

RSA® Conference 2019 Asia Pacific & Japan

Singapore | 16–18 July | Marina Bay Sands



BETTER.

SESSION ID: FLE-R03

Tessa88: Uncovering the True Identity of the Notorious Hacker

Andrei Barysevich

Director of Advanced Collection
Recorded Future
@DeepSpaceEye

#RSAC

tessa88 in the media

TEC

Home » Technology

The Twitter

Image: elyKJ/Flickr

MYSPACE | By [Lorenzo Franceschi-Bicchieri](#) | Jun 17 2016, 12:37pm

on JUNE 9, 2016

f FA

Russ

This Is The Hacker Allegedly Behind The LinkedIn and MySpace Megabreaches

Who is Tessa88, the other hacker who's spreading and selling hacked passwords stolen from your social networks?

SHARE TWEET

SHCC2017
Asia Pacific & Japan

The Actor's Indicators Known Before Investigation

- Usernames:
 - tessa88
 - stervasgoa
 - jannet93
- Jabbers:
 - tessa88@exploit[.]im
 - tessa88@xmpp[.]jp
 - mrfreeman777@xmpp[.]jp
 - darksideglobal@exploit[.]im
- Email addresses:
 - firetessa@yahoo[.]com
- Twitter:
 - @firetessa
- ICQ:
 - 740455
- Website:
 - darkside.global.deer[.]io
- Bitcoin wallet:
 - 1AbMLfZPB59H6gwqWHnA9bnUQt3JB2gAoC

Female? Male? Two Different People?

- tessa88
- stervasgoa [bitch from Goa]
- jannet93

www.iconexperience.com



www.iconexperience.com

www.iconexperience.com

TraX - a Member of 0Day Forum Claimed That He Met tessa88 in Person, the Actor is a Man



TraX's Post in Recorded Future Platform Saying That tessa is a Man

Cached Document ×

Title Killing Tessa
Author TraX
Downloaded Jul 11, 2018, 20:24
Original URL <http://qzbkwsfv5k2oj5d.onion/thread-11787-post-40392.html#pid40392>

Translate All

```
1. @DealMan it's not she by the way it's he and yes he do look like girls if you
2. ask me
```

CLOSE

OSINT for “tessa88” Revealed the Imgur Account “tarakan72511”

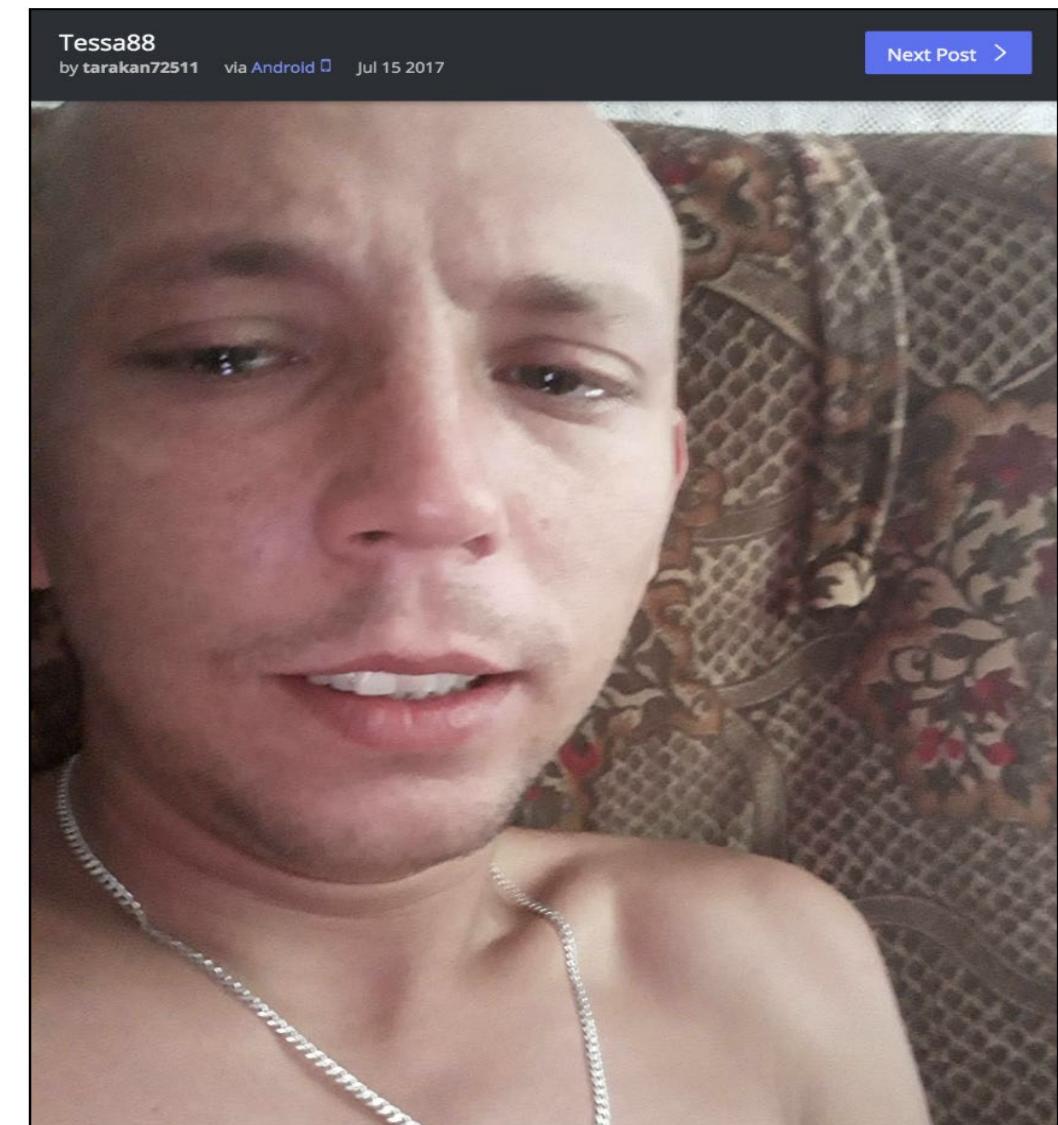
We used Google Advanced Search using a combination “intitle:tessa88”

