

MOSCOW FORENSICS DAY '25

НАТАЛИЯ КОТОВА

«SPYNOTE В ДЕЙСТВИИ: КАК СОЗДАЕТСЯ,
ВНЕДРЯЕТСЯ И ИССЛЕДУЕТСЯ МОБИЛЬНЫЙ
ШПИОНСКИЙ ТРОЯН»



MFD

{SpyNote} в действии

как создается, внедряется и
исследуется мобильный
шпионский троян

НАТАЛИЯ КОТОВА

MOSCOW FORENSICS DAY '25



Будем знакомы!

- эксперт отдела компьютерных и радиотехнических экспертиз и исследований ЭКЦ УМВД России по Ярославской области
- МосУ МВД России им. В.Я. Кикотя, 2024 г.
10.05.05 Безопасность информационных технологий в правоохранительной сфере.
Специализация: Компьютерная экспертиза
- стаж экспертной работы один год

Кто такой ваш SpyNote?



RAT-троянец

Remote Administration Tool – средства удалённого администрирования или управления

Топ 10

Согласно отчету Лаборатории Касперского за 2024 вердикт входит в 10-ку популярных и стабильно растущих.

Since 2016

2016 год – в сети появились инструменты для его создания.
2022 год – утечка исходного кода одной из версий

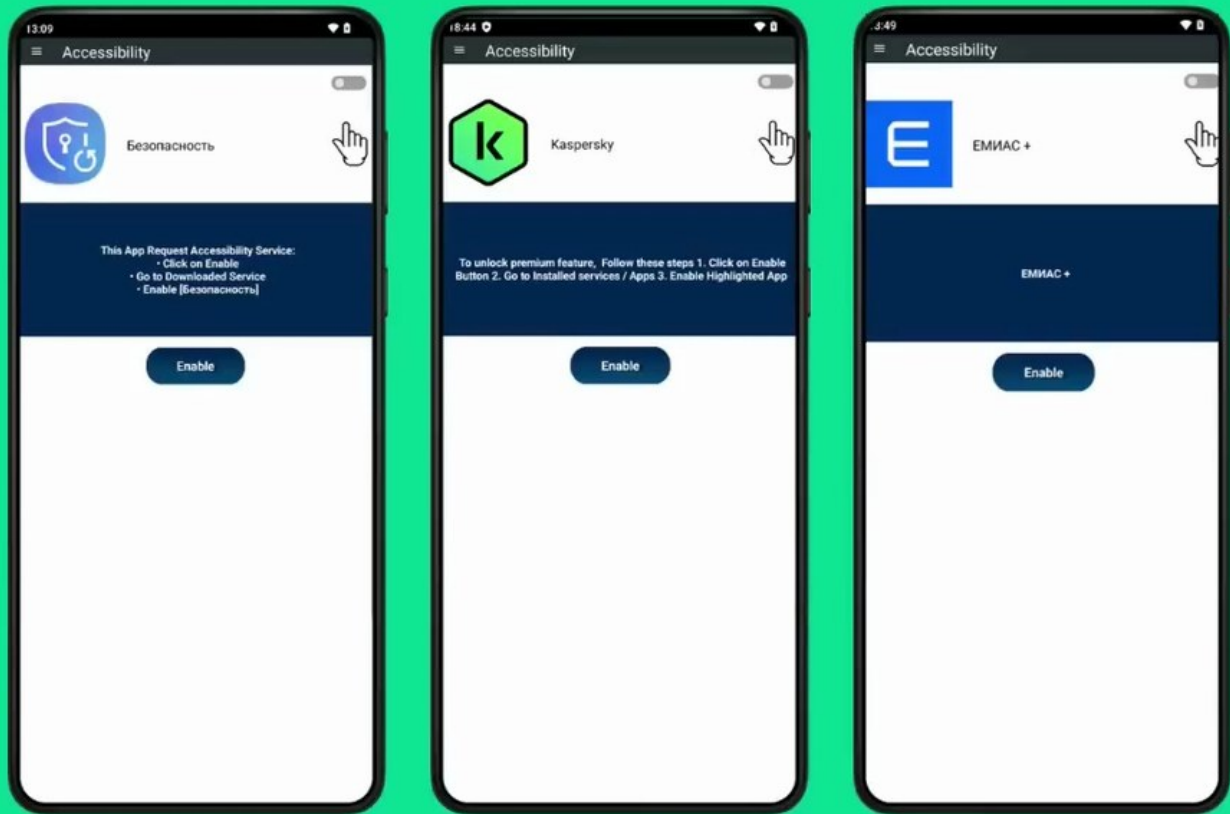
Кто такой ваш SpyNote?

