We know what you did this summer: Android Banking Trojan exposing its sins in the cloud

Siegfried Rasthofer (TU Darmstadt / CASED)
Eric Bodden (TU Darmstadt / Fraunhofer SIT)
Carlos Castillo (Intel Security)
Alex Hinchliffe (Intel Security)

Stephan Huber (Fraunhofer SIT)

Siegfried Rasthofer

- 3rd year PhD-Student at TU Darmstadt
- Research interest in Static-/dynamic code analyses
- Found 2 AOSP exploits, various App security vulnerabilities

Prof. Dr. Eric Bodden

- Professor at TU Darmstadt
- Research interest in Static-/dynamic code analyses
- Heading the Secure Software Engineering Group at Fraunhofer SIT and Technische Universität Darmstadt

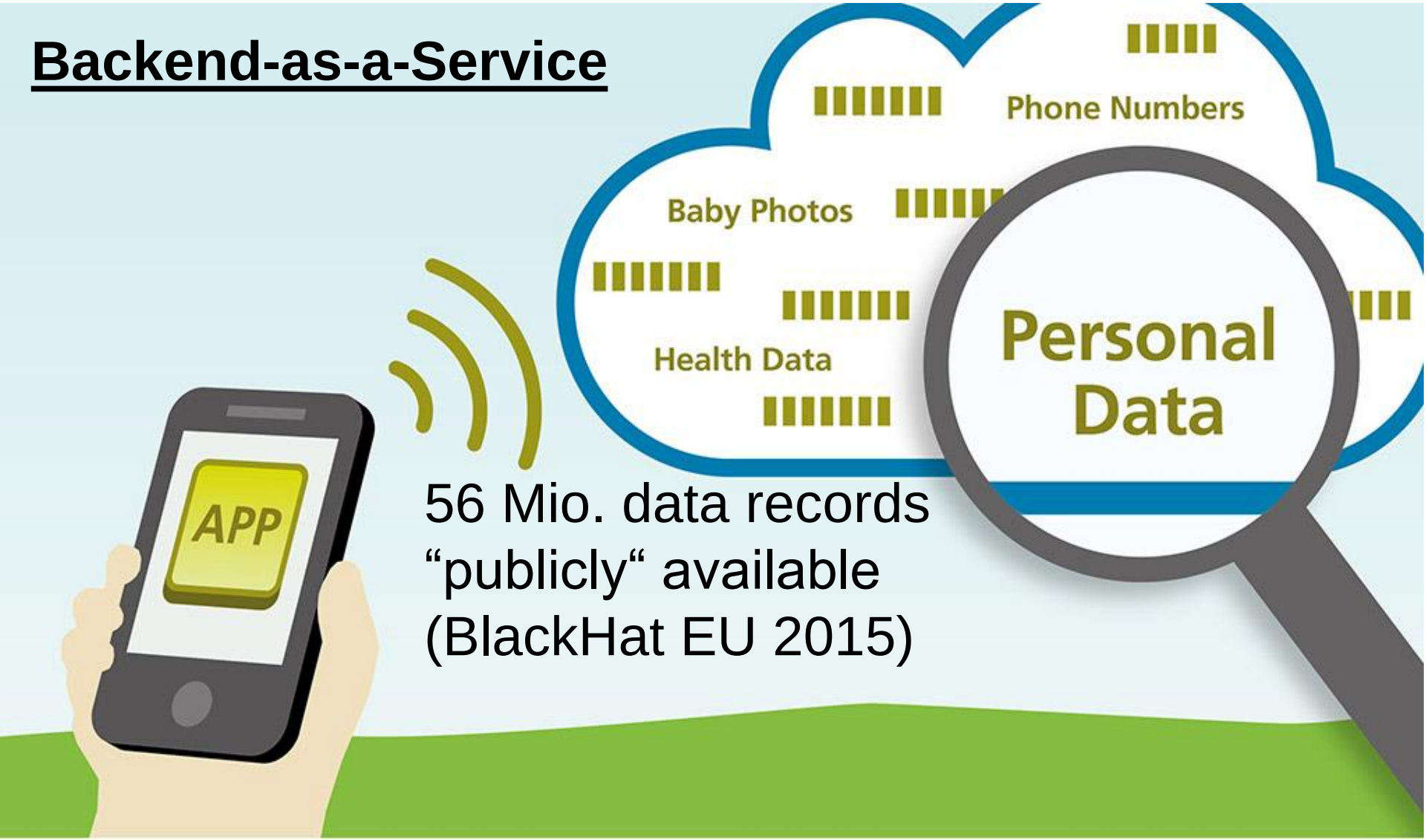
Carlos Castillo

- Mobile Security Researcher at Intel Security.
- Hacking Exposed 7 co-author (Hacking Android).
- ESET Latin America's Best Antivirus Research winner 2009.

Alex Hinchliffe

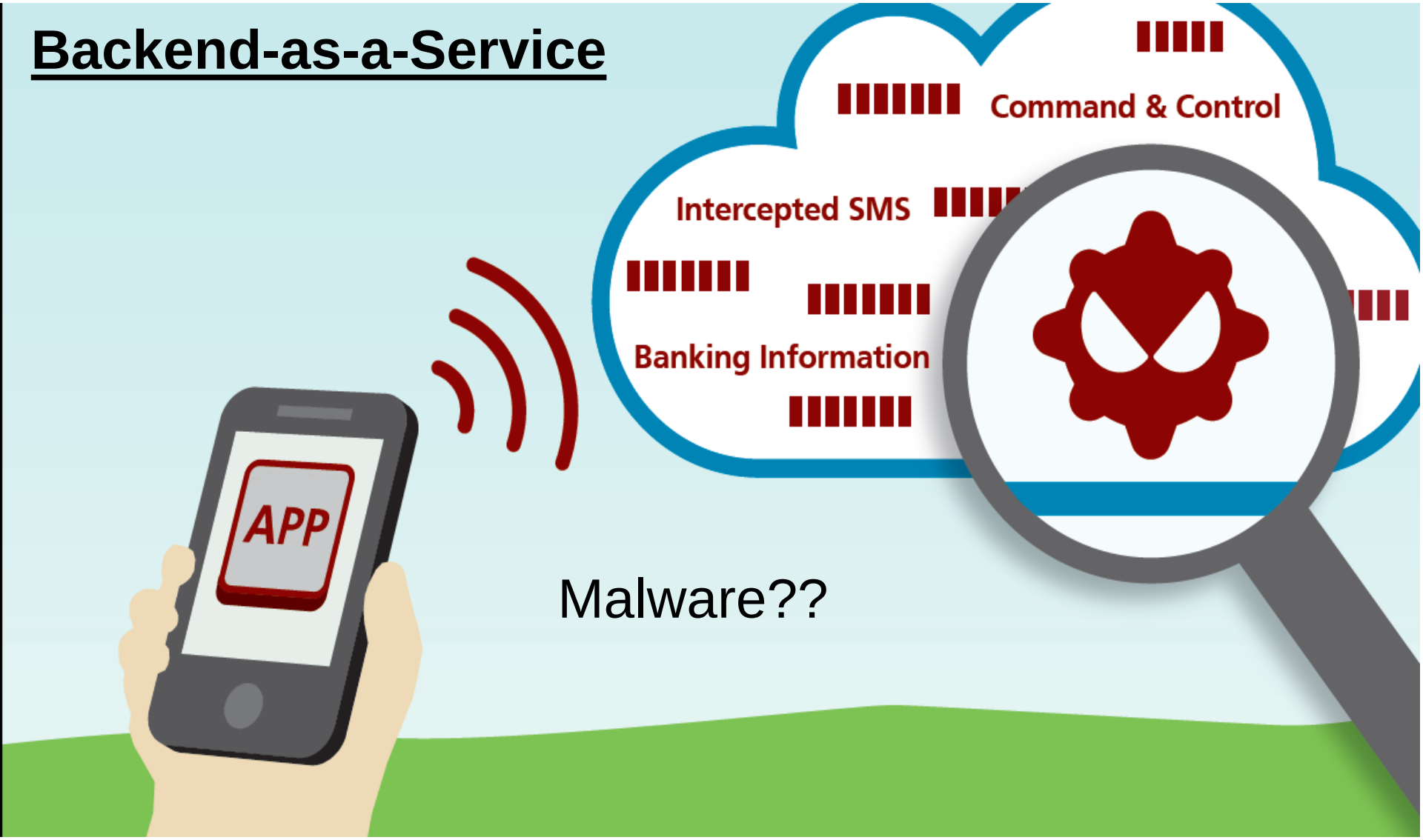
- Mobile Security Research Manager at Intel Security
- Co-developer of cloud based Anti-Malware technology, Artemis
- Project partner of MobSec, S^2Lab, Royal Holloway University, London

Backend-as-a-Service

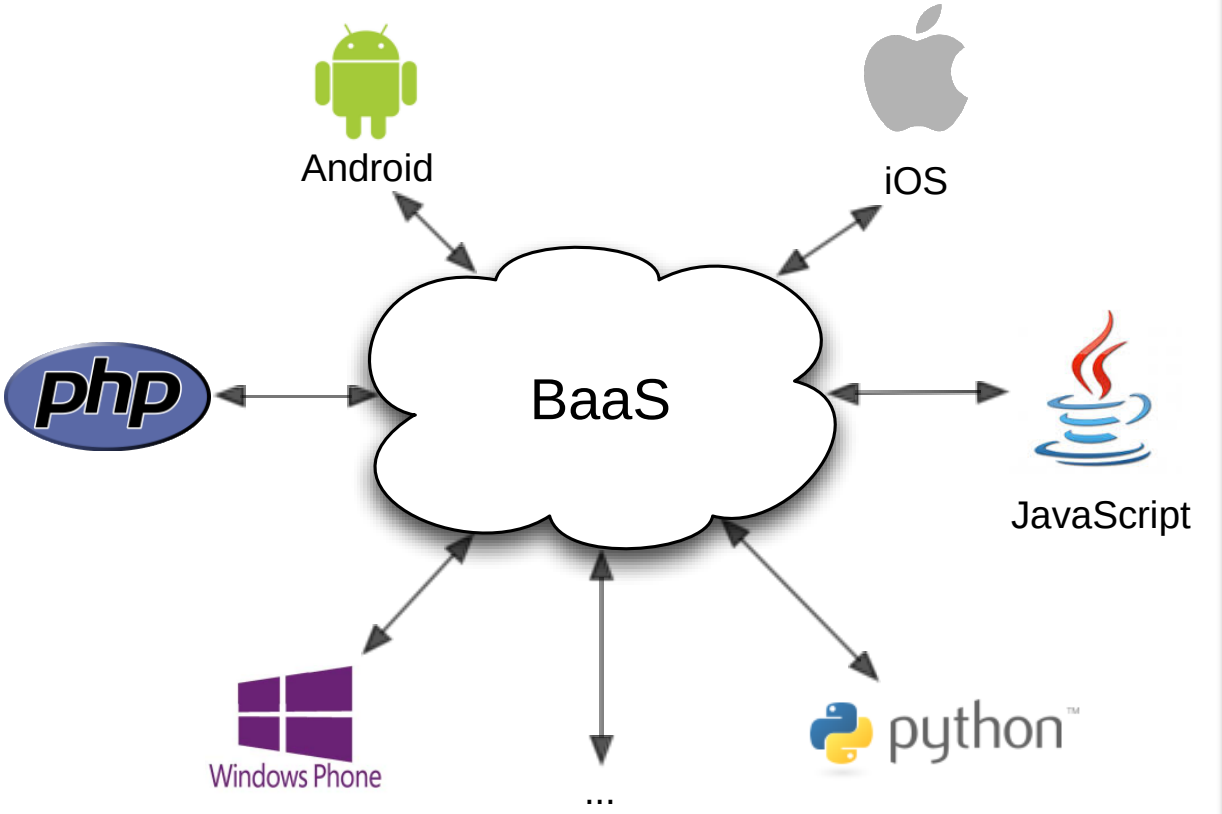


56 Mio. data records “publicly“ available (BlackHat EU 2015)

Backend-as-a-Service



Backend-as-a-Service (1)



