



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

Sebastian Garcia
@eldracote

Anna Shirokova
@anshiroкова

Maria Jose Erquiaga
@MaryJo_E



Do attackers care about attacking?





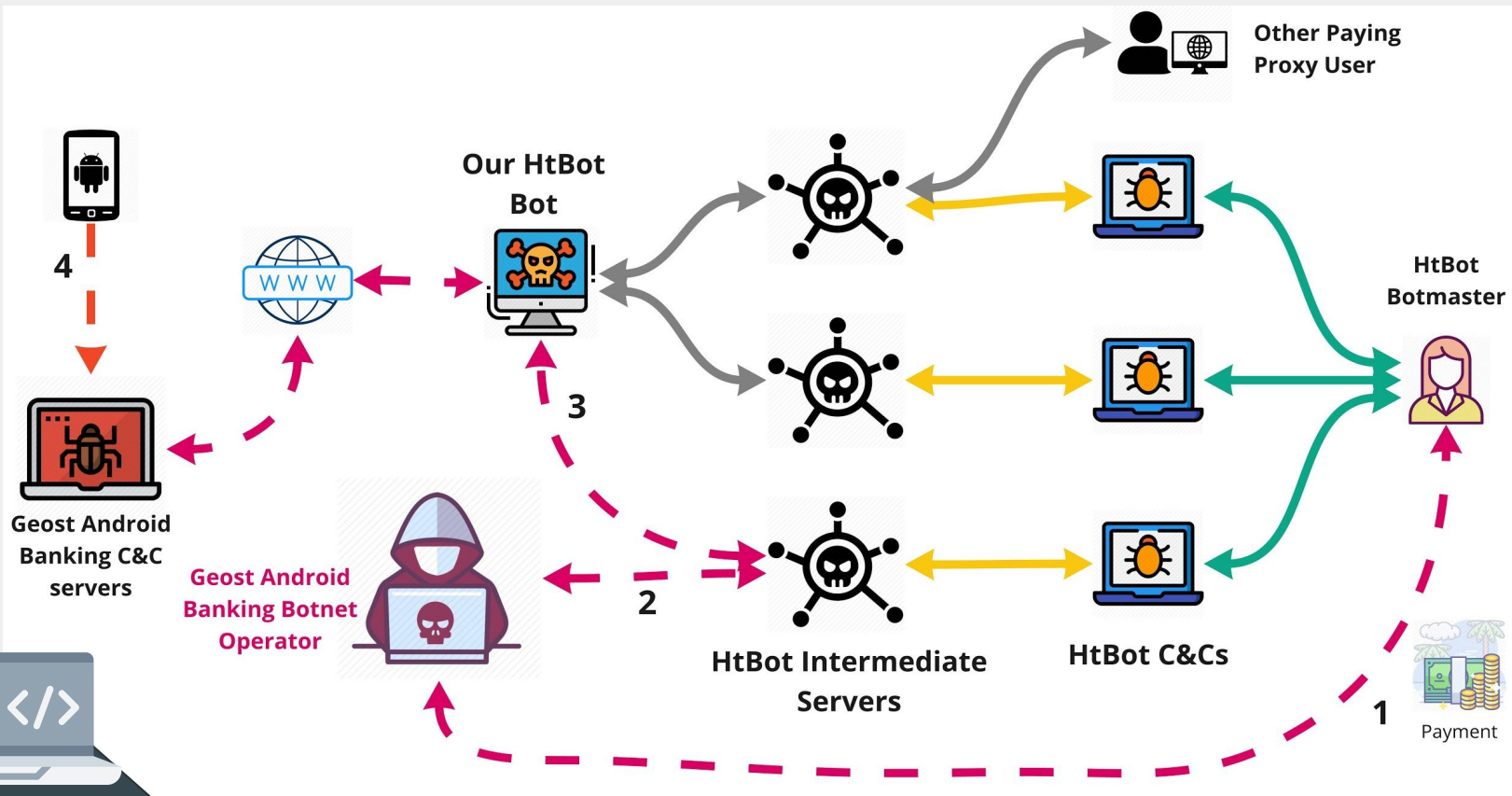
Let's look at the attackers



FINDING GEOST



THE DISCOVERY. FROM HTBOT TO GEOST



CAPTURED THE UNENCRYPTED PATTERN IN HTBOT

Unencrypted traffic pattern

Unicode encoding

Russian language

List of SMS from a victim

[illegible]