Основной вектор атаки

- обход двухфакторной аутентификации путем перехвата SMS-сообщений

Методы маскировки

- использование имен и иконок легитимных приложений
- скрывание приложения в списке установленных приложений



Конструктор apk-файла

SpyNote 6.4

1

Build

App InfoDNS InfoPropertiesMerging AppBuild

Delete

C:\Users\qwerty\Desktop\apple-settings.png

Victim Name

test

App Name

Настройщик

Service Name

test 1

Version

1.1.1.0

2

Build

App InfoDNS InfoPropertiesMerging AppBuild

IP

tcp.cloudpub.ru

Port

26286

Pass

null

3

Build

App InfoDNS InfoPropertiesMerging AppBuild

Hide Application

Accessibility(Keylogger)

Deactivate icons

Device Administration

Permission Root SuperSU

Действия над зараженным устройством

SpyNote | Cracked By B0u3zizi | https://protection-tips.com/vb/

Tools View Help

Image	Victim Name	Country	Flag	Remote Address	Model	Ver & Api	n/a	n/a	n/a	SMS & Calls
	test	n/a		127.0.0.1:54359	HUAWEI ANA-NX9	10 & 29				null & null

File Manager

SMS Manager

Calls Manager

Contacts Manager

Location Manager

Account Manager

Camera Manager

Shell Terminal

Applications

Microphone

Keylogger

Settings

Victim

Phone

Chat

Fun

SMS_Manager_test94df27f28e2f748e

Address	Name	Date	Part Of Message
+7915...	null	Tue May 13 15:35:41 GMT+03:00 2025	Хэллоу

Calls_Manager_test94df27f28e2f748e

Number	Name	Call Type	Call Date	Duration
+7915...	null	null	Tue May 13 15:41:07 GMT+03:00 2025	00:00:00

Contacts_Manager_test94df27f28e2f748e

Name	Number	Connected Via
Контакт центр	88007001606	com.android.huawei.phone
Контакт 1	1234567890	com.android.huawei.phone
Контакт 2	12364569870	com.android.huawei.phone

Действия над зараженным устройством

- File Manager
- SMS Manager
- Calls Manager
- Contacts Manager
- Location Manager
- Account Manager
- Camera Manager
- Shell Terminal
- Applications
- Microphone
- Keylogger
- Settings
- Victim
- Phone
- Chat
- Fun

File_Manager_test16721fc243c90cb2

/storage/emulated/0

	Name	Size	File extension	Last Modified	Recently
Folder	Android		Folder Files(3)	05/09/2025 Fri	
Folder	Music		Folder Files(0)	05/13/2025 Tue	(New)
Folder	Download		Folder Files(1)	05/13/2025 Tue	(New)
Folder	test 1		Folder Files(2)		
Folder	Pictures		Folder Files(0)		
Folder	DCIM		Folder Files(0)		
Folder	Huawei		Folder Files(2)		



