



# Nisos Research: Coldriver

## **Adversary Insights™**

Delivered January 2023

# TABLE OF CONTENTS

|                                       |          |
|---------------------------------------|----------|
| <b>EXECUTIVE SUMMARY</b>              | <b>3</b> |
| <b>Andrey Stanislavovich Korinets</b> | <b>4</b> |
| <b>Andrey Georgievich Yushkov</b>     | <b>6</b> |
| <b>Alexey Valerievich Doguzhiev</b>   | <b>7</b> |

## EXECUTIVE SUMMARY

Nisos operators investigated links between the Coldriver group (aka SEABORGIUM) and the Russian Government. The Coldriver Group, also known as Callisto and SEABORGIUM, is a Russia-based espionage threat actor group known to attack government organizations, think tanks, and journalists in Europe and the Caucasus regions through spearphishing and hack-and-leak campaigns.

Nisos investigated PII selectors associated with domains used in recent Coldriver Group activity in order to identify further selectors and identify links between the Russian Government and the Coldriver Group. Investigators traced a selector back to an individual named Andrey Korinets.

Andrey Stanislavovich Korinets (Коринец Андрей Станиславович), through a company email address, it@ugs[.]center, is linked to LLC УХТАГАЗСЕРВИС (ООО УХТАГАЗСЕРВИС), a Russian company that contracts with Russian governmental entities.

Korinets is currently employed by Trustlink, an SEO exchange that has been operating in the internet marketing and SEO industry since 2008, while still residing in Syktyvkar. The email address used by his VK account was used as the contact email address for an ezine published by the hacker underground in Syktyvkar.<sup>1</sup> He is currently employed by Trustlink[.]ru.

This organization is an “exchange of trusted links and unique articles,” used for sharing links between web site owners and advertisers and is built on top of the SEOPult[.]pro marketing platform. It is possible that the Coldriver group is using Trustlink infrastructure or the SEOPult platform to build out their phishing infrastructure.<sup>23</sup>

Two email addresses, cp.regname@googlemail[.]com and vladimirdj90@gmail[.]com, attributed to Korinets, provided reviews for Syktyvkar-based Lavina Private Security Company (Лавина Частное Охранное Предприятие).

While researchers identified no indication of Korinets’ employment with Lavina, the company hires former Russian military and intelligence personnel to address clients’ physical and technical security as well as security alarm response.

Researchers also identified two individuals, Andrey Georgievich Yushkov (Юшков Андрей Георгиевич) and Alexey Valerievich Doguzhiev (Догужиев Алексей Валерьевич) through email addresses andrey\_usk@mail[.]ru and vladimirdj90@gmail[.]com respectively that appear to be shared with Andrey Korinets.

The email it@ugs[.]center is linked to ООО УХТАГАЗСЕРВИС (LLC УХТАГАЗСЕРВИС), a Komi, Ukhta-based company that conducts business spanning from construction to natural resources

---

<sup>1</sup> [https://museum.netstalking\[.\]ru/xaknotdie/index-27.htm](https://museum.netstalking[.]ru/xaknotdie/index-27.htm)

<sup>2</sup> [https://trustlink\[.\]ru](https://trustlink[.]ru)

<sup>3</sup> [https://www.facebook\[.\]com/Trustlinkru](https://www.facebook[.]com/Trustlinkru)

infrastructure, according to Russian corporate data and the company website.<sup>4</sup> <sup>5</sup> LLC UHTAGAZSERVICE, INN 1102073810, has had seven government contracts totaling more than 100 million Rubles, one of which was with the government administration SE “Sosnogorsk”, according to the same Russian corporate record.<sup>6</sup> Efforts to identify a connection between Andrey and LLC UHTAGAZSERVICE other than the it@ugs[.]center email provided no results.

Efforts to definitively determine whether the actors are a network of individuals or an individual provided inconclusive results.

---

<sup>4</sup> [https://www.rusprofile\[.\]ru/okved/7041149#other](https://www.rusprofile[.]ru/okved/7041149#other)

<sup>5</sup> [https://ugs\[.\]center/?yandex-source=desktop-maps#preimuschestva](https://ugs[.]center/?yandex-source=desktop-maps#preimuschestva)

<sup>6</sup> [https://www.rusprofile\[.\]ru/gz/7041149](https://www.rusprofile[.]ru/gz/7041149)

# Andrey Stanislavovich Korinets

Researchers identified a possible legal name for Andrey Korinets and potential name spelling variants; Коринец Андрей Станиславович (Korinets Andrey Stanislavovich) and Корипец Андрей Станиславович (Koripets Andrey Stanislavovich). Based on shared selector data, we judge Korinets and Koripets are the same person.