The screenshot shows a Google search results page with the query "intitle:tessa88" entered in the search bar. The results are filtered under the "All" tab. The search results include:

- Tessa88 hacker continues rampage, puts Twitter account info up for ...**
https://www.scmagazine.com › Home › News ▾
Jun 9, 2016 - Already linked to the LinkedIn, Myspace, Tumblr and VK.com breaches, Russian hacker Tessa88 earlier this week claimed access to 379 ...
- Tessa88 Archives - Hacking Insider**
www.hackinginsider.com/tag/tessa88/ ▾
In light of the news that the Russian seller, who goes by the name of Tessa88, claimed in an encrypted chat to have obtained Twitter's database. This includes ...
- Tessa88 - Album on Imgur**
https://imgur.com/gallery/3SBSY
Jul 14, 2017 - Post with 15 votes and 73 views. Shared by tarakan72511. Tessa88.

We Identified an Alleged Photo of tessa88

The user tarakan72511 [posted](#) a photo of the man titled “Tessa88” in 2017, whose body type and hairstyle is similar to the individual depicted in the picture posted by TraX on 0Day forum.



tarakan
72511

Connection Between Threat Actors tessa88 and paranoid777

- The username “tarakan72511” likely belongs to the actor paranoid777, who used the Jabber account **tarakan72511@chatme[.]im** on several underground forums in 2017.
- Recorded Future earlier investigated the activity of paranoid777. This actor, as well as tessa88, had previously been selling stolen email databases from the large social media and technology companies. The actors have not been observed corresponding with one another openly on dark web forums.



tarakan72511@chatme[.]im



paranoy777 Used the jabber “tarakan72511@chatme[.]im” on Antichat and Other Forums

The screenshot shows a forum post with several user profiles and a highlighted email address.

User Profiles:

- vasiliy18** (New Member): Registration: 24.01.2016, Messages: 6, Approvals: 0, Reputation: 0. Last activity: 23.02.2017 by paranoy777.
- Keylogger** (New Member): Registration: 5.09.2012, Messages: 4, Approvals: 0. Last activity: 23.02.2017.
- paranoy777** (Member): Registration: 23.01.2016, Messages: 71, Approvals: 23. Last activity: 23.02.2017.

Text Content:

Не работает жаба говоришь ?
Просил человека отписать тебе в лс на ачате
скриншот:
CHAT.RU

12.02.2017

привет, дай контакт

highlighted_email: tarakan72511@chatme.im

Connection Between the Actors **paranoy777** and **daykalif**

Underground forum search for the mentioned above jabber account **tarakan72511@chatme[.]im** revealed a claim by the actor **MeXaHHuK**, who posted on 0Day forum that **daykalif** is a Russian-speaking scammer involved in the sale of large databases, and used the Jabber accounts **daykalif@xmpp[.]jp** and **tarakan72511@chatme[.]im**.

These facts mean that **paranoy777** and **daykalif** might be the same individual.

MeXaHHuK's Post on 0DAY Accused daykalif of Scamming

daykaliff - russian Scammer		Threaded Mode Linear Mode
Author	Message	
MeXaHHuK  Junior Member  Posts: 36 Joined: Oct 2016 Reputation: 0 Jabber:	<p>BLACK LIST Contacts: daykalif@xmpp.jp tarakan72511@chatme.im</p> <p>Daykalif offers to buy interesting large databases. Displays screenshots, makes lines, but I think that they are not all real. The database is not his, he takes them if he takes, it is unknown who. By and large it's a hoax.</p> <p>But most importantly! Do not transfer money to him first! After you transfer money to him, he will deceive you!</p> <p>After transferring money to him, he will ignore you! I tried several times to make a deal with him, and every time he deceived me, then he said that he had some problems, he blurted out or on departure and then offered an interesting database, and then again he wanted to cheat.</p>	Post: #1
12-03-2017	<input type="button" value="email"/> <input type="button" value="pm"/> <input type="button" value="find"/> <input type="button" value="rep"/>	<input type="button" value="report"/>



tarakan72511@chatme[.]im



daykalif@xmpp[.]jp
tarakan72511@chatme.im



Connection Between the Actors **paranoy777** and **daykalif**

26.01.2017



paranoy777
Banned

Регистрация: 23.01.2016
Сообщения: 77
Одобрения: 24
Репутация: 10

Пожаловаться

- According to the media, **daykalif sold** the Rambler and Last.fm databases to the currently-defunct LeakedSource in September 2016.
- On January 26, 2017, during the discussion of recent takedown of the **LeakedSource** by the FBI, between members of the Antichat forum, **paranoy777 admitted** that he was happy to see the website being seized
“I known this “rat” personally, he deserved it. He should have paid on time.”
- Another evidence that **paranoy777** and **daykalif** are the same person who sold stolen databases to LeakedSource

LeakedSource is Back

[Home](#) [Register](#) [Purchase](#) [Blog](#) [API](#) [TOS](#) [FAQ](#) [Contact](#) [Leaked Sites](#) [Log in](#)



There are currently 2,649,875,832 / 3,109,103,084 accounts in our database.

[Click here to subscribe and view your Raw data! As low as \\$0.76 a day!](#)

Check for free to see if your email or account was hacked.

Search term

Search Term

Search type

Email

Wildcard (Limit first 200 results) ([What's wildcard?](#))

[Search](#)

ibmZZa0DAY, Another Alias of tarakan72511, paranoid777, and daykalif

Time ▾ Event Information

User name ibmZZa0DAY scammer and tarakan72511@chatme.im mentioned

MAR
2
2018

User name ibmZZa0DAY scammer

This other jabber tarakan72511@chatme.im a legit scammer i should say" [Forum Thread](#)

Source Flakka Forum by terminal on Mar 2, 2018, 17:21

<http://q6wh7jvr7pohmnwe.onion/topic/166> • [Reference Actions](#) • 1+ reference

tarakan72511@chatme[.]im belongs to **ibmZZa0DAY**, a member of the Flakka forum. The actor used the same jabber and was also accused of scamming.



tarakan72511@chatme[.]im

A large black vertical arrow pointing downwards from the "daykalif" node to the "ibmZZaODAY" node.