Camera_Manager_test94df27f28e2f748e

Select Camera:0

Size:400*400

Quality:Auto

Flash Mode:Off

Foces:Off

Multi-Capture:Off

ZOOM:0%

Stop

7fps
15.24 KB

Действия над зараженным устройством



- File Manager
- SMS Manager
- Calls Manager
- Contacts Manager
- Location Manager
- Account Manager
- Camera Manager
- Shell Terminal
- Applications
- Microphone
- Keylogger**
- Settings
- Victim
- Phone
- Chat
- Fun

key_logger_test16721fc243c90cb2

Start Stop

Offline Online

Y

Y

Y

Y

Y

Y null

Y qwertyasdff

Y qwertyasdffb

Y qwertyasdffb

Y qwertyasdffbd

Y qwertyasdffbd

Selected 1

key_logger_test16721fc243c90cb2

Start Stop

Offline Online

•

Изображение, (P)

•#

Изображение, (W)

•#0

0, +

•#06

6, MNOPCTY

•#06#

Изображение, (W)

IMEI, IMEI1:863725044876496IMEI2:863725044888509SN:VWS0220902000398, OK

Selected 1

Count 163

Ln 1



Действия над зараженным устройством

- File Manager
- SMS Manager
- Calls Manager
- Contacts Manager
- Location Manager
- Account Manager
- Camera Manager
- Shell Terminal
- Applications
- Microphone
- Keylogger
- Settings**
- Victim
- Phone
- Chat
- Fun

Settings_test16721fc243c90cb2

Phone Info Votes and alerts Phone bar

Device Policy Manager

Screen Lock

Factory reset

...

Add a screen lock password

Password Reset

Enter your new password



Settings_test16721fc243c90cb2

Phone Info Votes and alerts Phone bar

Device Policy Manager

Screen Lock

Factory reset

...

Add a screen lock password

Success Password 1234

Прочие функциональные возможности SpyNote

Отслеживание
местоположения



Возможность
совершения
вызовов



Доступ к
микрофону



Чат с
пользователем



Shell-терминал



Доступ к
сведениям об
аккаунтах



Типовые вопросы

1. Имеются ли на предоставленном на экспертизу мобильном телефоне файлы, детектируемые антивирусным программным обеспечением?
2. Имеются ли в предоставленном на экспертизу мобильном телефоне сведения об установленном программном обеспечении для удаленного доступа?
3. Имеются ли в предоставленном на экспертизу мобильном телефоне сведения об истории вызовов и SMS-сообщениях в явном или удаленном виде?
4. Имеются ли в предоставленном на экспертизу мобильном телефоне сведения об истории обмена сообщениями посредством мессенджеров и социальных сетей?
5. Имеются ли в предоставленном на экспертизу мобильном телефоне сведения об истории посещения веб-страниц посредством браузеров?

Этапы исследования



Статический анализ

1. Извлечение и декомпиляция APK
2. Изучение метаданных (AndroidManifest.xml)
 - имя пакета, версия, minSdk/targetSdk.
3. Анализ структуры приложения (AndroidManifest.xml)
 - активити, сервисы, ресиверы
4. Определение методов защиты (APKiD)
 - обфускация, упаковка
5. Анализ исходного кода
 - список используемых Android API
 - поведенческий анализ
6. Анализ ресурсов и строк
 - поиск URL-адресов, IP, доменов, e-mail

Динамический анализ

1. Установка и запуск в изолированной среде
2. Мониторинг поведения приложения
 - запрашиваемые разрешения
 - взаимодействие с пользователем
 - поведение при разных условиях
3. Анализ сетевой активности
 - сетевые соединения (TCP/UDP, HTTP/HTTPS)
 - анализ полезной нагрузки сетевых пакетов
4. Анализ файловой активности
 - создаваемые и изменяемые файлы
 - данные приложения

Статический анализ

Декомпиляция

- apktool
- JADX / JADX-GUI
- dex2jar
- Androguard

Поиск и анализ

- strings
- grep
- APKiD

Динамический анализ

Эмуляторы

- AndroidStudio (AVD)
- Genymotion
- Nox, LD player

Анализ трафика

- Burp Suite
- ZAP
- Wireshark

Статический + динамический анализ



<https://mobsf.live>

Mobile Security Framework (MobSF)