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**



GHOST CC PANEL

BOTS

TASKS

SMS+2616

INJECTS

SPAM

STATISTICS

SETTINGS

ID / IMEI / Comments

Flow

Country

Category

Inject

Online (2 min)

With number

Status	ID	IMEI	The rights	V	Operator	Country	Balance > 0	Category	Flow
Online	d15f9a46bb907cc		Not	5.1	Tele2	RU	bank_old: * 4376 - 852.41r;	Balance	marion1+1
Online	90d9cf5214b8f1c		admin / sms	6.0	TELE2	RU		Spam	marion1+1
Online	d9cdd61a0d0195a		admin	5.1		RU		Uncategorized	give
Online	cf3b3de4a965142		admin	4.0.4		RU		Uncategorized	give
Online	ea9e6c980df6b20		sms	7.0	MTS RUS	RU		Spam	marion1+1
Online	aa52613223d5786		admin	4.1	Beeline	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



Grant permissions



Detect emulators



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

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

“Log in ■■bank■■ Online for Android 07:33 04.03.18.”

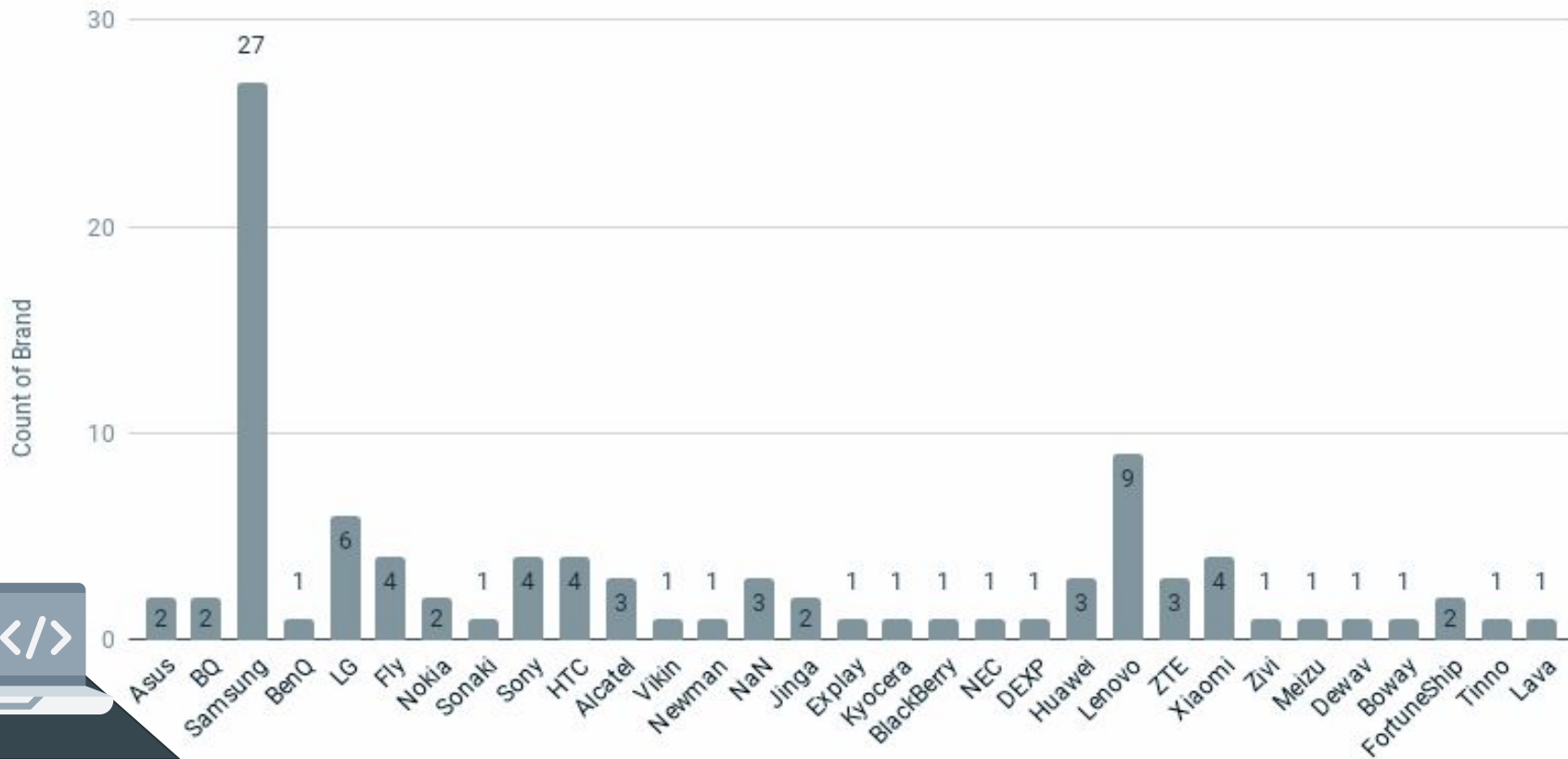
“Al■■■■e R■■ova, pay your mobile one SMS and without commission! To replenish your balance at 100 p. your card, send an SMS to the number 900 with the text 100. ■■■■■Bank ■■■”