Analysis of tarakan72511's Imgur Account

The Imgur account also revealed that the actor is an avid dog-lover

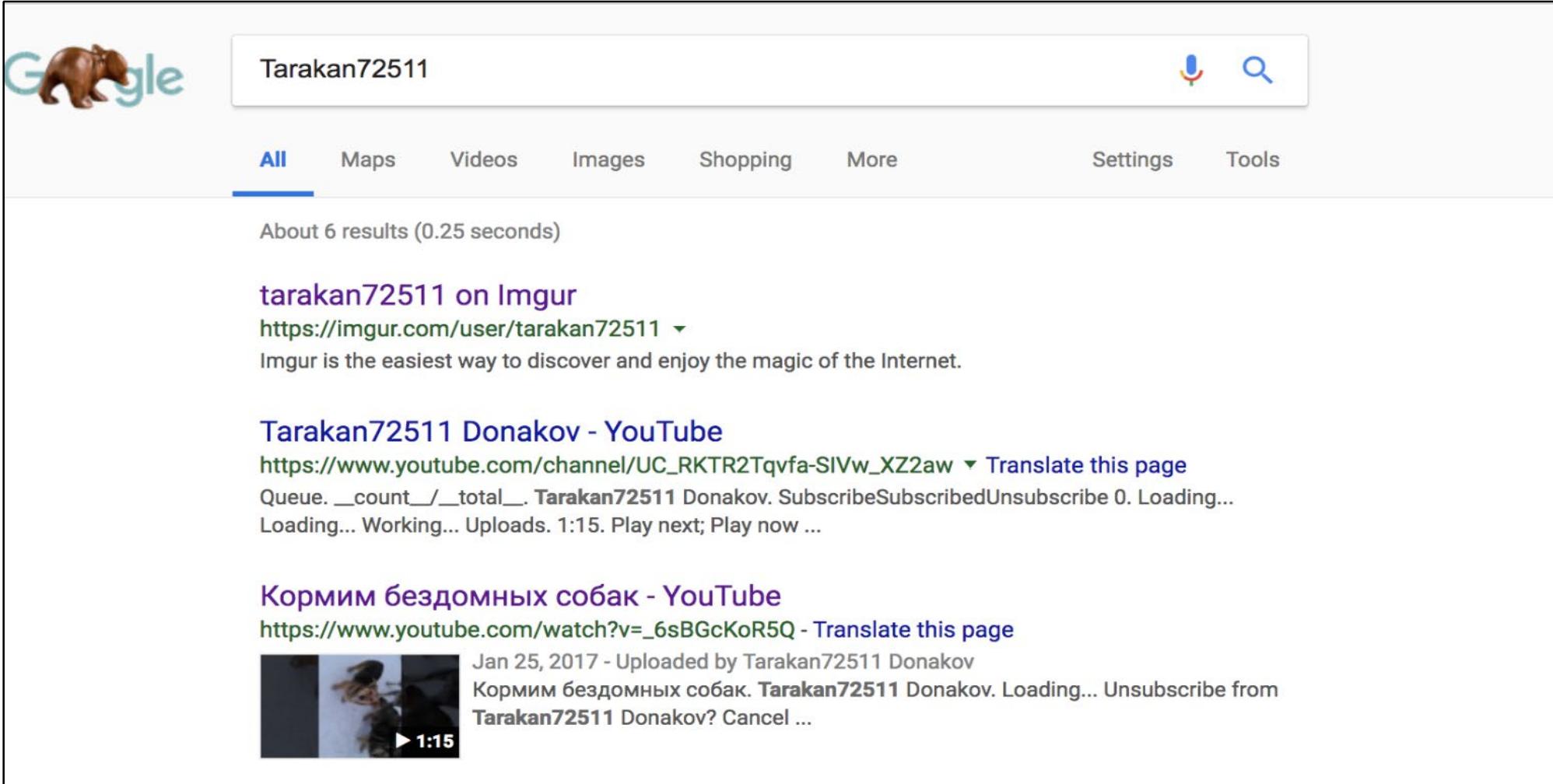
The screenshot shows the Imgur user profile for **tarakan72511**. The profile includes:

- Submitted images:** A grid of images including a multi-story residential building, a screenshot of a bank statement in Russian, a close-up of a dog's head, a dog climbing a tree, a view of a house through a window, and a screenshot of a file manager.
- Comments:** A sidebar with a list of comments, one of which discusses a dog named Vasya.
- Submitted images:** A section listing files uploaded to Imgur, such as "j2r" (54.81 MB), "damien2 data.rar" (18.25 MB), "dumps.rar" (31.31 MB), and "Evony.com_M..._unc_2016.txt" (374.27 MB).
- Gallery favorites:** A section showing favorite images.
- send message:** A button to send a message to the user.
- 88 reputation · since May 2017:** The user's current reputation and when it was last updated.
- Notoriety: Neutral**: The user's notoriety level.
- show list**: A link to view a list of users.

At the bottom of the page, there is a footer with links: Love Imgur? Join our team! · about · store · help · blog · request deletion · forum · terms · privacy · apps · api · advertise · ad choices. © 2018 Imgur, Inc.

Tarakan72511's YouTube video

OSINT for tarakan72511 revealed the YouTube user Tarakan72511 Donakov



A screenshot of a Google search results page. The search bar at the top contains the query "Tarakan72511". Below the search bar, the "All" tab is selected, along with other options like Maps, Videos, Images, Shopping, More, Settings, and Tools. A message indicates "About 6 results (0.25 seconds)". The first result is a link to "tarakan72511 on Imgur" with the URL <https://imgur.com/user/tarakan72511>. The description below the link says "Imgur is the easiest way to discover and enjoy the magic of the Internet.". The second result is a link to "Tarakan72511 Donakov - YouTube" with the URL https://www.youtube.com/channel/UC_RKTR2Tqvfa-SIVw_XZ2aw. The description includes "Translate this page", "Queue. __count__ / __total__.", and "Tarakan72511 Donakov. SubscribeSubscribedUnsubscribe 0. Loading... Loading... Working... Uploads. 1:15. Play next; Play now ...". The third result is a link to "Кормим бездомных собак - YouTube" with the URL https://www.youtube.com/watch?v=_6sBGcKoR5Q. The description includes "Translate this page", a thumbnail image showing a person feeding dogs, the upload date "Jan 25, 2017", and the uploader "Tarakan72511 Donakov". It also mentions "Кормим бездомных собак. Tarakan72511 Donakov. Loading... Unsubscribe from Tarakan72511 Donakov? Cancel ...".

