Card holder's name*"</string>
    <string name="card_num">Card number*</string>
    <string name="cvv">CVV*</string>
    <string name="bvb">VBV</string>
    <string name="date">Date expiration(MM/YYYY)*</string>
    <string name="firstname">Name*</string>
    <string name="lastname">Surname*</string>
    <string name="emptyfields">* Please, enter valid information.</string>
```

Partnerka



POWERFAER

MIRREXX777

How much money???

20 rub (0.3 USD)

1 installation

5,000 rub (77 USD)

250 installation

20,000 rub (310 USD)

1,000 installation

Installations in Geost

694dea5.apk

POWERFAER

MIRREXX777

Relation to Geost

Mirexx777

694dea5.apk

http://2[redacted]e.xyz/stats.php?sid=7NDNI0aercTtwPA

Conclusions

- Good OpSec is very hard to **maintain**
- One small mistake compromised a very large part of the operation
- Chat log is unique.
- Where to go now?
    - Social analysis of underground group operation
    - Deeper analysis of the APKs samples

Thank You!

Questions?

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

Anna Shirokova
shirokova@avast.com
@anshirokova

Maria Jose Erquiaga
maria.erquiaga@aic.fel.cvut.cz
@MaryJo_E