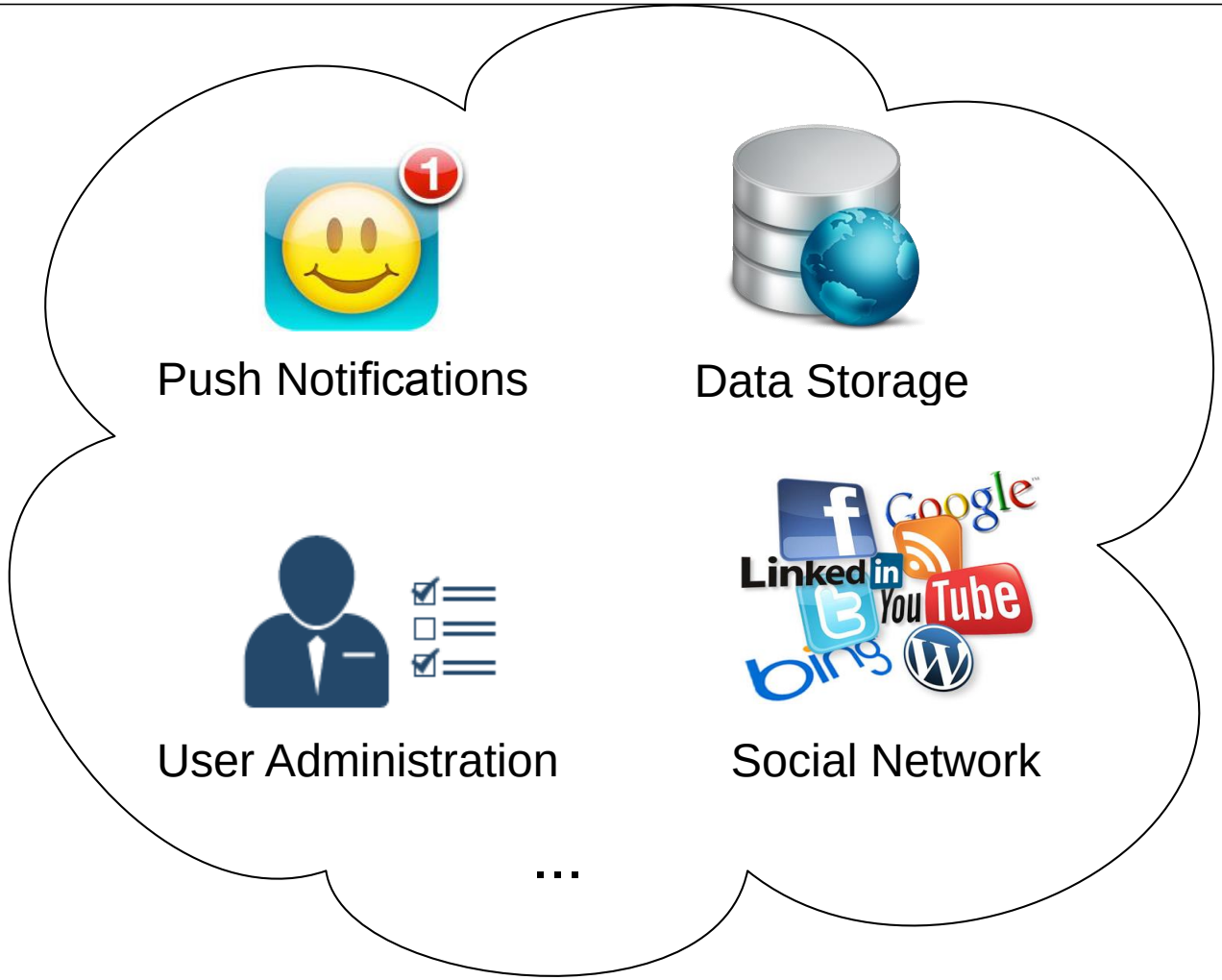
Parse
The Cloud Application Platform

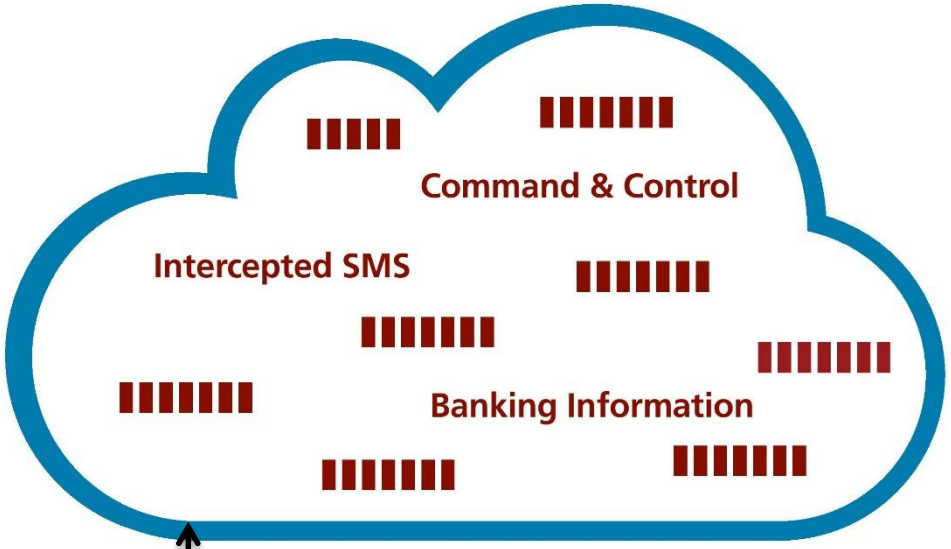
amazon web services™

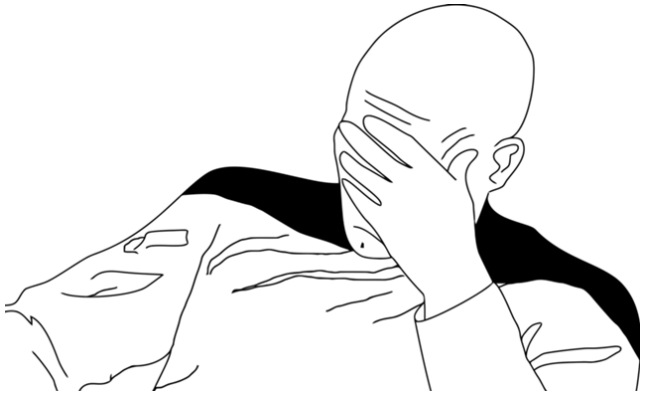
cloudmine

...

Backend-as-a-Service (2)





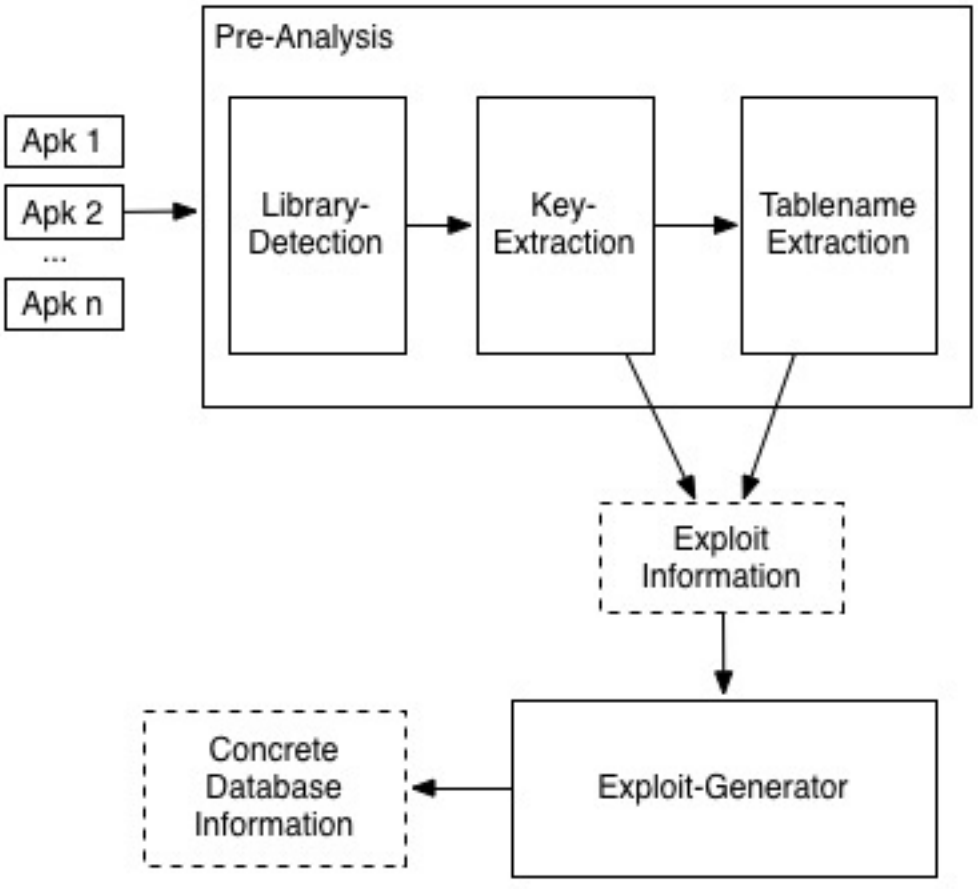


ID Keys != Authentication Keys!

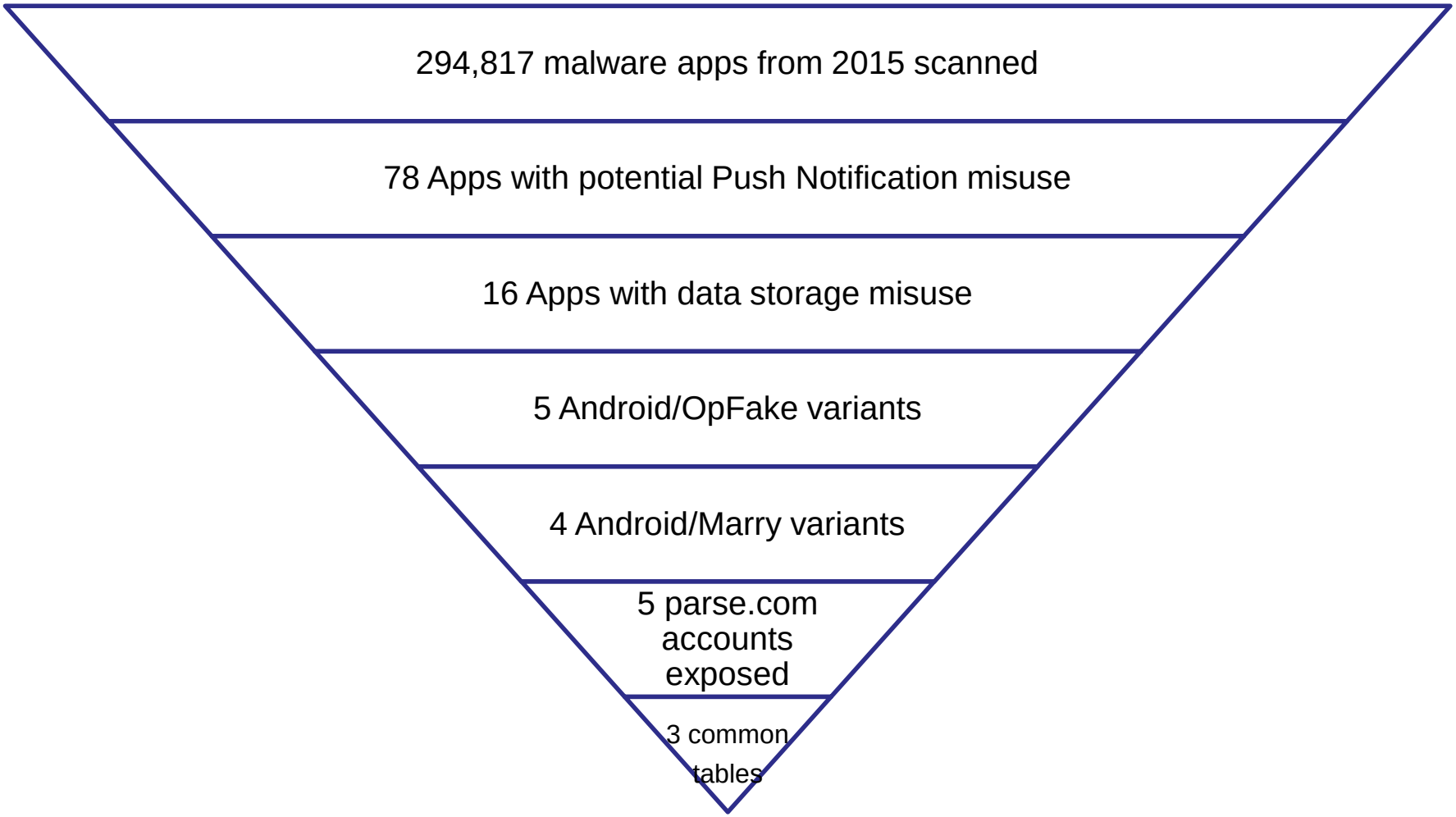
```
Parse.initialize(this, APPLICATION_ID, CLIENT_KEY);
ParseObject sms = new ParseObject("Intercepted SMS");
sms.put("message", "Hi VB2015");
```

Use Proper Access Control Rules on the Server Side!