Tarakan72511 Donakov's Video Showing Two Individuals Feeding Dogs

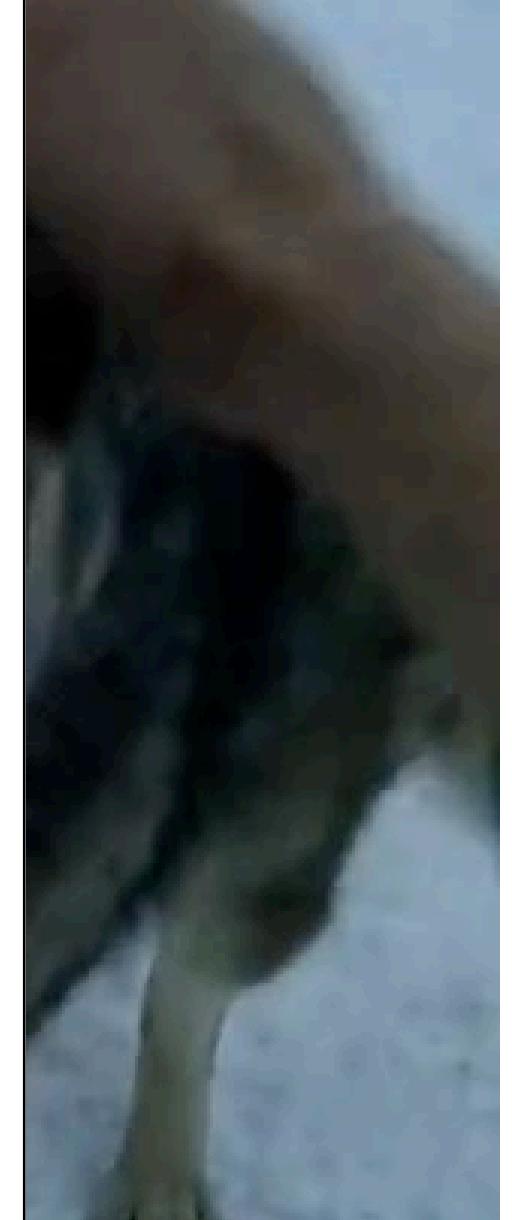
#RSAC



- The two individuals feeding the stray dogs in the video saying that they are residing in Penza, Russia.
- The vehicle make is Mitsubishi with the license plate "K 652BO 58." (we confirmed, that the car was bought by Donakov M.V on December 18, 2016).



#RSAC



**RSA®Conference2019
Asia Pacific & Japan**

Mitsubishi License Plate “K 652BO 58” and a Guy Fawkes Mask





Tarakan72511 Donakov

1 subscriber

HOME

- On the 00:56 second, a Guy Fawkes mask seen on the video. A similar mask used as an avatar of the Tarakan72511 Donakov YouTube profile and also worn by the person in the image shared by TraX.



- OSINT for “Донаков” (Donakov) from Penza/Пенза revealed that someone Донаков М.В. committed several crimes in Yaroslavl and Penza, Russia, including a car theft and traffic accident that happened while driving “Mitsubishi Lancer” in 2017.
- Prior moving to Penza in 2014, Donakov Maksim Vladimirovich/Донаков Максим Владимирович resided in Yaroslav, were mentioned in several articles on SuDact, the largest non-governmental Russian website of judicial records. According to the website, Donakov spent several years in prison prior to the car accident in 2017.



Court Records for Donakov M.V. (Донаков М.В.)

Донаков М.В.

Участник судебных дел

Последние документы:

1. Решение от 19 октября 2017 г. по делу № 2-1756/2017

Первомайский районный суд г. Пензы (Пензенская область) - Гражданские и административные
Суть спора: 2.145 - Иски о возмещении ущерба от ДТП (кромеувечий и смерти кормильца)

2. Постановление от 13 сентября 2017 г. по делу № 5-587/2017

Ленинский районный суд г. Пензы (Пензенская область) - Административные правонарушения

3. Апелляционное постановление от 27 марта 2014 г. по делу № 22-423/2014

Ярославский областной суд (Ярославская область) - Уголовное

4. Приговор от 20 февраля 2014 г.

Кировский районный суд г. Ярославля (Ярославская область) - Уголовное

- OSINT for Maxim Donakov revealed several profiles in the Russian social media Odnoklassniki. The first profile belongs to a man residing in Yaroslavl and who was born on July 2, 1989.



The 1st Donakov's Odnoklassniki Profile

This profile indicates his date of birth July 2, 1989 and residence in Yaroslavl, Russia

The screenshot shows Maxim Donakov's profile on the Odnoklassniki social network. At the top, there is a large profile picture of him wearing a red hooded jacket and a blue face mask, looking out of a car window. Below the picture, his name "Maxim Donakov" is displayed, along with the date "Last visit: 9 Sept 2013". There are three main action buttons: "Add to friends", "Write", and "Send a gift". On the left side of the profile, there are several status updates: "Date of birth July 2 1989 (29 years old)", "Lives in Ярославль", "Subscriptions 2 people", and a link to "More information about Maxim". Below this, a section titled "Friends 3" shows two friend profiles: "Алексан..." and "Леночка". The main content area features a news feed with the latest update: "Maxim Donakov received a birthday gift from Одноклассников" posted on "2 Jul 2015". This update includes a decorative graphic of a cupcake with the letters "OK" on it and the Russian text "С ДНЕМ РОЖДЕНИЯ". At the bottom of the news feed, there is a "Like" button with a count of "0".