“■■■■■■■■, we congratulate you on your birthday! Thank you for being with us. your Savings.

2018-02-05”

PHONES SAMPLE FROM VICTIMS

per brand



DISCOVERY OF A CYBER GROUP



ONCE UPON A LOG . . .



CHAT LOG



6,200

Lines of text



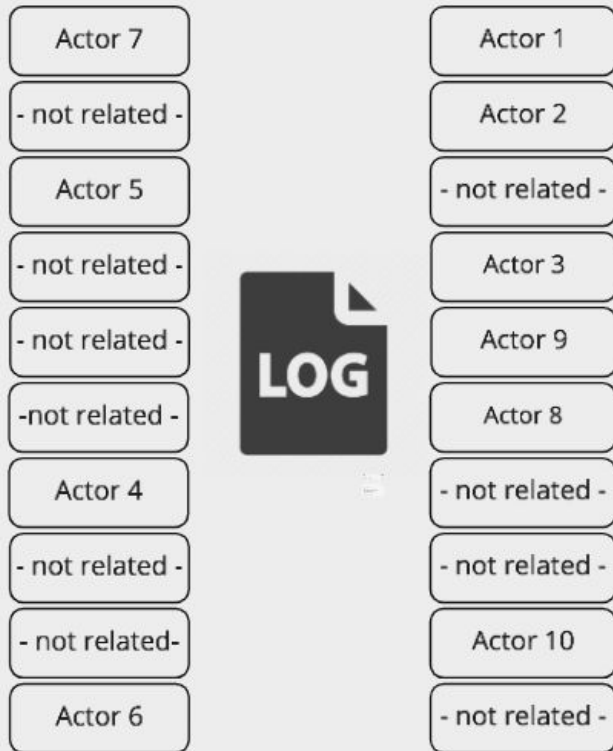