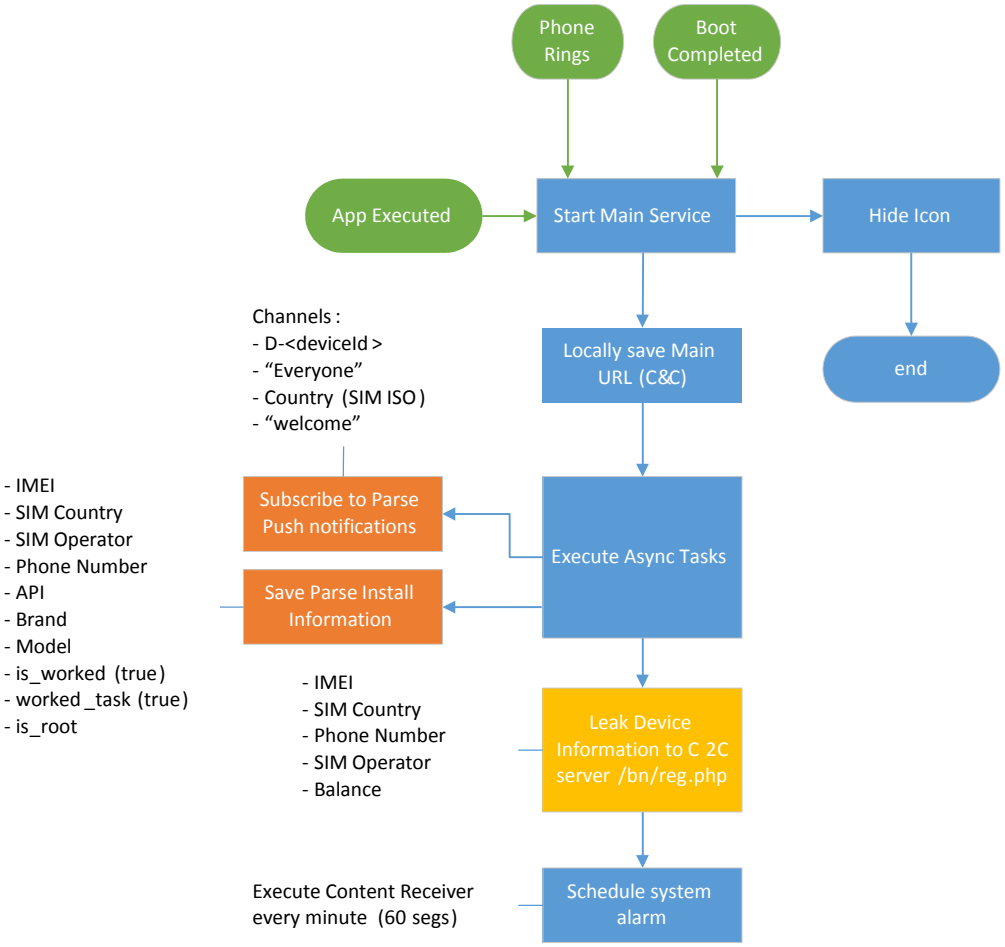
HAVOC: Automatic Exploit Generator



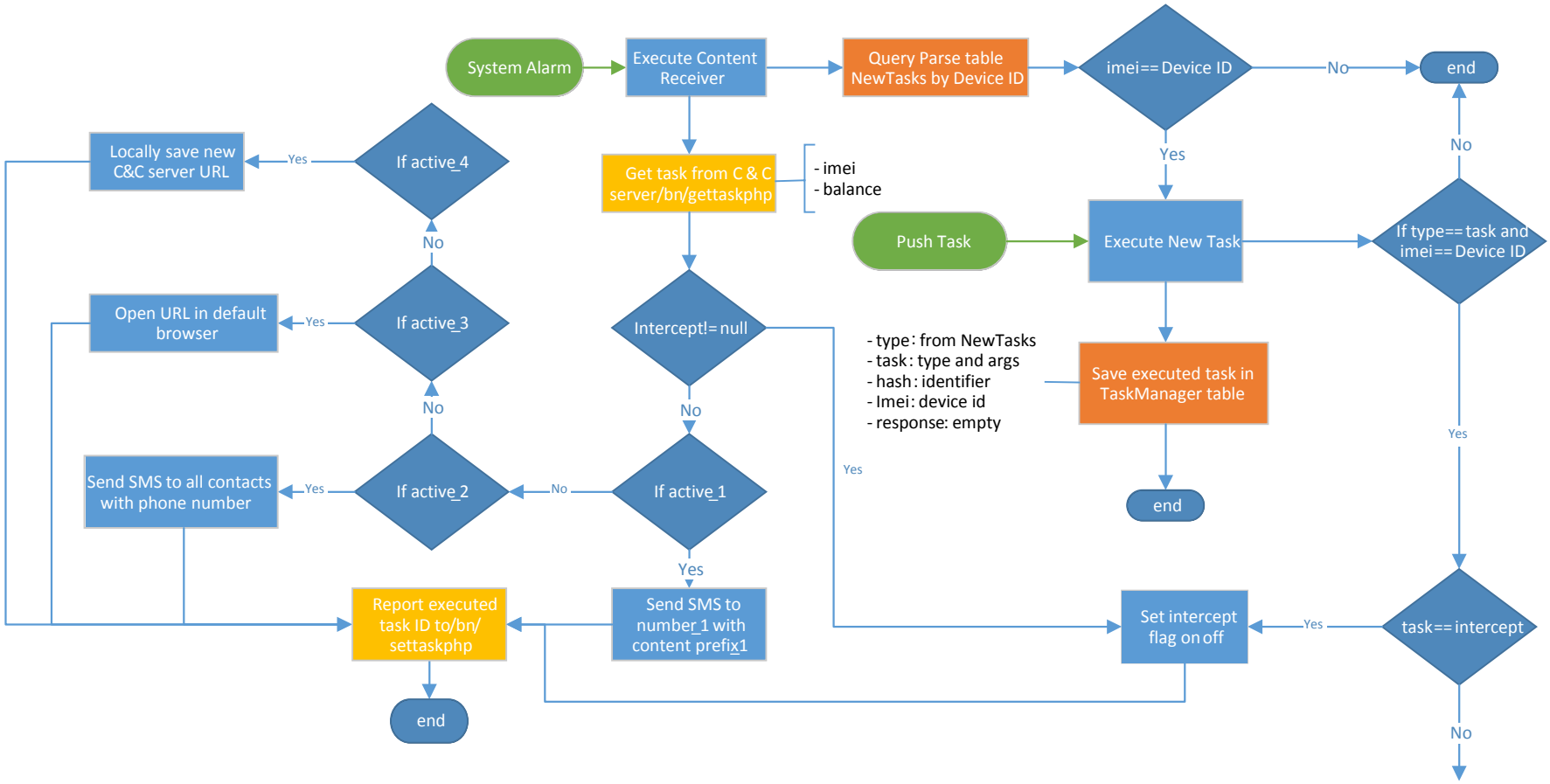
Malware using Facebook‘s Parse



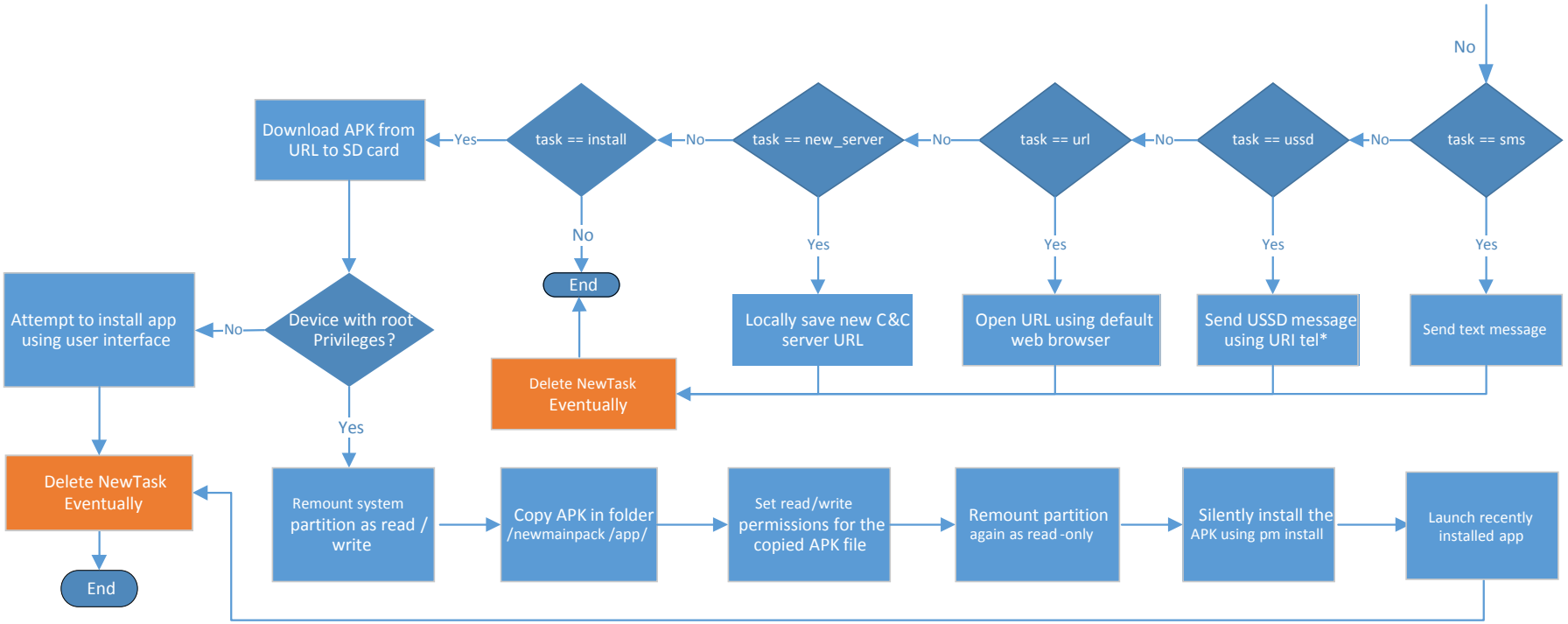
OpFake – App Execution and Main Service



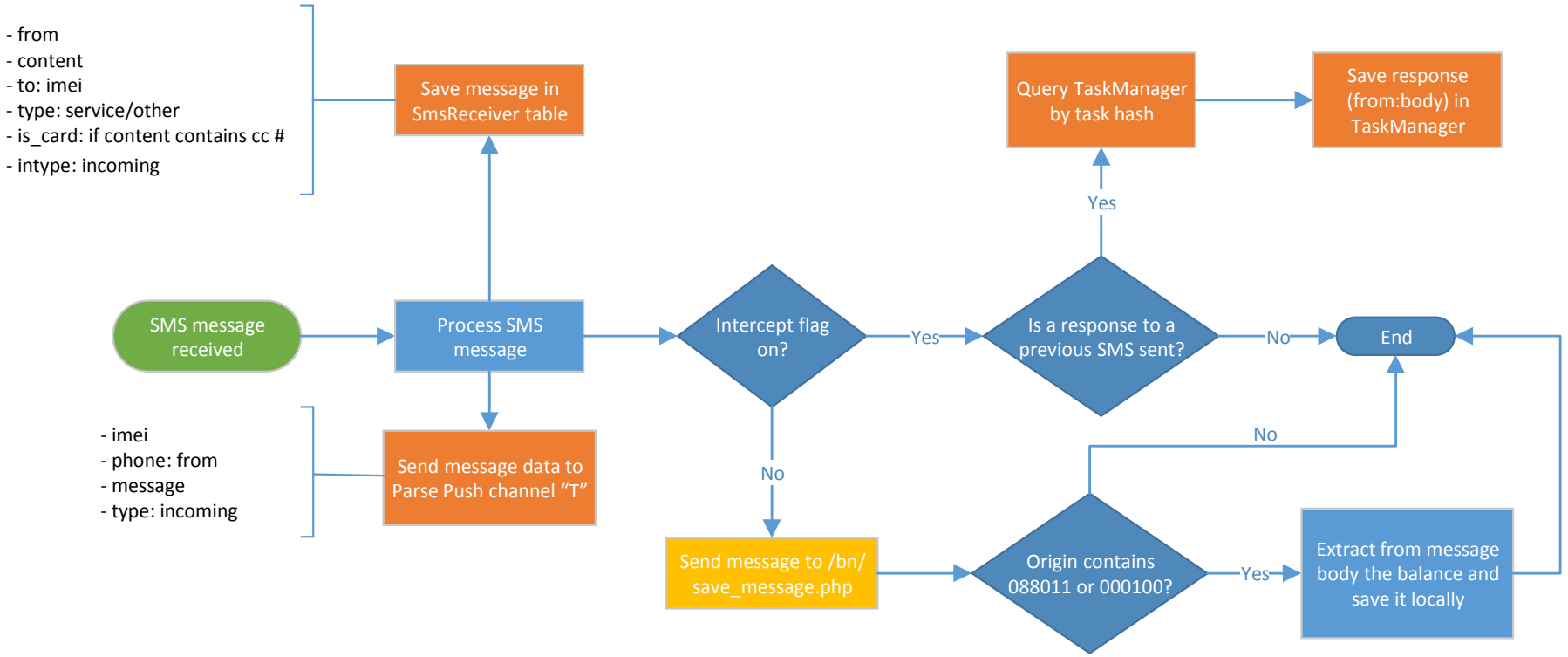
OpFake – System Alarm every Minute



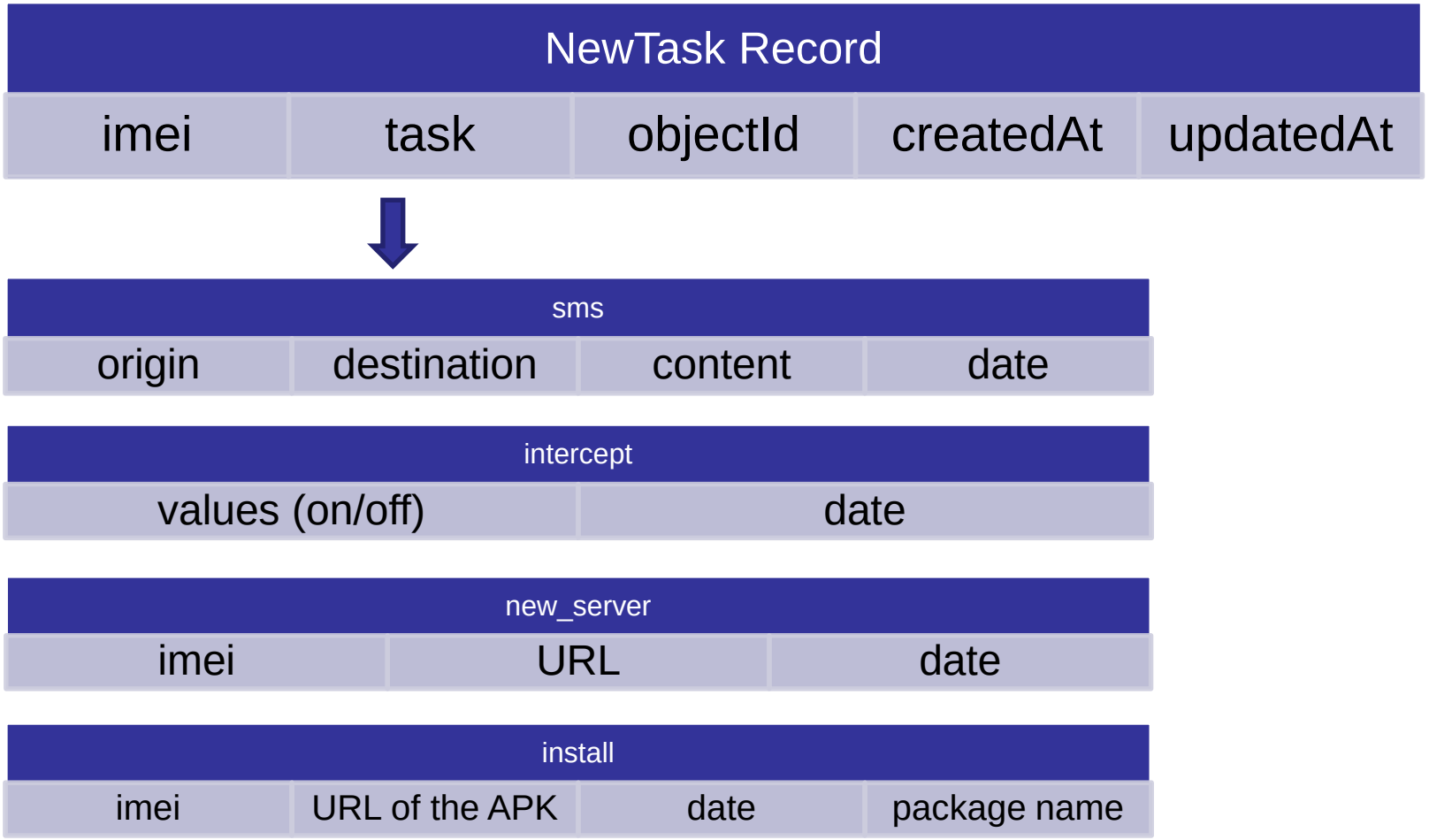
OpFake – Execute New tasks



OpFake – SMS Message Received

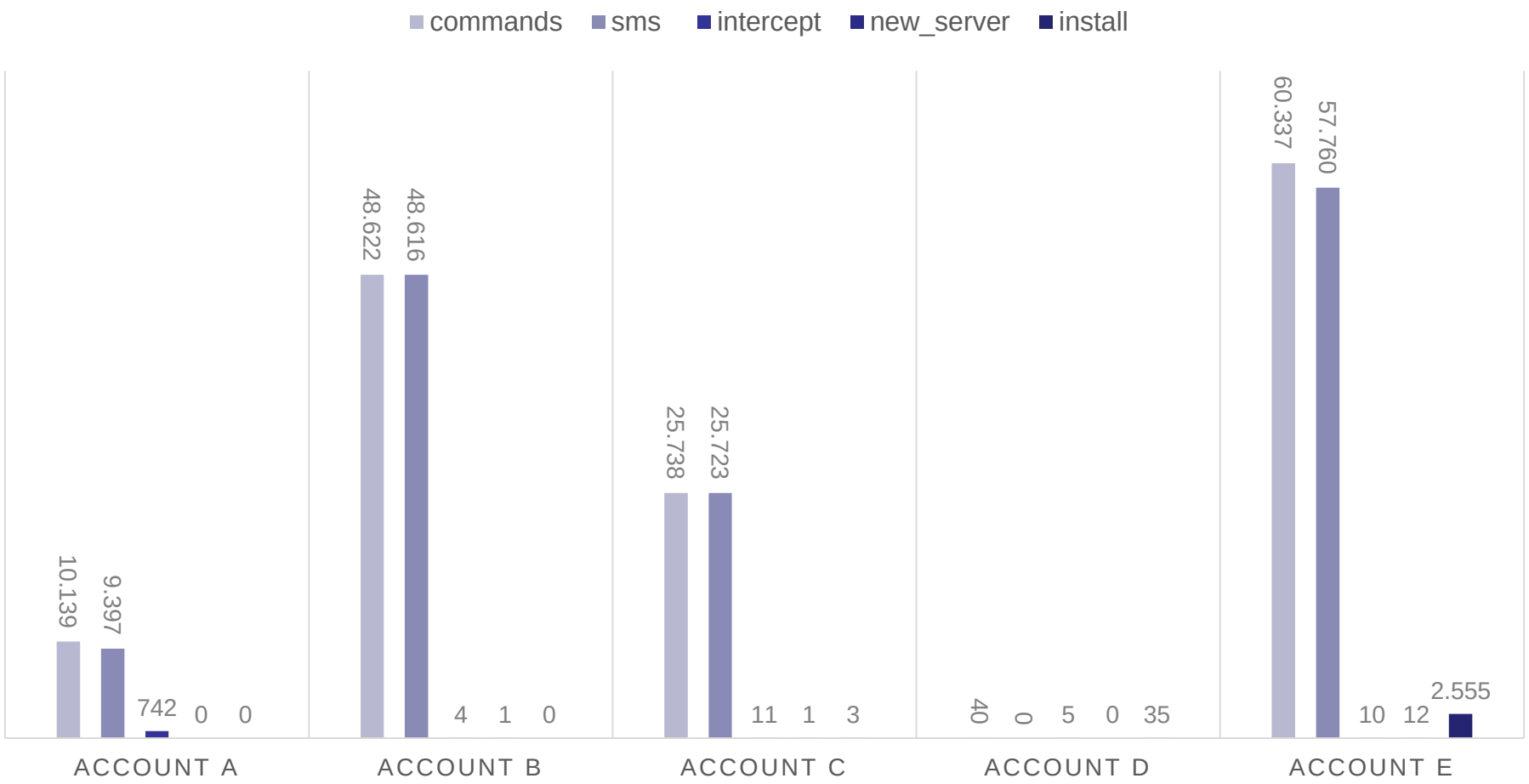


NewTasks Schema



Exposed Malware Parse.com Accounts

NewTasks – Commands received



TECHNISCHE UNIVERSITÄT DARMSTADT

SECURE SOFTWARE ENGINEERING GROUP

intel Security

Exposed Malware Parse.com Accounts

NewTasks – Examples of commands delivered

sms

- send sms to number 900 with content “BALANS”
- send sms to number 900 with content <confirmation_code>
- send sms to number 3116 with content “card <card_number> <exp_month> <exp_year> <CVV>”