Repo: <https://github.com/MobSF/Mobile-Security-Framework-MobSF>

Doc: <https://mobsf.github.io/docs/#/>



- автоматизированный статический анализ
- динамический анализ с возможностью отслеживания активности приложения
- создание отчётов

AndroidManifest.xml

<manifest package=имя пакета versionName= версия>

<uses-permission>

разрешения (права) приложения на доступ к различным функциям и данным на устройстве

</uses-permission>

<application>

<activity>

графические формы (экраны) приложения

<intent-filter> тип намерения </intent-filter>

</activity>

<service>

определяет фоновые службы приложения

</service>

<receiver>

определяет приёмники широковещ-х broadcast'ов

</receiver>

</application>

</manifest>

<https://developer.android.com/guide/topics/manifest/manifest-intro>

Статический анализ

```
<uses-permission android:name="android.permission.WRITE_CONTACTS" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.RECORD_AUDIO" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.READ_CALL_LOG" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.CALL_PHONE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.GET_TASKS" />
```

```
<activity android:label="@string/app_name" android:name="cmf0.c3b5bm90zq.patch.C7" android:
  <intent-filter>
    <action android:name="android.intent.action.MAIN" />
    <category android:name="android.intent.category.LAUNCHER" />
  </intent-filter>
</activity>
```

MAIN+LAUNCHER → основная активити

```
<service android:name="cmf0.c3b5bm90zq.patch.C1" android:permission="android.permission.B
  <intent-filter>
    <action android:name="android.accessibilityservice.AccessibilityService" />
  </intent-filter>
</service>
```

фоновая служба с доступом к специальным возможностям

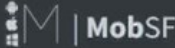
```
<receiver android:name="cmf0.c3b5bm90zq.patch.C10">
  <intent-filter>
    <action android:name="android.provider.Telephony.SMS_RECEIVED" />
  </intent-filter>
</receiver>
```

контроль входящих SMS

```
<receiver android:name="cmf0.c3b5bm90zq.patch.C4" android:enabled="true" android:exp
  <intent-filter>
    <action android:name="android.intent.action.BOOT_COMPLETED" />
  </intent-filter>
</receiver>
```

контроль запуска устройства

Mobile Security Framework – статический анализ



Static Analyzer

Information

Scan Options

Signer Certificate

Permissions

Android API

Browsable Activities

Security Analysis

Malware Analysis

Reconnaissance

Components

PDF Report

APP SCORES



Security Score 44/100

Trackers Detection 0/432

FILE INFORMATION

File Name .apk

Size 11.67MB

MD5 ae0efc20dc6bc4ba3626ad758140db4d

SHA1 c1e65053dac4ea59589e9a6a51ff867a8db5157a

SHA256 c6fa95d2619e08229b1c30034dffdc2f6c466745dd8c7f3f726b9266c8d574aa

DECOMPILED CODE

View AndroidManifest.xml

View Source

View Smali

Download Java Code

Download Smali Code

Download APK

App Name Настройщик

Package Name cmf0.c3b5bm90zq.patch

Main Activity cmf0.c3b5bm90zq.patch.C7

Target SDK 22 Min SDK 10 Max SDK

Android Version Name 1.1.1.0 Android Version Code 1

APPLICATION PERMISSIONS

android.permission.ACCESS_COARSE_LOCATION

dangerous

coarse (network-based) location

Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

Show Files

android.permission.ACCESS_FINE_LOCATION

dangerous

fine (GPS) location

Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery

Show Files

android.permission.CALL_PHONE

ANDROID API

API

FILES

GPS Location

Show Files

Execute OS Command

Show Files

Starting Activity

Show Files

TCP Socket

Show Files

Mobile Security Framework – статический анализ

 Malware Analysis

 Malware Lookup

 APKiD Analysis

 Behaviour Analysis

 Abused Permissions

 Server Locations

APKiD ANALYSIS



Search:

DEX

↑

classes.dex

DETECTIONS

↓

FINDINGS

↑

Anti-VM Code

DETAILS

↓

Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL check

Compiler

dexlib 2.x

BEHAVIOUR ANALYSIS



RULE ID	BEHAVIOUR	LABEL	URLS
00188	Get the address of a SMS message	sms	
00191	Get messages in the SMS inbox	sms	
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	cmf0/c3b5bm90zq/patch/C11.java
00049	Query the phone number from SMS sender	sms collection	cmf0/c3b5bm90zq/patch/C10.java
00163	Create new Socket and connecting to it	socket	cmf0/c3b5bm90zq/patch/C11.java cmf0/c3b5bm90zq/patch/C5.java

A STRINGS

From APK Resource

Show all 1365 strings

From Code

Show all 428 strings

Статический анализ – поиск сетевых адресов

Источники поиска:

- ресурсы
(AndroidManifest.xml, <res>, <assets>)
- исходный код

Методы поиска:

- поиск строк "host", "port", "http://" и т.п.
- поиск по регулярному выражению (ip-адрес)
- поиск по Java-методам, напр. "Socket" "URLConnection", "OkHttpClient"
- поиск методов декодирования/ дешифраторов в коде (напр. Base64 / XOR / AES)

```
<string name="app_name">Настройщик</string>
<string name="gp">01011</string>
<string name="h">tcp.cloudpub.ru</string>
<string name="n">test</string>
<string name="p">26268</string>
<string name="ps">null</string>
<string name="s">test 1</string>
<string name="search_menu_title">Search</string>
<string name="status_bar_notification_info_overflow">
<string name="v">1.1.1.0</string>
```

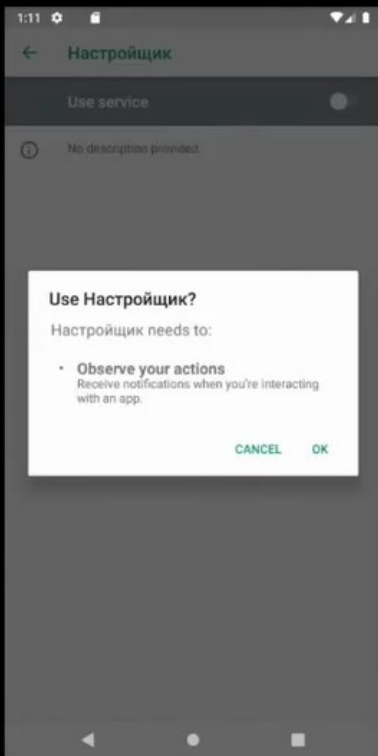
В тестовом арк-файле SpyNote v.6.4 информация об адресе управляющего сервера находится в ресурсах (res/values/strings.xml)

MobSF + AVD (Android 10) + Wireshark

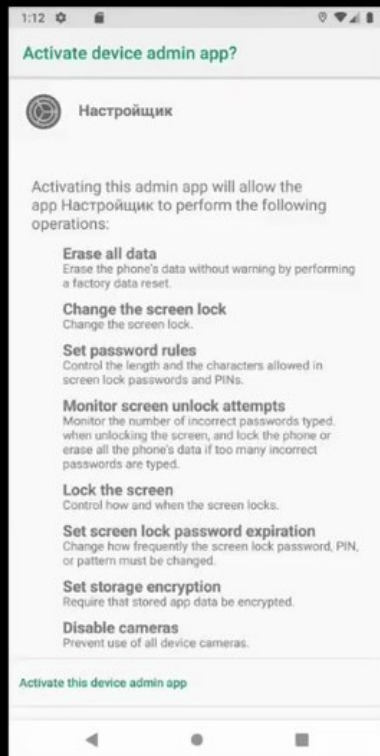
Создание каталога
`/data/media/0/test 1/`