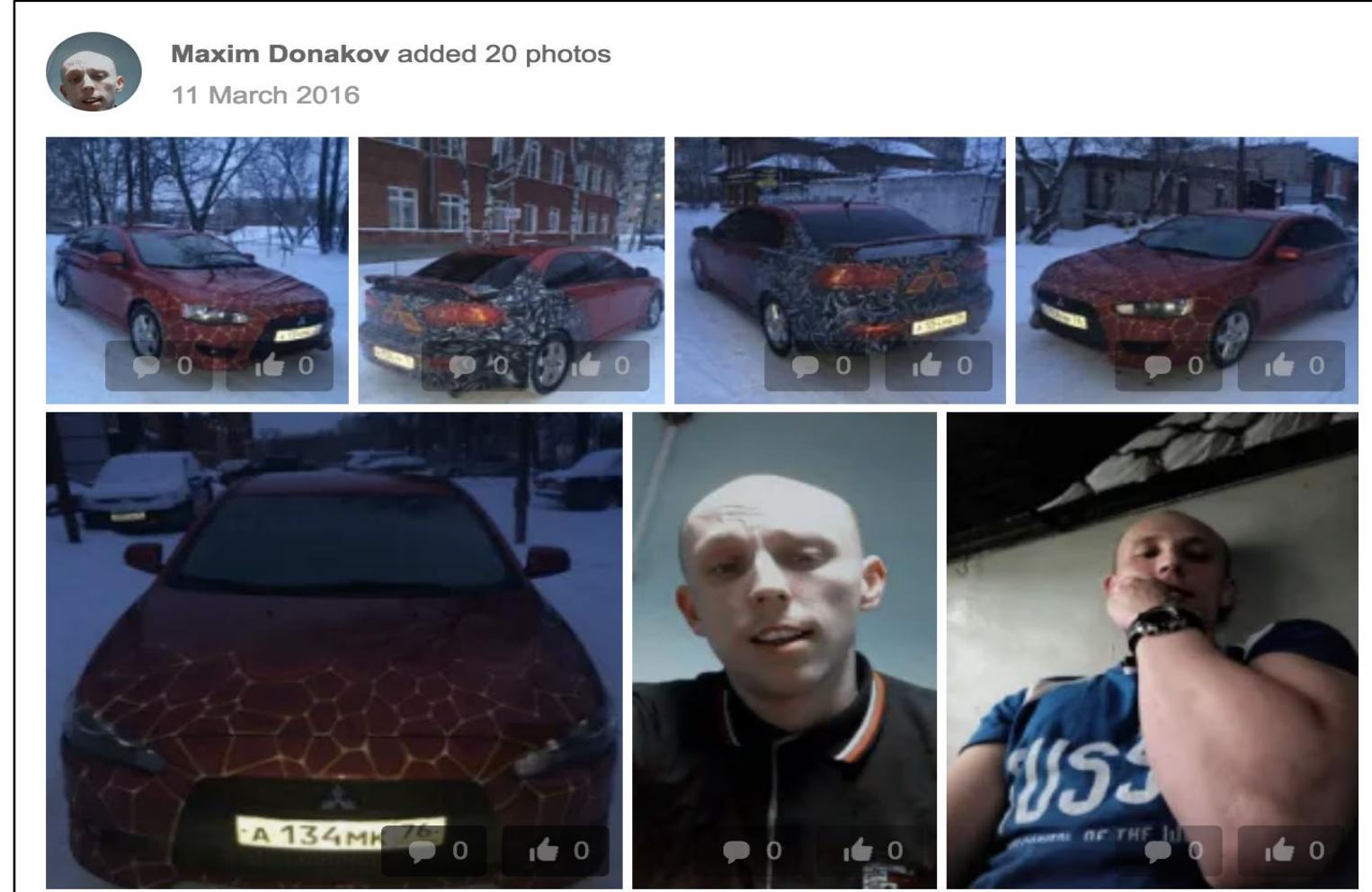
M.Donakov`s Odnoklassniki Profile #2 (OK.RU)

Date of birth - July 2, 1989

The screenshot shows Maxim Donakov's profile on Odnoklassniki. At the top, there is a large profile picture of him, followed by his name "Maxim Donakov" and the date of birth "July 2 1989 (29 years old)". Below this, there are buttons for "Add to friends", "Write", "Send a gift", and more options. To the right, it says "Last visit: 1 May". On the left sidebar, there are sections for "Date of birth", "Subscriptions", and "Friends 8". The main feed shows a post from Maxim about receiving a birthday gift from the site, accompanied by a decorative cake graphic with the text "С ДНЕМ РОЖДЕНИЯ" and "OK".

Photos of Donakov and Mitsubishi Lancer on the 1st OK.RU

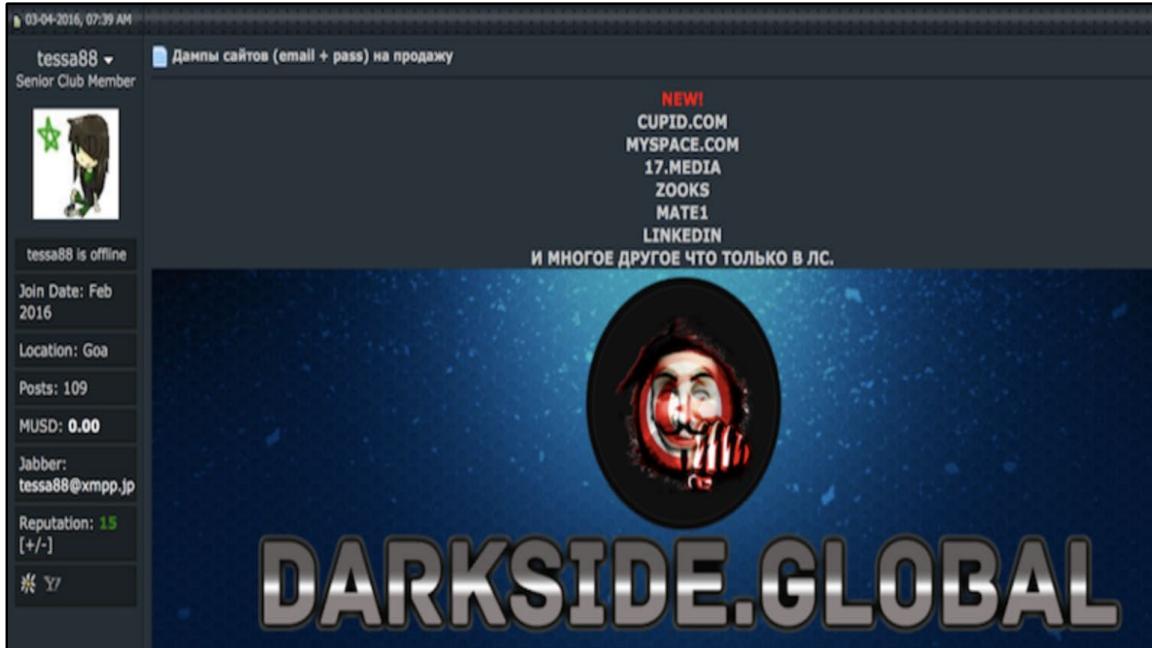
Posted images depict the same individual seen in the Imgur image from tarakan72511, and Mitsubishi Lancer with the license plate “A 134MK 76” mentioned in the court records