intercept

- on/off

new_server

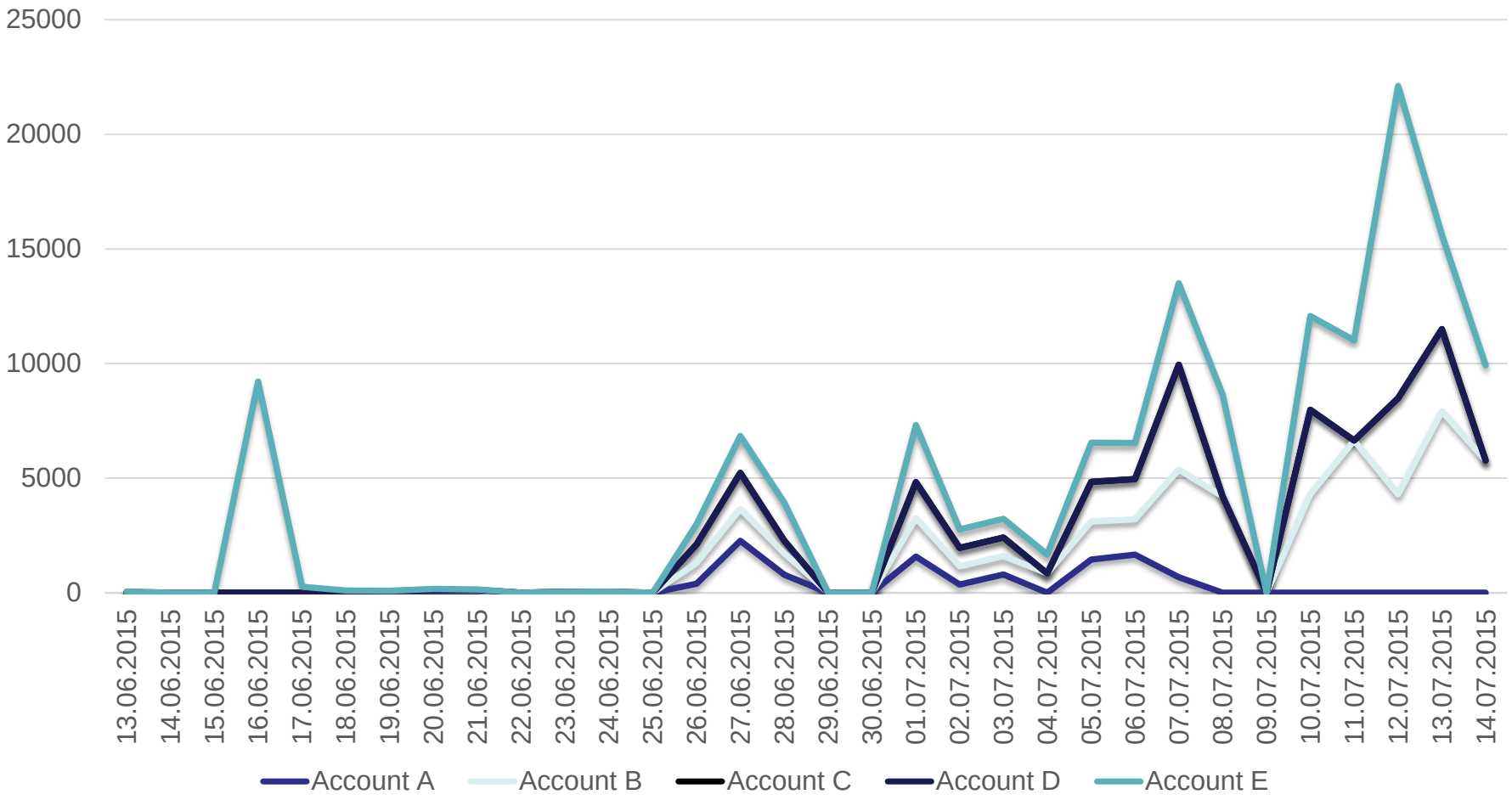
- hxxp://newwelcome00.ru
- hxxp://newelcome00.ru

install

- Android/OpFake delivering Android/Marry:
  - hxxp://newwelcome00.ru/appru.apk (marry.adobe.net.threadsync).
  - hxxp://newwelcome00.ru/app.apk (marry.adobe.net.nightbuid).
- hxxp://notingen.ru/Player.apk (com.adobe.net)
- hxxp://швждаыдлпждв

Exposed Malware Parse.com Accounts

NewTasks – Command created by date



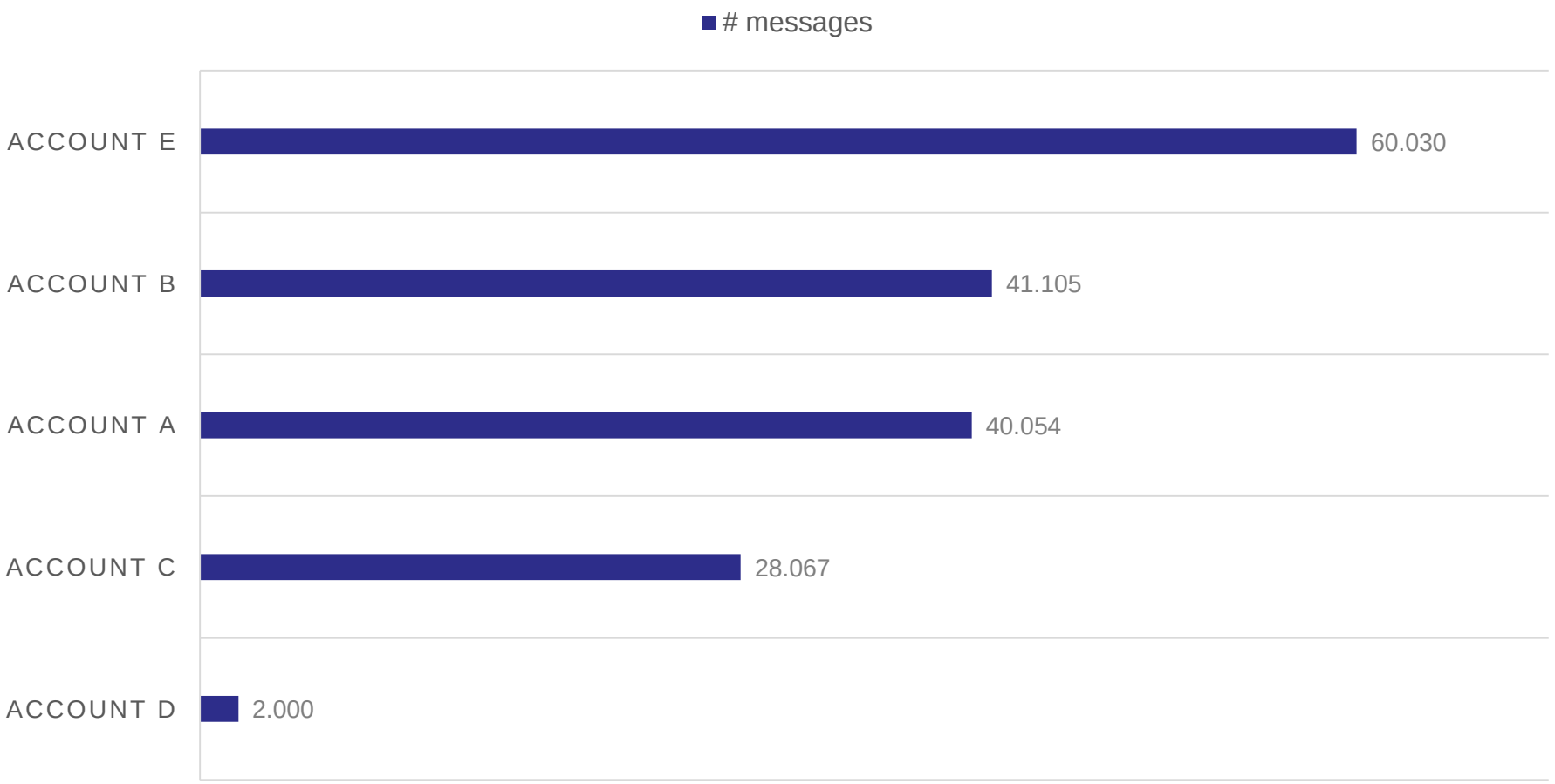
SmsReceived Schema

SmsReceived Record							
body	from	objectId	intype	is_card	updatedAt	type	createdAt

- from: origin of the text message (phone number/company name)
- intype: incoming/outgoing
- to: device identifier of the infected device
- is_card: true/false if the message contains a credit card number
- type:
  - service: origin is a company (e.g. MegaFon)
  - other: origin is another phone number (personal messages)