1. APK приложения для склейки*
2. Лог файл SpyNote (записи keylogger)

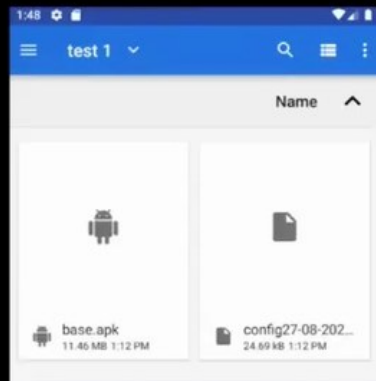
Текстовые данные + Base64



Активация
Accessibility Service



Активация
Device Admin App



```
2DlLKVS0HdEUBRCKh3Sq0j+wukQudAbiYimTdFlfPU0x/tN/1/dS1b/X7x60YAAAAASUVORKSCYII=10251Activate this
device admin app10251com.android.settings1025113:12 PM10250-110251Apps
list10251com.google.android.apps.nexuslauncher1025113:12 PM10250-110251Calculator, Calendar,
Camera, Chrome, Clock, Contacts, Drive, Files, Gmail, Google, Maps, Messages, Phone, Photos,
Play Movies & TV, Play Music, Settings, WebView Browser Tester, YouTube,
Настройщик10251com.google.android.apps.nexuslauncher1025113:12 PM10250-110251Apps
list10251com.google.android.apps.nexuslauncher1025113:12 PM10250-110251Package
installer10251com.google.android.packageinstaller1025113:12 PM10250-110251Настройщик, For your
security, your phone is not allowed to install unknown apps from this source., CANCEL,
SETTINGS10251com.google.android.packageinstaller1025113:12 PM10250-110251Package
installer10251com.google.android.packageinstaller1025113:12
PM10250-110251SETTINGS10251com.google.android.packageinstaller1025113:12
PM10250iVBORw0KGgoAAAANSUHEugAAABGAAAYCAYAAADgdz34AAAAABHNCSVOICAgIfAhkIAAAAH1JREFUSImN1U9sG0Uux
n9vdr12mig0TQE1XJBoJcqB3jlRcuF1XCrEBQ71UiGhXhLqTZzUcVLbat1W6EJFSEUCYEKfw4IceHMVSABErTc+kegOiUhx
PbuPA673j9eJ82TLNvfPm+7828mRGeFJcuvIEx340d0/AMK9e+2W+67DnS8neAiScaiJR6LHcQbX04
+uEkfwf7YMQj4XCYSuPs5Dj7bT882P3VRfRktCMPTaCalEgZ3NW9eL4ChrnDlGa+XecMQkt2wuNHdZ1vYE6Zlw6GdnC0uVu
voI9yIfuc6J7VQFg9VGiBUDL181V8VRxbURSQt3xD3A5kiJwJZrcax5QfKCTb8H4MZ/D2wddrfwXjvLhGMM2ynSU9dwudeJ
ifC1r1b1NZAFInL12zPvcPr54wXC+S++
5PPbPwHw1skX+f19s4Wc2/fu8cqtT8CY4WqcnUPYGBhLpusvsvHLrw1MkGlzK07d5n1Fwt5p+bmcLd1l0pk198GAk+
1a/SDTHx+1dFvKsfP/gw610hoga/x+SKPLYm8
```

Динамический анализ – анализ сетевого трафика

Без доступа к интернету

DNS-запрос по доменному имени "tcp.cloudpub.ru" без ответа

7	15.965001000	192.168.232.2	10.0.2.3	DNS	77	Standard query 0x486c AAAA tcp.cloudpub.ru
---	--------------	---------------	----------	-----	----	--