11 MONTHS

June 2017 to April 2018

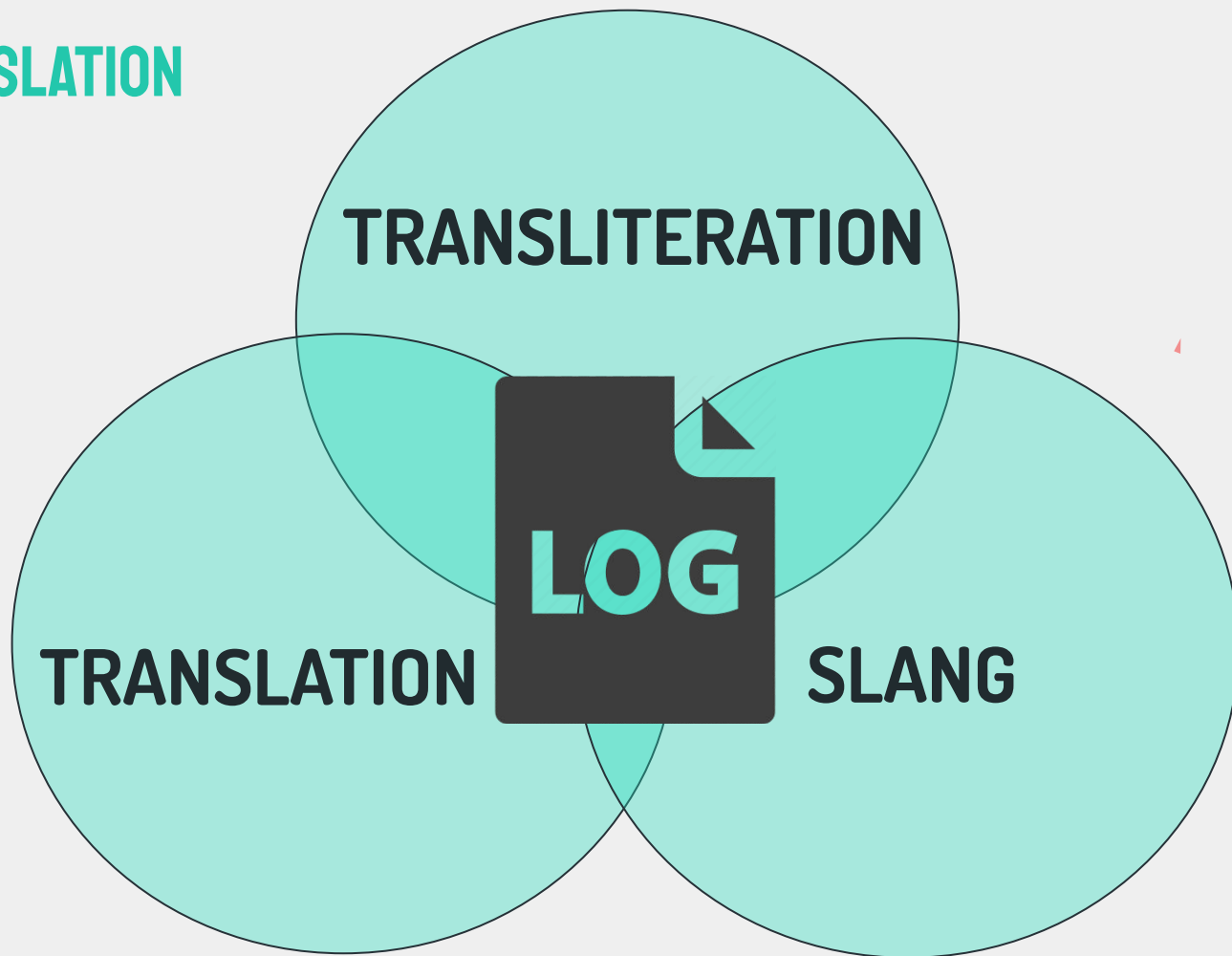


10 PEOPLE

Conversations



LOST IN TRANSLATION



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

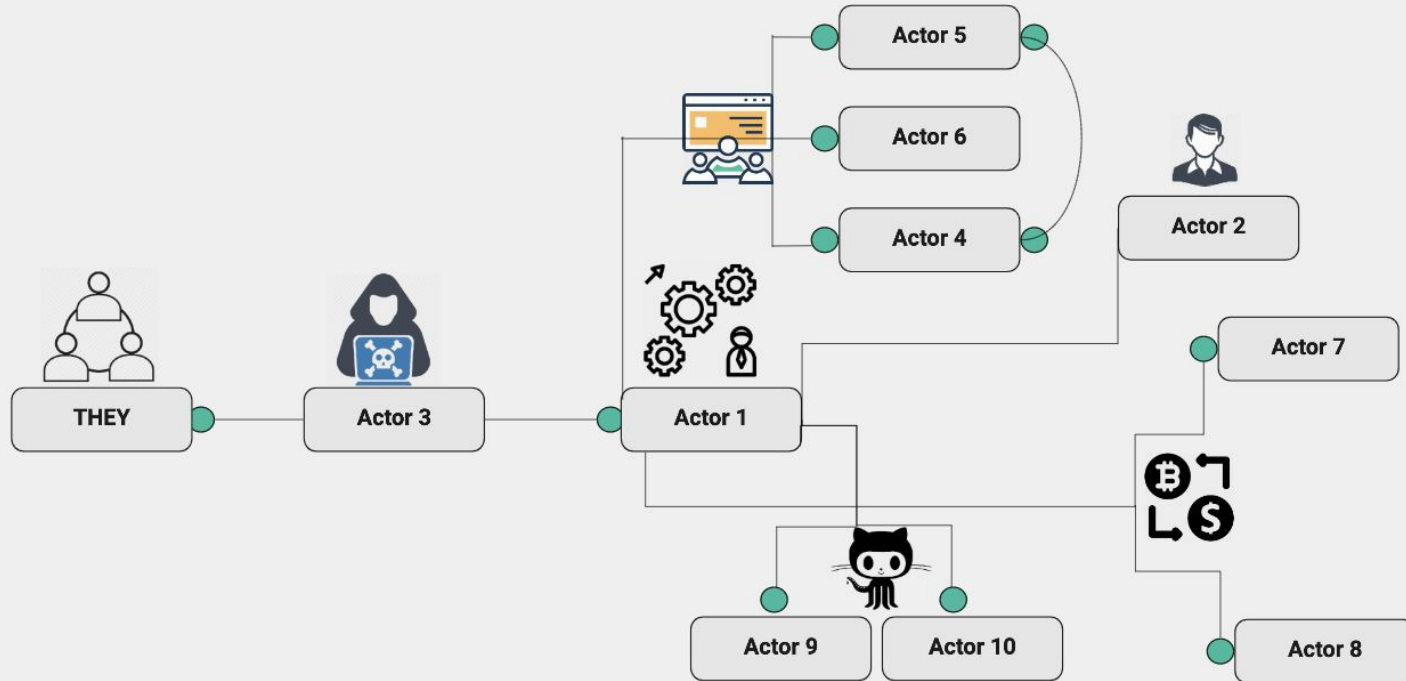
In Cyrillic “**АБОН**” stands for **subscriber**