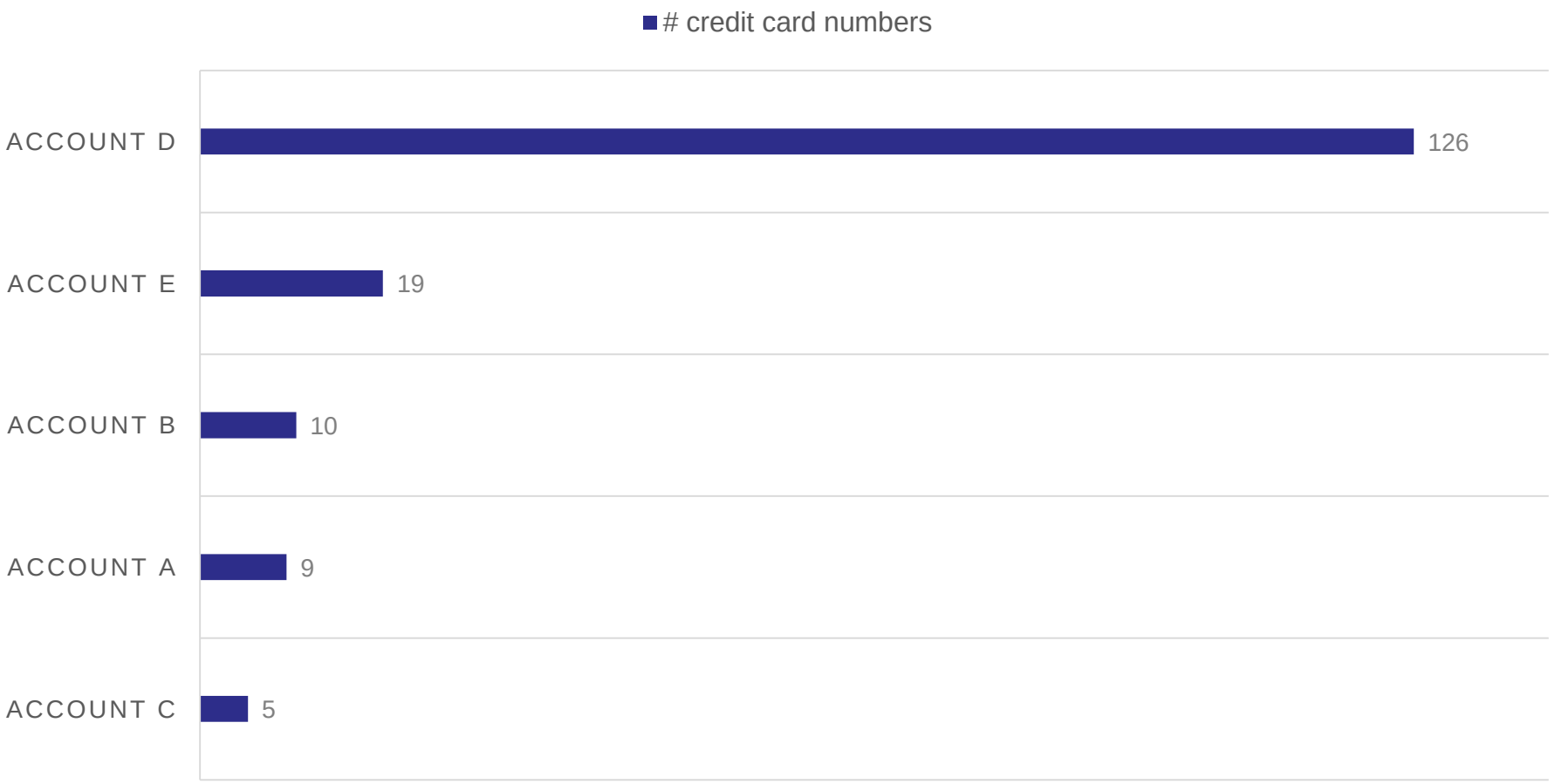
Exposed Malware Parse.com Accounts

SmsReceiver – # Intercepted SMS messages



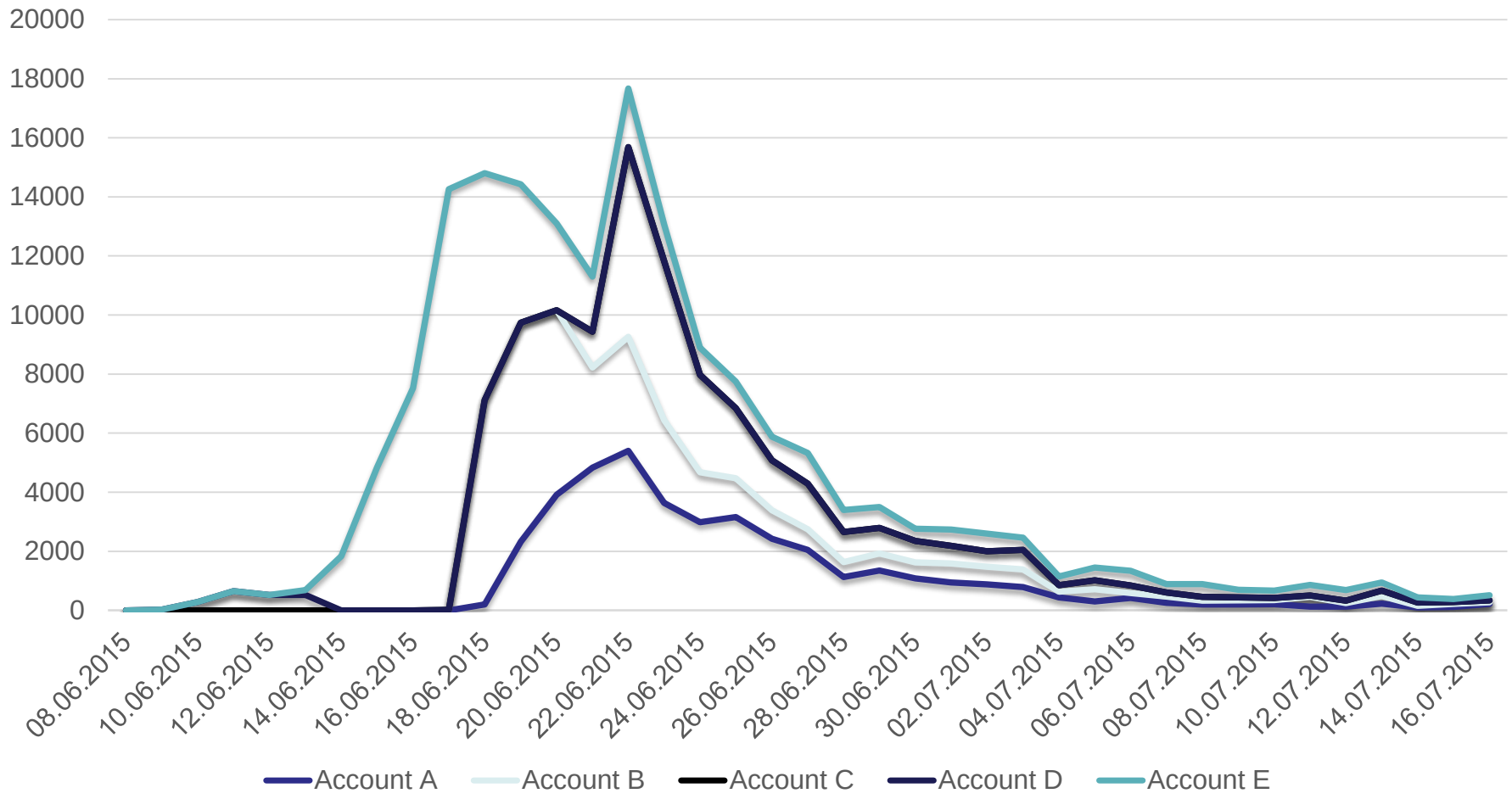
Exposed Malware Parse.com Accounts

SmsReceiver – Credit card numbers in incoming SMS messages

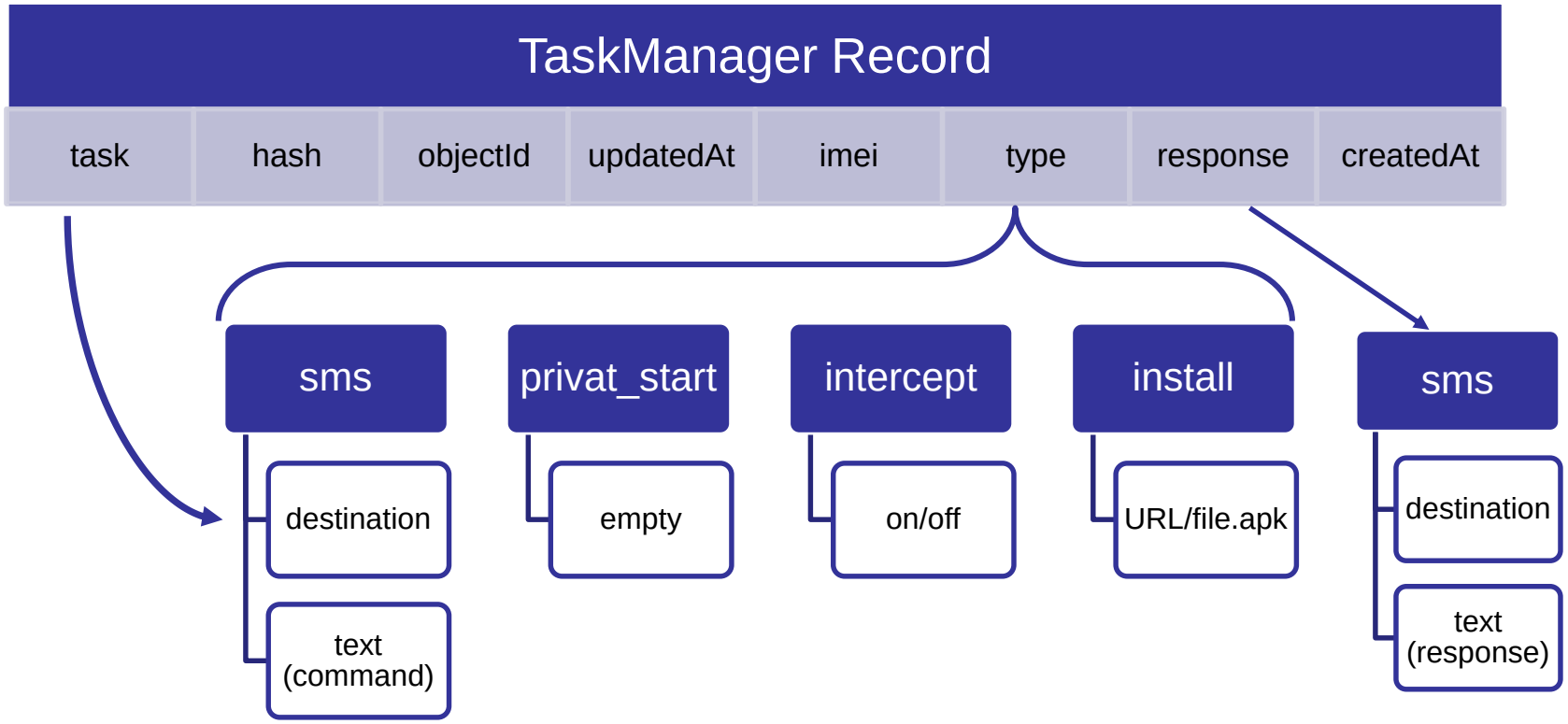


Exposed Malware Parse.com Accounts

SmsReceived – Messages by date

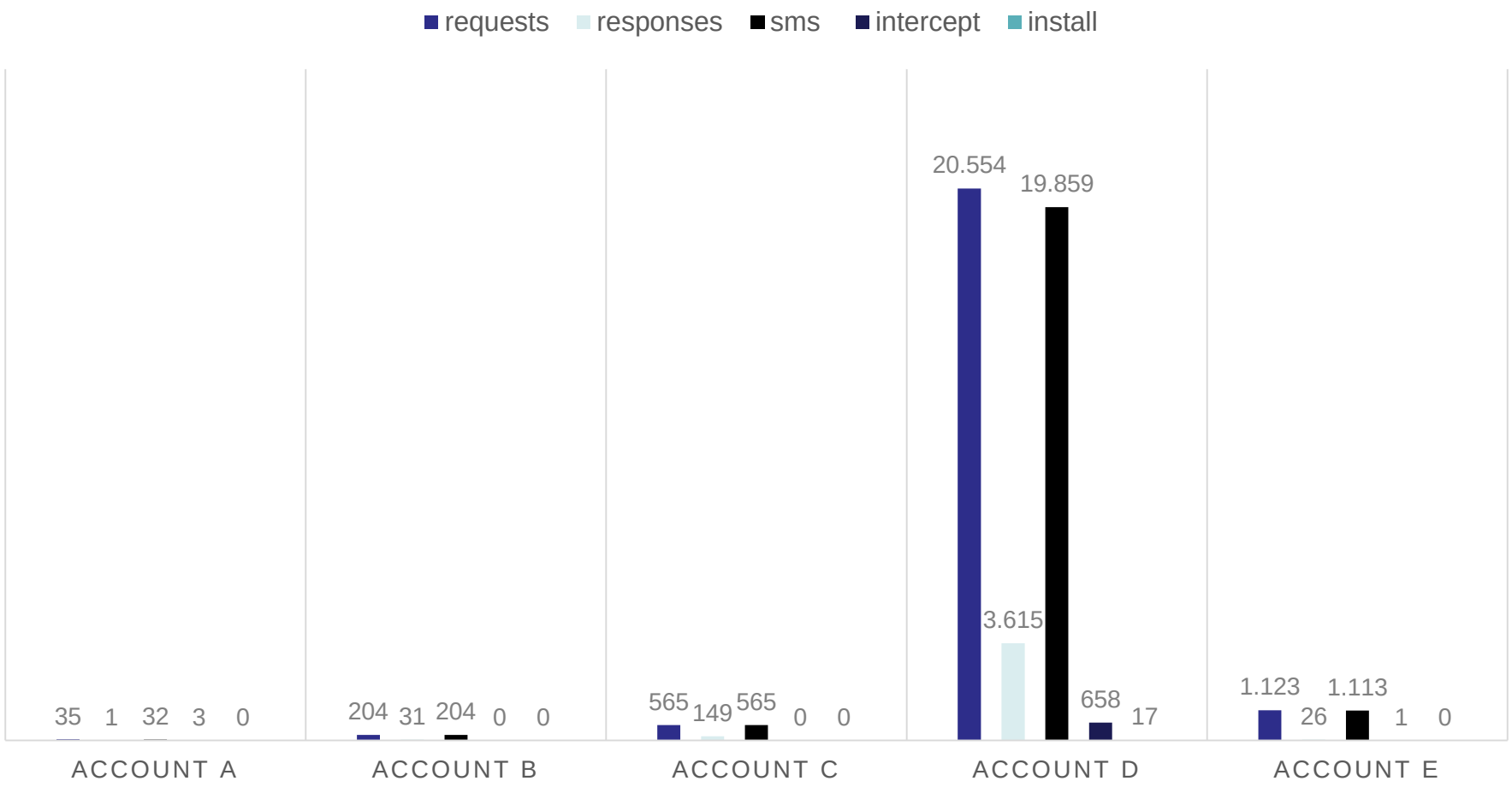


TaskManager Schema



Exposed Malware Parse.com Accounts

TaskManager – Command Executed



Exposed Malware Parse.com Accounts

TaskManager – Examples of tasks executed

sms 900 (Sberbank):

- Get list of connected cards and commands available: sms INFO
- BALANS/BALANCE <card>
- Payment of services: sms <amount>

sms 000100 (MegaFon)

- B (balance)

sms 7878 (Beeline):