Адрес нашего управляющего сервера

С доступом к интернету

DNS-запрос по доменному имени "tcp.cloudpub.ru" с ответом

40	35.752435000	192.168.232.2	10.0.2.3	DNS	77	Standard query 0x4fab AAAA tcp.cloudpub.ru
41	35.803319000	10.0.2.3	192.168.232.2	DNS	132	Standard query response 0x4fab AAAA tcp.cloudpub.ru SOA ns1.reg.ru
42	35.804194000	192.168.232.2	10.0.2.3	DNS	77	Standard query 0x0fa8 A tcp.cloudpub.ru
43	35.862414000	10.0.2.3	192.168.232.2	DNS	93	Standard query response 0x0fa8 A tcp.cloudpub.ru A 87.242.106.13

Установление TCP-соединения с "87.242.106.13" и обмен данными

44	35.864728000	192.168.232.2	87.242.106.13	TCP	76	55016 → 26268 [SYN] Seq=0 Win=65535 Len=0 MSS=1360 SACK_PERM TSval=4294962891 TSecr=0 WS=64
45	35.909881000	87.242.106.13	192.168.232.2	TCP	60	26268 → 55016 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
46	35.910227000	192.168.232.2	87.242.106.13	TCP	56	55016 → 26268 [ACK] Seq=1 Ack=1 Win=65535 Len=0
47	36.942962000	192.168.232.2	87.242.106.13	TCP	1416	55016 → 26268 [ACK] Seq=1 Ack=1 Win=65535 Len=1360
48	36.943365000	192.168.232.2	87.242.106.13	TCP	184	55016 → 26268 [PSH, ACK] Seq=1361 Ack=1 Win=65535 Len=128
49	36.944045000	87.242.106.13	192.168.232.2	TCP	56	26268 → 55016 [ACK] Seq=1 Ack=1361 Win=8760 Len=0
50	36.944117000	87.242.106.13	192.168.232.2	TCP	56	26268 → 55016 [ACK] Seq=1 Ack=1489 Win=8760 Len=0
51	38.112548000	87.242.106.13	192.168.232.2	TCP	74	26268 → 55016 [PSH, ACK] Seq=1 Ack=1489 Win=8760 Len=18
52	38.112843000	192.168.232.2	87.242.106.13	TCP	56	55016 → 26268 [ACK] Seq=1489 Ack=19 Win=65535 Len=0
53	38.553716000	87.242.106.13	192.168.232.2	TCP	63	26268 → 55016 [PSH, ACK] Seq=19 Ack=1489 Win=8760 Len=7
54	38.553985000	192.168.232.2	87.242.106.13	TCP	56	55016 → 26268 [ACK] Seq=1489 Ack=26 Win=65535 Len=0

Полезная нагрузка пакета

Gzip сигнатура

30	50 10 ff ff e3 df 00 00	31 34 38 33 00 1f 8b 08	P..... 1483....
40	00 00 00 00 00 00 00 ad	56 c9 d2 ab b8 0e 7e 95	 V.....
50	b3 ea 0d 8b 30 84 00 8b	5e 18 30 33 01 33 85 b0	...0... ^03-3..
60	23 cc 43 80 30 87 a7 bf	9c bf bb ba ba ee ba e5	#-C-0...

→ unzip → Decode Base64 → .jpeg

Image	Victim Name	Country	Flag	Remote Address	Model
	test	n/a		127.0.0.1:61018	GOOGLE

Админка управляющего сервера

Сведения об установке

«frosting.db»

/data/data/com.android.vending/databases/

«verify_apps.db»

/data/data/com.android.vending/databases/

«packages.xml»

/data/system/

- имя пакета
- путь к файлу приложения
- время установки
- инициатор установки
- установщик приложения

/data/data/<package name> – каталог с данными приложения

Установленные приложения\История установок приложений			
▼	Время последнего обновления (Москва)	ID приложения	Путь к APK
	17.12.2024 16:32:50 (UTC +3)	com.whh.premium	base.apk