The 2nd OK.RU Profile Contains an Image of the Avatar Used by tessa88^{#RSAC} on Multiple Underground Forums



OK.RU profile page for Maxim Donakov. The profile picture is a Guy Fawkes mask. Below the profile picture, there are buttons for 'Comment' (0) and 'Like' (0). The user's name is Maxim Donakov, 29 years old, from Russia. A mobile album was posted on March 11, 2016. There are links for 'Full screen' and 'Get a link'. At the bottom, there is a link to 'Log in or sign up to add a comment'.



Screenshot of a forum post by tessa88. The post title is 'Дампы сайтов (email + pass) на продажу'. The user information shows tessa88 is offline, Senior Club Member, joined in Feb 2016, location Goa, 109 posts, MUSD 0.00, Jabber tessa88@xmpp.jp, Reputation 15. The post content includes a link to 'DARKSIDE.GLOBAL' which features a Guy Fawkes mask profile picture. The sidebar lists 'NEW!' sites for dump sale: CUPID.COM, MYSPACE.COM, 17.MEDIA, ZOOKS, MATE1, LINKEDIN, and many others.

- The analysis of the second Odnoklassniki profile revealed that it was linked to another profile created under the username “Ядовитый Таракан” (Yadovitiy Tarakan/Toxic cockroach) who is allegedly residing in Pervomaysk, Ukraine.
- The profile photo of the person depicted on it resembles Donakov Maxim very closely. Pervomaysk is Maxim Donakov `s real place of birth. We assess with a high degree of confidence that this profile also belongs to Donakov Maxim.



The Third OK Profile Identified

The screenshot shows a social media profile for a user named Maxim Donakov. The profile picture is a close-up of a young man with short hair, smiling. Below the profile picture, there are two small icons: a compass rose and a heart. The user's name, "Maxim Donakov", is displayed in a large black font. Below the name is an orange button with the text "Add to friends". On the left side of the profile, there is a sidebar with the following information:

- Date of birth July 2 1989 (29 years old)
- Subscriptions 1 person
- [More information about Maxim](#)

Below the sidebar, there is a section titled "Friends 8" which lists several user profiles. One profile, "Ядовитый", is highlighted with a red rectangular box. The names listed are: Данил, Ядовитый, Александ..., агбар.

On the right side of the profile, there is a "News Feed" section with tabs for "News Feed", "Friends 8", and "Photos". The "News Feed" tab is selected. Below the tabs, there are filters: "All", "Important", "Photos", and "Posts". A recent post from Maxim Donakov is shown, featuring a small profile picture and the text "Maxim Donakov received..." followed by "2 Jul". At the bottom of the profile page, there is a decorative graphic of a two-tiered cake with strawberries, blueberries, and mint leaves, with the word "OK" written on it.

The 3rd Donakov's OK.RU Profile Under the Username “Ядовитый Таракан”

#RSAC

The image of the individual resembles Donakov

The screenshot shows a user profile on the OK.RU social network. The profile picture is a man wearing sunglasses and a black t-shirt. Below the profile picture, there is a banner for the "MOTOCROSS WORLD CHAMPIONSHIP" event. The profile information includes the username "Ядовитый Таракан" with a lock icon, the last visit date "20 Jun 2017", and three buttons: "Add to friends", "Write", and "Send a gift". Below the profile, there is a navigation bar with links: News Feed, Friends 29, Photos 4, Groups, Games, Posts, Videos, and Other ▾. A large padlock icon is centered on the page, indicating that the profile information is available only to friends.

Information is available only to friends

Another Evidence That paranoid777 is Donakov

On February 17, 2016, paranoid777 mentioned on [Antichat](#) forum that his real date of birth is in summer (as well as Donakov's)

День рождения в соц.сети
Discussion in 'Болталка' started by paranoid777, 17 Feb 2016.

17 Feb 2016 #1



Сменил дату рождения в соц.сети и меня стали поздравлять с днём рождения близкие мне люди.
Хотя день рождения летом))
Я понял что вообще, даже близкие мне люди не знают про меня ничего((((

paranoid777
Banned

Joined: 23 Jan 2016
Messages: 77
Likes Received: 24
Reputations: 10

Last edited: 17 Feb 2016

Kapaso likes this.



tarakan72511@chatme[.]im

A blue horizontal arrow pointing from left to right, indicating a connection between the two users.



daykalif@xmpp[.]jp
tarakan72511@chatme.im

A dark blue horizontal arrow pointing from left to right, indicating a connection between the two users.



tarakan72511@chatme[.]im

A thick black vertical arrow pointing downwards, indicating a connection between daykalif and ibmZZaODAY.



Additional Evidence That paranoid777 is Donakov

The image shows a screenshot of a forum profile. At the top, it says "khaym" in large black letters. Below it, there are two sections: "байт" (post) and "目" (profile picture). Underneath, the profile information is listed:
Группа: ~~BANNED~~
Сообщений: 14
Регистрация: 26.11.2015

At the bottom, it says "Репутация: -1" and "(1% - плохо)".