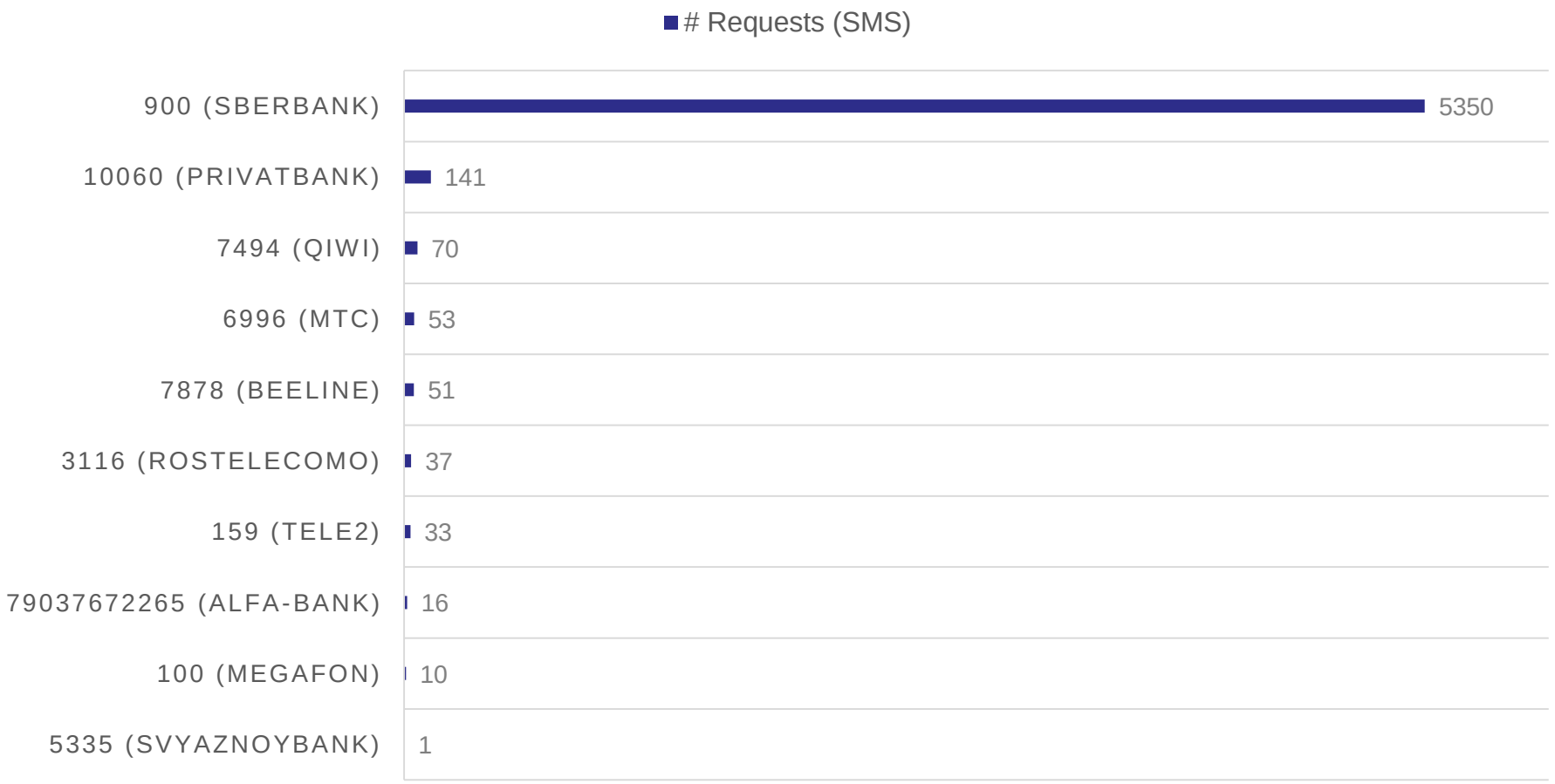
- Pay credit card: <Brand> <card_number> <amount>

Smishing (newwelcome00.ru)

- Russia: У вас 1 непрочитаное сообщение (You have 1 unread message) hxxps://tinyurl.com/phelju3
- Russia: Ваша ссылка для скачивания (Your download link) hxxp://goo.gl/TR5GjP
- Uzbekistan: Получено новое (Received new MMC) hxxp://goo.gl/RINTTQ

Exposed Malware Parse.com Accounts

Targeted Companies – Task (TaskManager table) in Account D



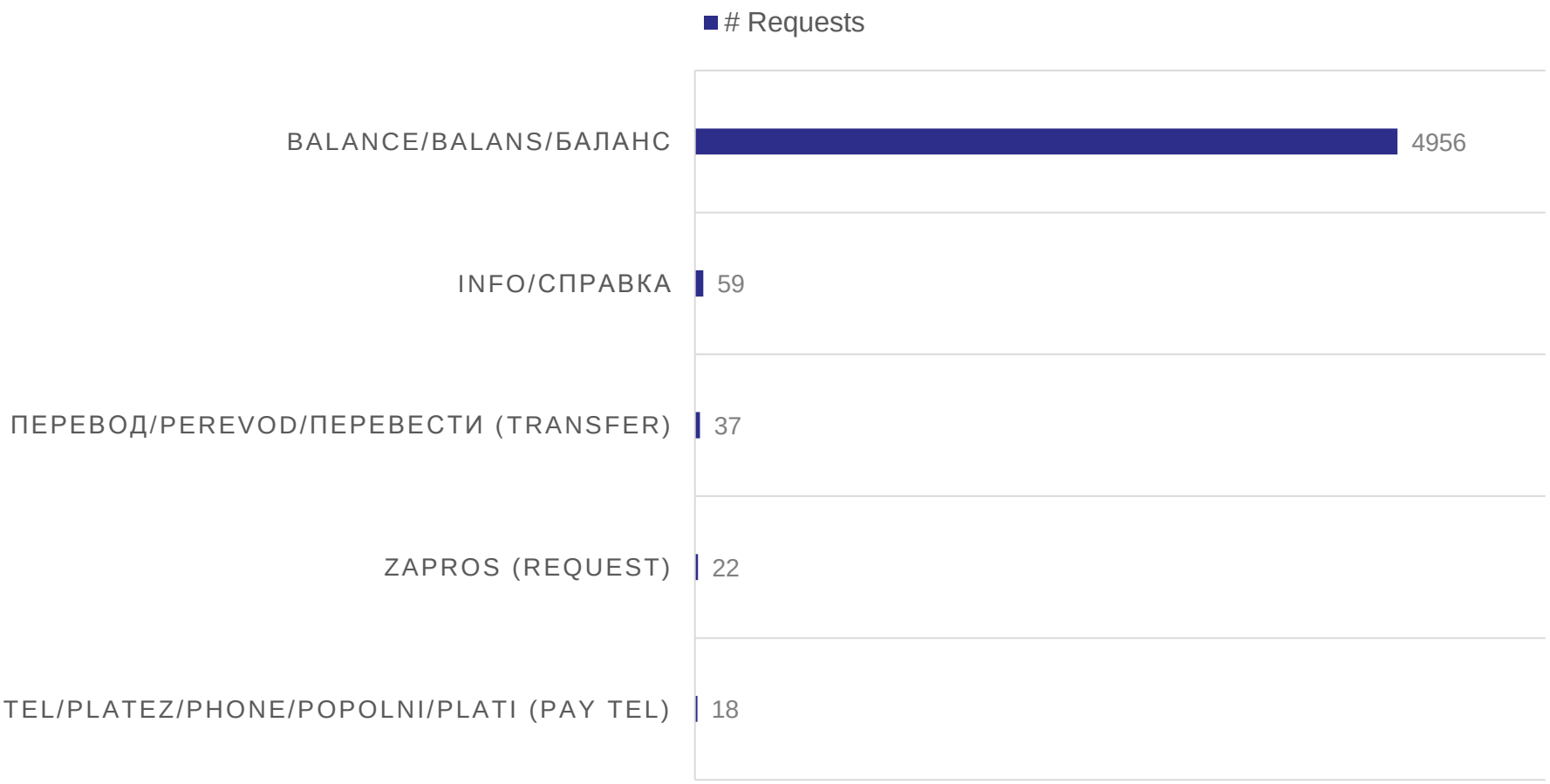
Exposed Malware Parse.com Accounts

Sberbank commands – Tasks (TaskManager table) in Account D

Command	Format	Response
BALANCE/BALANS/баланс	BALANS **<4-last-digits>**	VISA1234 Balance: **<amount>**
INFO/СПРАВКА	СПРАВКА	List of connected cards: VISA1234(ON);
ПЕРЕВОД/PEREVOD/ПЕРЕВЕСТИ (Transfer)	ПЕРЕВОД <4digits_card_origin> <4digits_card_destination> or <phone_number_destination> <amount>	To transfer **<amount>** from card VISA1234 the recipient **<name>** must send the code **<code>** to the number 900
ZAPROS (Request)	ZAPROS <phone_number> <amount>	Request transfer for **<amount>** to your card VISA4321 has been sent. After confirmation by the sender **<name>** the money will go to your account.
TEL/PLATEZ/PHONE/POPOLNI/PLATI (Pay mobile account)	TEL <phone_number> <amount>	To pay with card VISA1234 phone **<company>** **<phone_number>** the amount **<amount>** send the code **<code>** to number 900.

Exposed Malware Parse.com Accounts

Top Sberbank Commands – Task (TaskManager table) in Account D



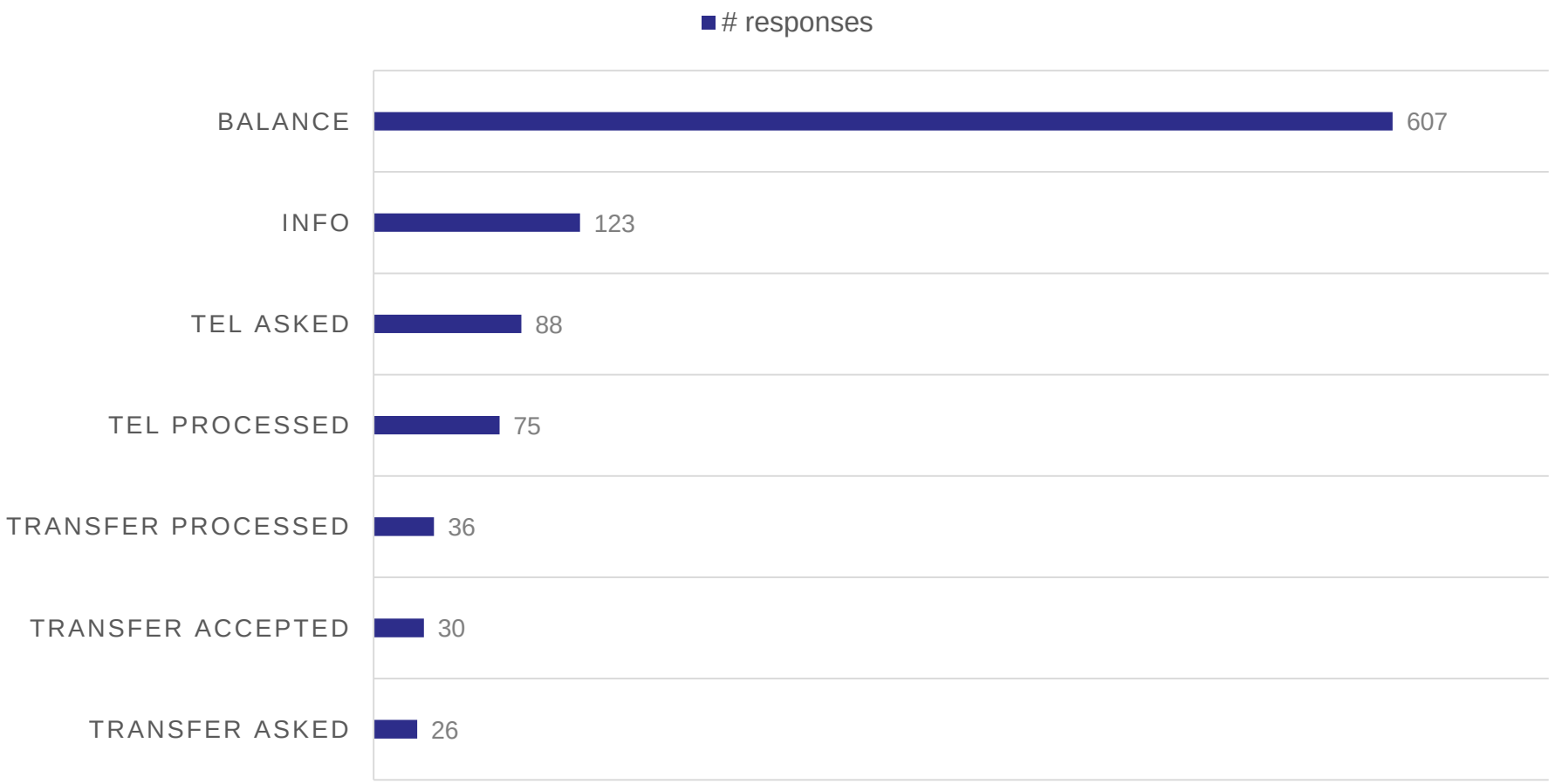
Exposed Malware Parse.com Accounts

Sberbank Responses – Tasks (TaskManager table) in Account D

Type	Response
Balance	VISA1234 Balance: **<amount>**
Info	List of connected cards: VISA1234(ON);
Tel Asked	To pay with card VISA1234 phone **<company>** **<phone_number>** the amount **<amount>** send the code **<code>** to number 900.
Tel Processed	VISA1234 **<date>** **<time>** payment for services **<amount>** **<operator>** **<phone_number>** Balance: **<amount>**
Transfer Processed	MAES1234: Transfer **<amount>** to the card recipient **<name>** is processed
Transfer Accepted	VISA1234: <time> Amount **<amount>** from the sender **<name>** received. Balance: **<amount>**
Transfer Asked	To transfer **<amount>** from card VISA1234 the card recipient **<name>** should send the code **<code>** to number 900.