PRILA

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



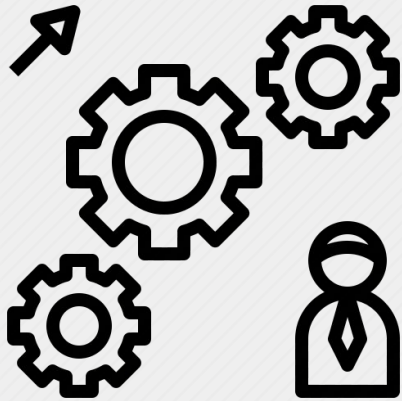
MAP OF THE GROUP



PUPPETEER



ACTOR I



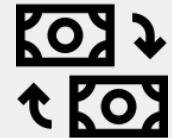
Owner of the chat log



Knows people with money



Knows money launders and exchangers



Creates websites



ACTOR 2



Used to subcontract others



Tracking payments



Prepares APKs



Creates websites



ACTOR 1 & ACTOR 2



Actor 1 is in control of the business. Actor 2 also has access to Geost CC



They both setup domains, and pay developers to create sites



Actor 2 creates APKs, reencrypt APKs (kaspersky detected them)



Actor 1 : “it seems that the money is coming from the phones credit. Not sure what is going on with the balances.”



Actor 2 shared his WebMoney wallet with Actor 1



They discuss the people paying as “they”. And discuss possible countries of origin



ACTOR 1 & ACTOR 2



Time between updates of the APK: 2 days in average



Domains get blocked by Yandex Browser and Chrome. They do official complains



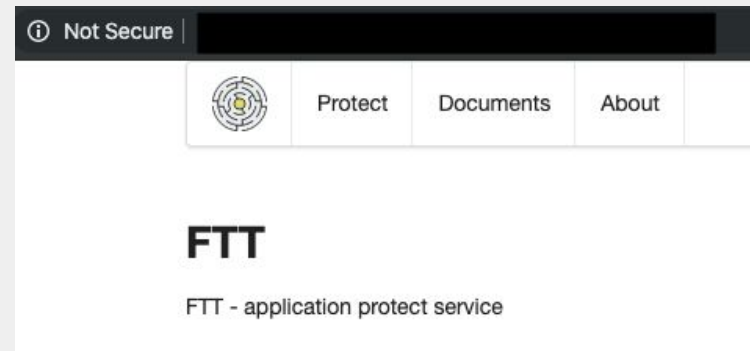
New domains for websites created every day (freedns.afraid.org)