Установленные приложения\Верифицированные приложения 1/1	
▼	Название
	Энергосбыт

package

```
name = com.whh.premium
codePath = /data/app/~5fmOrSm3aKS8E9SKjK9I9w==/com.whh.premium-ITqA8cmV9JJiomuIF-zZYw==
nativeLibraryPath = /data/app/~5fmOrSm3aKS8E9SKjK9I9w==/com.whh.premium-ITqA8cmV9JJiomuIF-zZYw==/lib
publicFlags = 945339972
privateFlags = -1409282048
ft = 193d4d23fe8
ut = 193d4d24462
version = 3000
userId = 10366
installer = com.google.android.packageinstaller
packageSource = 3
installInitiator = com.google.android.packageinstaller
installOriginator = org.telegram.messenger
loadingProgress = 1
domainSetId = aa070b91-1d0d-4671-874c-7b6e13391cc4
```

ft = 193d4d23fe8

⌚ Unix Milliseconds (Java Time)

2024-12-17 16:32:49.0000000 +03:00

ut = 193d4d24462

⌚ Unix Milliseconds (Java Time)

2024-12-17 16:32:50.1460000 +03:00

- ft – время последнего изменения
- it – время первой установки
- ut – время последнего обновления

Поиск по имени пакета

newbatterystats

/data/log/batterystats/

устройства Samsung

```
+1h20m36s334ms (2) 095 pkginst=57401:"com.iproxy.android"  
+1h20m36s503ms (2) 095 pkginst=57401:"com.iproxy.android"  
+1h20m36s594ms (2) 095 pkginst=57401:"com.iproxy.android"  
+1h20m36s639ms (2) 095 pkginst=57401:"com.iproxy.android"  
  
+9h42m55s610ms (2) 060 pkgunin=0:"com.iproxy.android"  
+9h42m55s666ms (2) 060 pkgunin=0:"com.iproxy.android"
```

```
2025-06-13 18:02:41.662: START INSTALL PACKAGE: observer{229554387}  
    stagedDir{/data/app/vmdl53600148.tmp}  
    stagedCid{null}  
    pkg{com.example.application}  
    Request from{com.google.android.packageinstaller}
```

```
2025-06-13 19:49:11.541: START DELETE PACKAGE: observer{216981792}  
    pkg{com.example.application}, user{0}, caller{10085} flags{2}
```

pm_debug_info.txt

/data/log/

Прочие артефакты

Встроенный антивирус приложения «СберБанк»

«threats.db»

/data/data/ru.sberbankmobile/databases

```
«{"virusName":"HEUR:Trojan-  
Spy.AndroidOS.SpyNote.bz","objectName":"/  
data/ app/~~aUtq8Y3Z3RGSyUUJ9fuMuA==/  
ate.asking.humanity-J32gBHsvrskliOSBIH  
L_Kw==/base.apk","fileFullPath":"/data/app/  
~~aUtq8Y3Z3RGSyUUJ9fuMuA==/  
ate.asking.humanity-  
J32gBHsvrskliOSBIHL_Kw==/  
base.apk","fileHash":null,"package Name":  
"ate.asking.humanity","severityLevel":"HIGH","ap  
plication":true,"adminThreat":false,"cloudCheckF  
ailed":false}»
```

Лог SpyNote

«log-yyyy-mm-dd.txt»

/data/media/0/Config/sys/apps/log

decode from Base64

Графический интерфейс
системы#[Панель уведомлений, RT-10,
Развернуть, Bluetooth, Развернуть, .
Нажмите для установки режима вибрации.
При этом могут также выключиться звуки
в службе специальных возможностей.,
19:59, чт, 21 нояб., Открыть настройки., NFC,
Вибровывозов, Bluetooth disconnected., VoLTE
для карт SIM1 и SIM2, 90 %, Удалить все
уведомления]#5