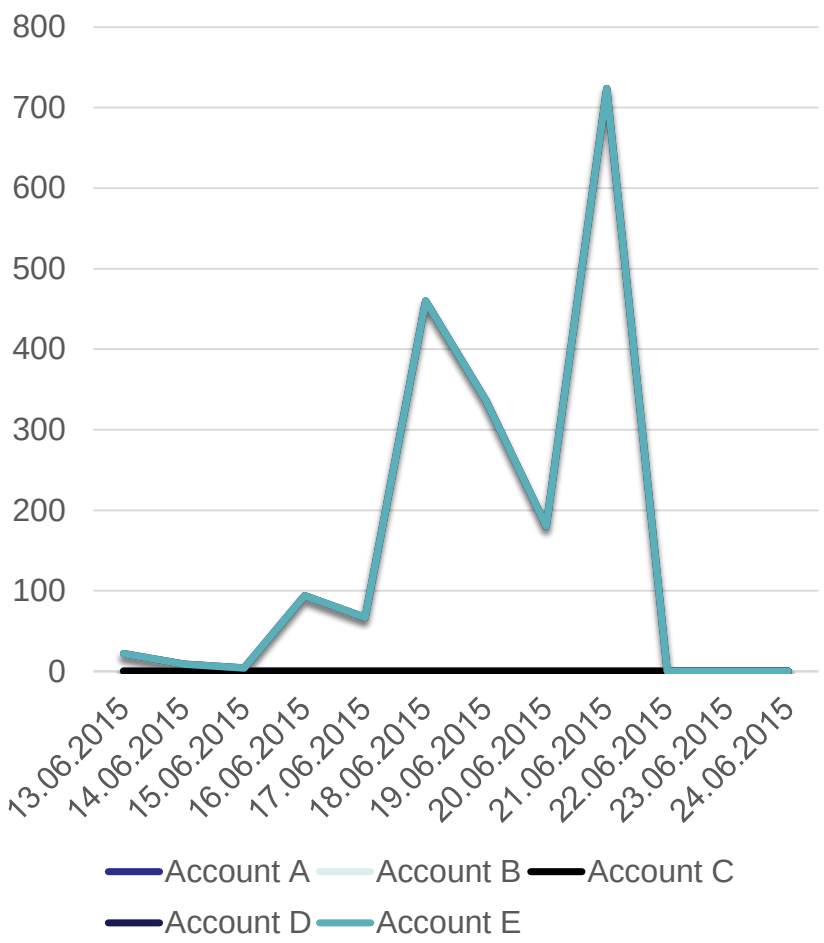
Exposed Malware Parse.com Accounts

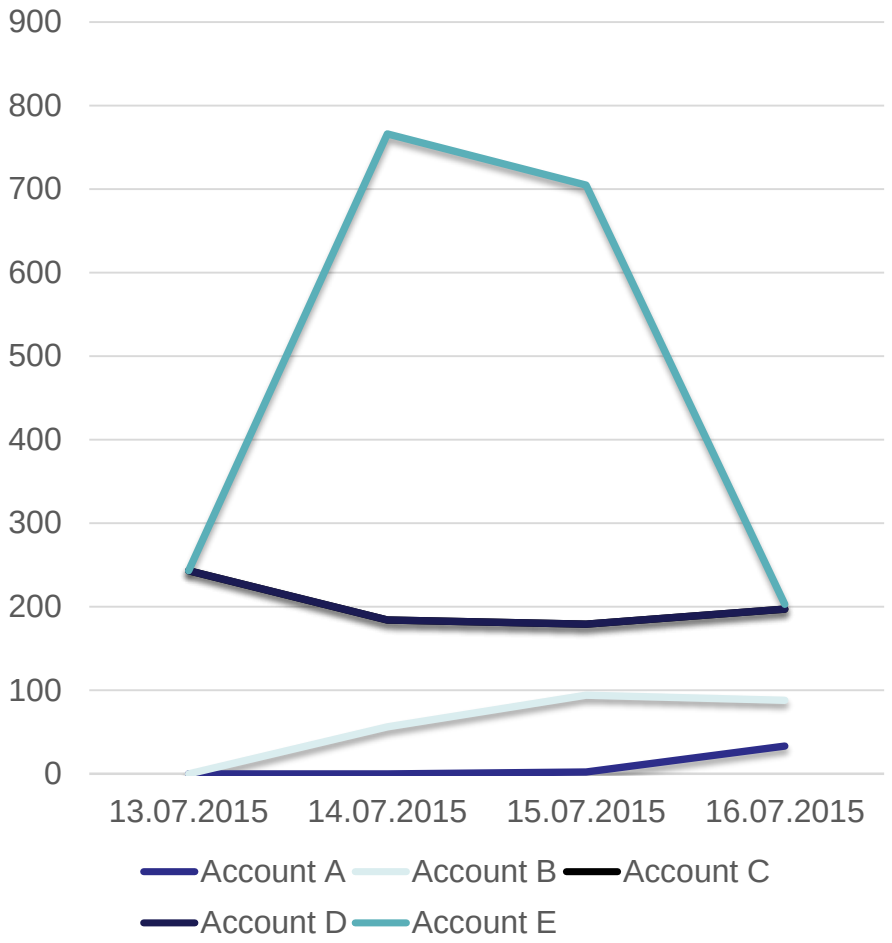
Top Sberbank fraud responses – Task (TaskManager table) - Account D



Exposed Malware Parse.com Accounts

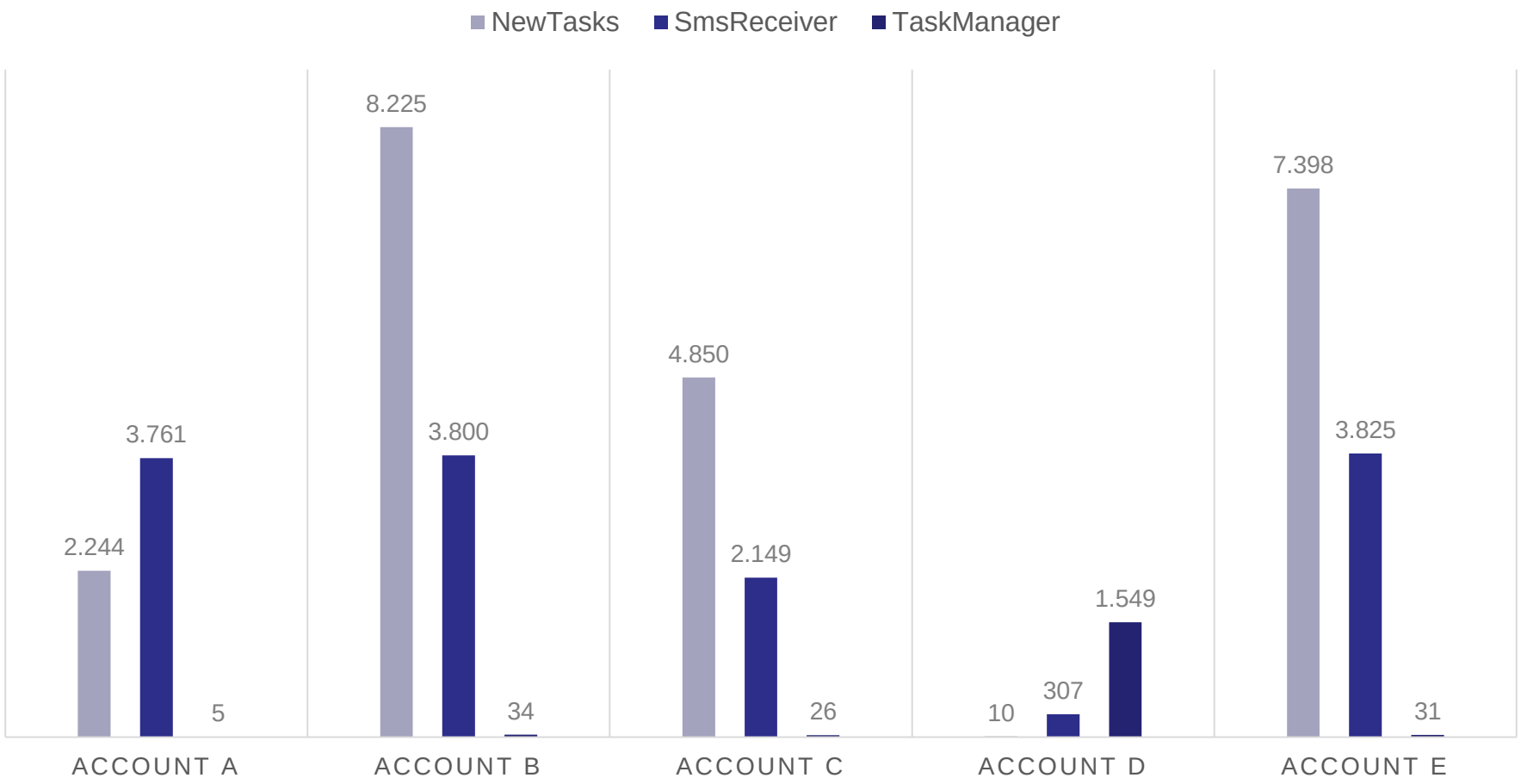
TaskManager – Command executed by date





Exposed Malware Parse.com Accounts

Unique Device IDs per table



Responsible Disclosure

2015-08-03: Reported finding to Facebook
2015-08-05: Facebook replied with "*... This issue does not qualify as a part of our bounty program...*"

2015-08-05: Facebook asked for more details
2015-08-06: We provided more details and Facebook blocked all Parse accounts
2015-08-28: Facebook offered room for collaboration

Facebook's responsible disclosure system only works with a Facebook account

Conclusions

- This Android Banking Trojans are actively performing financial fraud via SMS messages targeting Eastern Europe countries.

- Just like legitimate developers, Android malware authors also expose cloud accounts with sensitive (personal/financial) stolen information.

- Sensitive information stolen from victims by Android malware can be accessed by “anyone” without any authentication.

Siegfried Rasthofer
Secure Software Engineering Group
Email: siegfried.rasthofer@cased.de
Blog: http://sse-blog.ec-spride.de
Website: http://sse.ec-spride.de
Twitter: @CodeInspect

Carlos Castillo
Intel Security
Email: carlos.castillo@intel.com
Twitter: @carlosacastillo