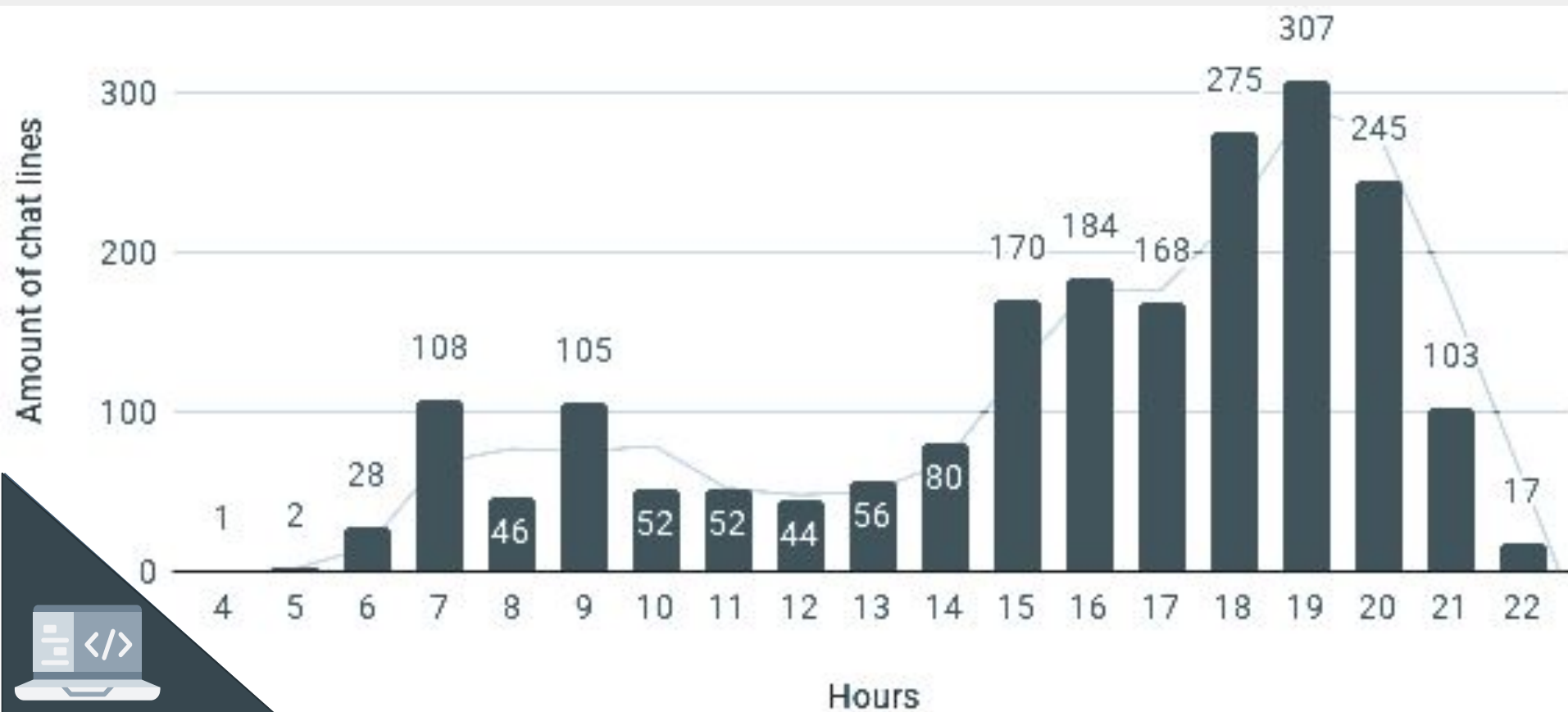
APKs are 'recrypted' in FTT hidden service



Actor 1 server was hacked



MOST COMMON CHAT TIME. ACTOR 1 - ACTOR 2



ACTOR 3



Providing encrypted APKs



Hires freelancers for different job types



Searching for advertising in an Android apps



WEB TRAFFIC, PPI



ACTOR 4



Sends traffic to web subscriptions



Sends traffic to wap click



Works with Partner 1



ACTOR 1 & ACTOR 4



Actor 1 needs traffic from Actor 4. The calls worked!



Previous redirections didn't work.



Actor 4 has access to Geost panels too



From Actor 1: *"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"*



ACTOR 5



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 :-["