Coincidentally, the initial activity of the second OK.RU profile for Maxim Donakov was detected on November 26, 2015, which is the same day the user “khaym,” registered on forum Exploit.

Connection Between the Actors paranoid777 and khaym

Insikt Group has confirmed earlier that “khaym” is another moniker used by paranoid777, who was banned on Exploit forum because of scamming. The actor used the following jabber accounts on the forum:

- khaym@exploit[.]im
- Bruno123123@yax[.]im
- demigrooop@exploit[.]im

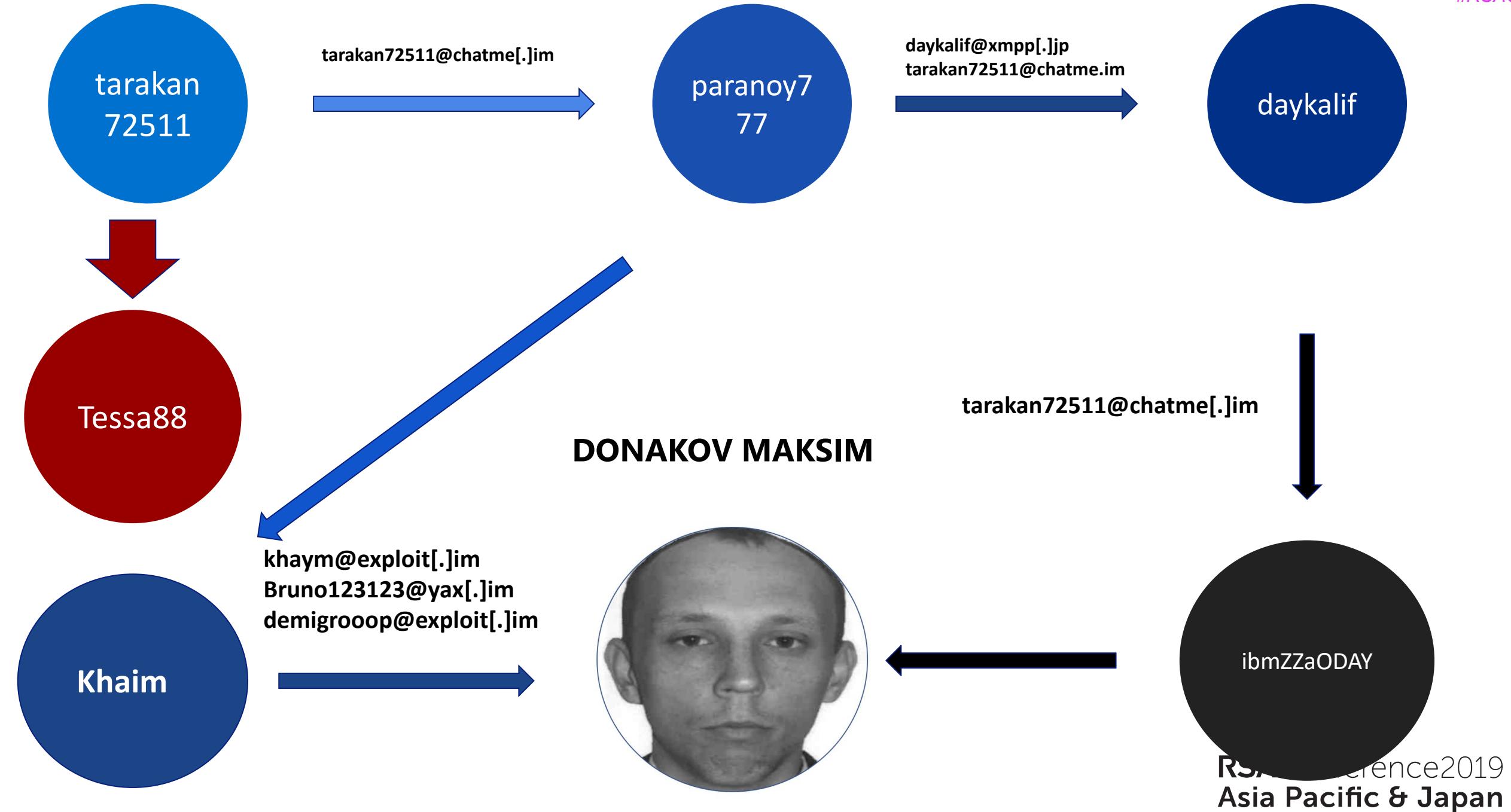
- Sources confirmed that Maxim (Maksim) Donakov is a real person with a real date of birth July 2, 1989. He conducted several crimes in Yaroslavl and Penza, including vehicle theft and traffic accident.
- The existence of several profiles can be explained with his arrest. His last visit to the 2nd OK.RU profile was on September 9, 2013. The 1st profile was started in November 2015.
- According to the information on SuDact website, Donakov was released under police supervision but was then imprisoned after committing another crime in 2014.



M.Donakov`s Passport Photo



M. Donakov's passport photo greatly resembles the alleged photo of tessa88 posted by the Imgur user tarakan72511 and a person depicted in Odnoklassniki profiles



Paranoy777 -> Khaim Link

Executive Summary

Paranoy777, also known as "Khaym" and "0db2016", is a member of several cybercriminal communities, including the top-tier Exploit forum, and has been primarily operating in the Russian-speaking underground. The actor's earliest involvement in illegal activities can be attributed to his registration on Exploit forum in November 2015.

Who Was the Real Hacker?



SELLER



HACKER



DONAKOV MAKSIM

Tessa88@bk.ru Link to Denisova

(4862) 751-318
info@oreluniver.ru

ВИДЫ ДЕЯТЕЛЬНОСТИ ▶ ОБРАЗОВАТЕЛЬНАЯ ▶ НАУЧНАЯ ▶ МЕЖДУНАРОДНАЯ ▶ СОЦИАЛЬНАЯ ▶ ВОСПИТАТЕЛЬНАЯ ▶
НАШ УНИВЕРСИТЕТ ▶

Денисова Татьяна Геннадьевна



Занимаемые должности:
инженер Контрактная служба

[Контактная информация ▾](#)

Образование:

В 2006 году окончила среднюю общеобразовательную школу № 20 им. Героя Советского Союза Л.Н. Гуртьева. В 2011 году, с отличием окончила ФГБОУ ВПО "Госуниверситет-УНПК" по специальности "Автоматизация технологических процессов и производств".