ACTOR 6



Recruiting webmasters with their websites



Active on russian hacker forum Antichat.ru



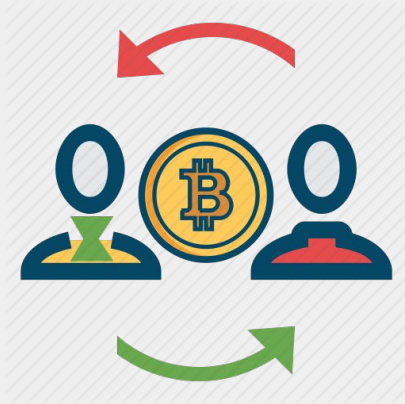
Buys Android installs



MONEY EXCHANGERS



ACTOR 7



Doesn't work with banks or legal entities



Active on darkmoney.sg forum for money mules



Charge up to 3% fee for exchange



ACTOR 8



Charges 3-5% more for legal accountant papers



Exchanges cash to BTC



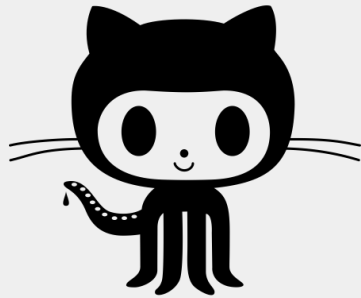
Doesn't give loans



DEVELOPERS



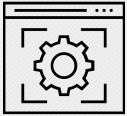
ACTOR 9



PHP and Java developer



CMS datalife engine



Lacks of motivation



ACTOR 1 & ACTOR 9. A MOTIVATIONAL TALE

Actor 1: “maybe you can still try to pull yourself together?”

“No”

Actor 1: “Shame, we had such great plans. Ok, i will inform that money for links would be hand over to another person.”

“No”

Actor 1: “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”

Actor 1: “Hi, can you just tell me if we are going to continue or not. SO i dont have to bother you every day

“No”

Actor 1: “i got it, shame, the money would come in handy. Think it over till 20th,you will change your mind”

“I cant do it”

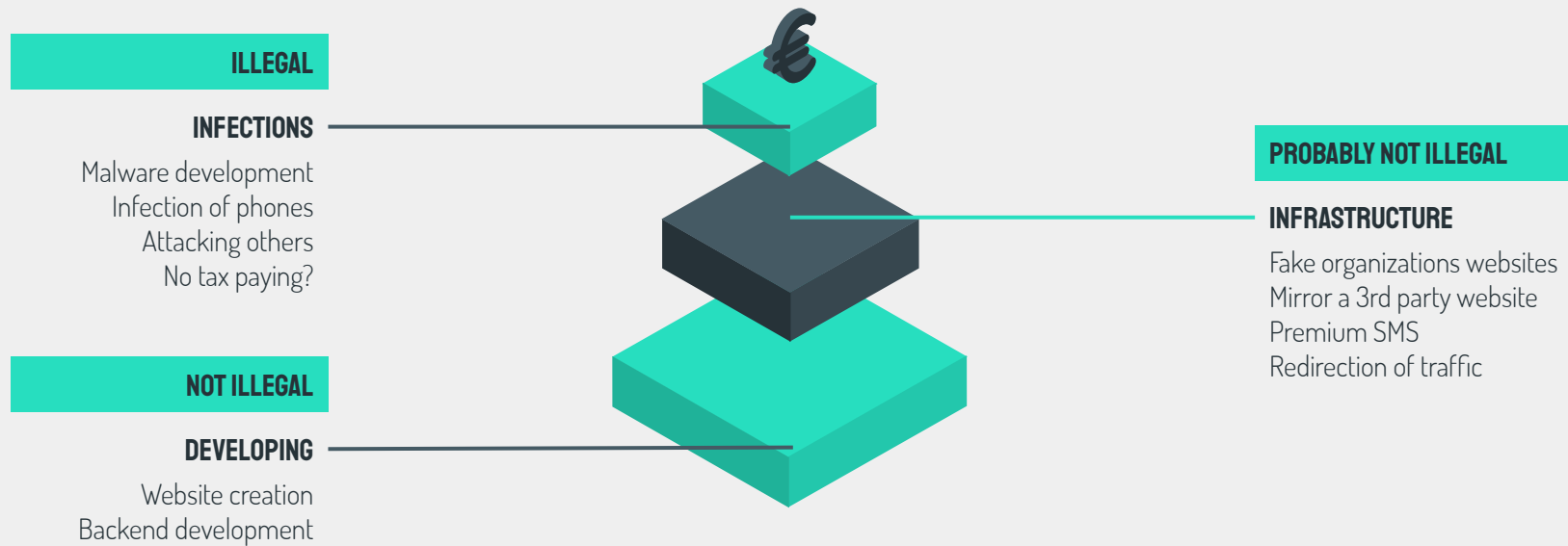
Actor 1: “Of course, you have to force yourself to do it! nothing will happen if you are not going to make an effort. I judge from my experience. i will pay you double”



FINAL THOUGHTS



ATTACKERS PERCEPTION ABOUT ATTACKING



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

 @anshiroкова

shirokova@avast.com

Avast Software

Maria Jose Erquiaga

 @MaryJo_E

maria.erquiaga@aic.fel.cvut.cz

AIC, CTU University