Квалификация:

инженер

Повышение квалификации и профессиональная переподготовка:

С 2011-2014 . проходила обучение в аспирантуре по специальности 05.13.06 "Автоматизация и управление технологическими процессами и производствами (по отраслям)."

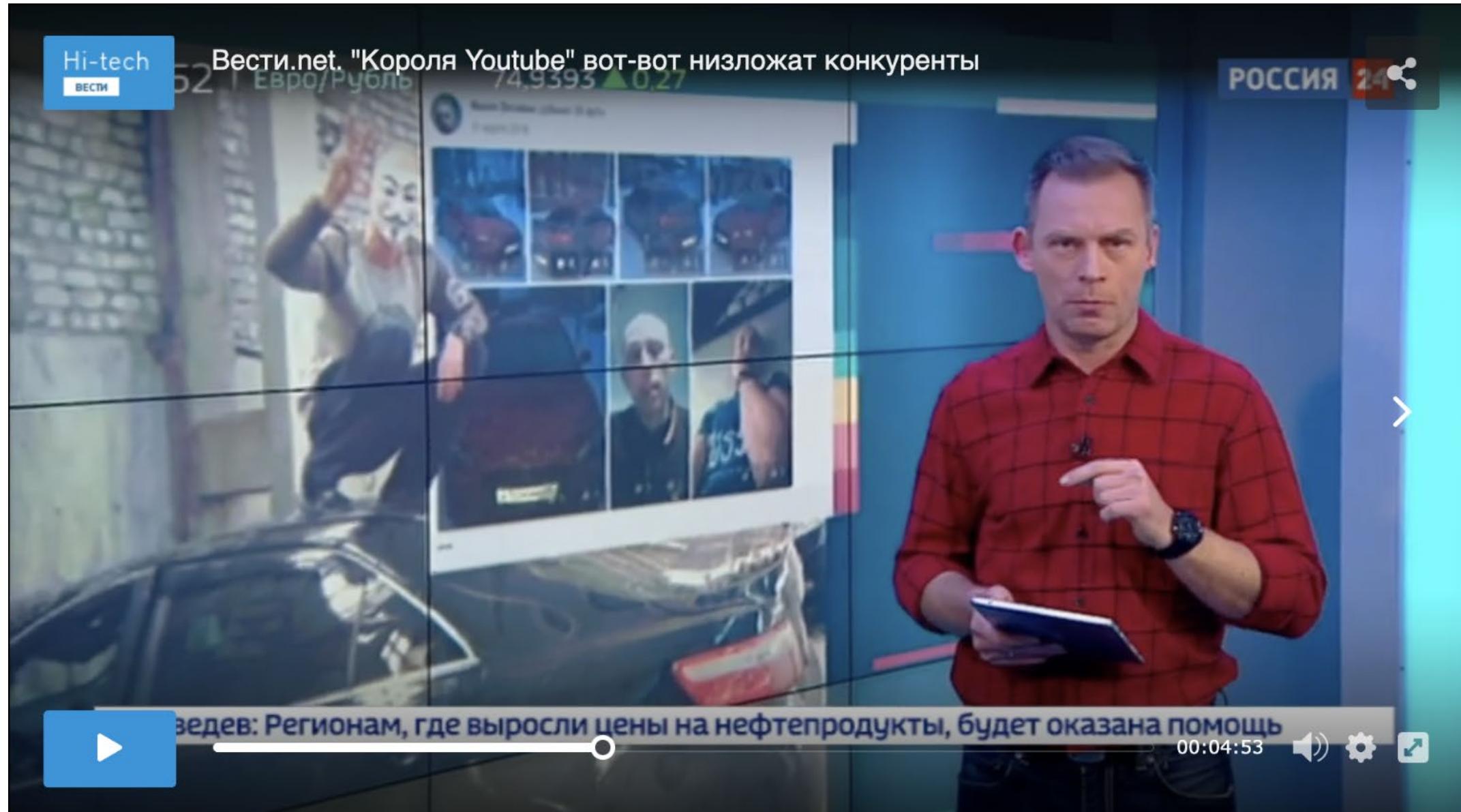
Общий стаж работы: 5

Стаж работы по специальности: 3

Преподаваемые дисциплины:

Дополнительная информация:

Rise to Fame



Other Known Indicators Used by paranoid777 aka tessa88

- Usernames:
 - 0db2016
 - khaym
- Jabbers:
 - paranoid777@exploit[.]im
 - khaym@exploit[.]im
 - Bruno123123@yax[.]im
 - demigrooop@exploit[.]im
 - tarakan72511@chatme[.]im
 - tanchik72511@exploit[.]im
 - db2016@swissjabber[.]ch
- Email addresses:
 - paraplan@mail[.]ru
- Skype:
 - Paranoy7771
- ICQ:
 - 709651701
- Web Money Wallets:
 - 947404114680
 - R125631224396
 - Z811745473923

New tessa88`s Indicators Were Revealed During Investigation

- Yahoo Messenger:
 - Tools.master2011
- M.Donakov`s Phone Numbers:
 - +79022222229
 - +17789981919
- Bitcoin Wallet:
 - 1HNXAXVQGw7RZ4sg2CjDMjpnhm36VHQSXJ

Key Take-Aways

- Evaluate Internal resources and identify the high-value/high-risk data.
- If budget permits, establish internal threat-intelligence program. At minimum provide additional training to the existing security personal
- Conduct threat-exposure research
 - Who
 - How
 - Why
- Maintain record of existing and emerging threats
 - Actors
 - Malware
 - TTP
- Prepare mitigation and contingency plan

RSA® Conference 2019 Asia Pacific & Japan

Thank You

Andrei Barysevich

@DeepSpaceEye