Researchers identified the following selectors via leak data:

- DOB: 18-May-1987, 18-Aug-1987
- Phone: 79087150442, tagged as “Andrey K” in Russian contact information
- Email: szine.info@gmail[.]com; nepkomi@gmail[.]com; jorgen2004@bk[.]ru; zeg888@gmail[.]com; it@ugs[.]center; cp.regname@googlemail[.]com; vladimirdj90@gmail.com
- VK: [https://vk\[.\]com/win32](https://vk[.]com/win32)

Email address [szine.info@gmail\[.\]com](mailto:szine.info@gmail[.]com) is directly linked to the aforementioned POI’s VK account, according to leaked data. Additionally, the email account is associated with a 2006 website for “Syktyvkar Underground eZine”.<sup>7</sup> The email address is named “Admin ezine” with a google id (GID) 100616394292596935260. Leak data also provided leaked passwords; “31337 eleetCrew”, “asdasd123”, “123qwert”, and “da3dce93f9ae3dc082b7f901c309b60e”

Email address [it@ugs\[.\]center](mailto:it@ugs[.]center) is linked to ООО УХТАГАЗСЕРВИС (LLC UHTAGAZSERVICE), a Komi, Ukhta-based company that conducts business spanning from construction to natural resources infrastructure, according to Russian corporate data and the company website.<sup>8 9</sup> LLC UHTAGAZSERVICE, INN 1102073810, has had seven government contracts totaling more than 100 million Rubles, one of which was with the government administration SE “Sosnogorsk”, according to the same Russian corporate record.<sup>10</sup> Efforts to identify a connection between Andrey and LLC UHTAGAZSERVICE other than the [it@ugs\[.\]center](mailto:it@ugs[.]center) email provided no results.

Email address [nepkomi@gmail\[.\]com](mailto:nepkomi@gmail[.]com) is associated with the name “Andrey K” with GID 103379369701150348386, according to google account data. This email address is also grouped with [arston11@yandex\[.\]ru](mailto:arston11@yandex[.]ru), according to a Google-ID search. According to 2016 information, [nepkomi@gmail\[.\]com](mailto:nepkomi@gmail[.]com) is the registrant email for the domain [sykt\[.\]su](http://sykt[.]su).<sup>11</sup>

Email address [zeg888@gmail\[.\]com](mailto:zeg888@gmail[.]com) is linked to an individual that is almost certainly not the POI, Быстрова Мария Сергеевна (Bystrova Maria Sergeevna), selector 79091233224, a Facebook account,

---

<sup>7</sup> [https://museum.netstalking\[.\]ru/xaknotdie/index-27.htm](https://museum.netstalking[.]ru/xaknotdie/index-27.htm)

<sup>8</sup> [https://www.rusprofile\[.\]ru/okved/7041149#other](https://www.rusprofile[.]ru/okved/7041149#other)

<sup>9</sup> [https://ugs\[.\]center/?yandex-source=desktop-maps#preimuschestva](https://ugs[.]center/?yandex-source=desktop-maps#preimuschestva)

<sup>10</sup> [https://www.rusprofile\[.\]ru/gz/7041149](https://www.rusprofile[.]ru/gz/7041149)

<sup>11</sup> [https://community.riskiq\[.\]com/search/sykt.su/whois](https://community.riskiq[.]com/search/sykt.su/whois)


and email accounts that are unrelated to the POI.<sup>12</sup> The email zeg888@gmail[.]com is named “Человек Волшебник” (“Man Wizard”), according to Google-ID information.

Email address arston11@yandex[.]ru is associated with website http://atlet11[.]ru according to data aggregator Pipl searches. While the website is no longer active, the site focused on sports nutrition in the Komi Republic and sold fat burning supplements.<sup>13</sup>

Email address cp.regname@googlemail[.]com is attributed to the name “Max Stoyovich” according to a Google-ID search, and Alexey Doguziev according to data aggregator Pipl. This email address is the registrant email address for the following domains:<sup>14 15 16</sup>

- Domain: gormonx[.]com
- Registrant name: Doguzhiev Aleksei Valerevich
- Street: Lenina 8-43
- City: Sofrino
- Postal code: 141220
- Telephone: 17177599152
  - This number, based in Myerstown, PA, is likely a randomly selected number.

The domain gormonx[.]com, no longer active, was a site dedicated to the sale of peptides and growth hormones. It hosted a VKontakte group, https://vk[.]com/gormonx, with contact email address gormonx@gmail[.]com.<sup>17</sup>



**hormone**  
Dealer

Messages: 24  
Ratings: +9 / 0

Hello everyone, many people already know us, some don't yet)

Our store offers a wide selection of Peptides of Growth Hormones, Eka and much more  
Fast delivery, consultations and generally a pleasant approach)  
Very often we make discounts and goods can be purchased at a price lower than that in the price list

OUR SITE <http://gormonx.com>

OUR VK GROUP <http://vk.com/gormonx> For all incomprehensible questions, you  
can write to Skype  
- GORMONX or  
mail - [gormonx@gmail.com](mailto:gormonx@gmail.com) 5mg 200p GHRP6 5mg 200p IPAMORELIN 2mg 250p HGH176-191 2mg 300p

**Graphic 1: Description of the gormonx[.]com website**

- Domain: newwinta[.]com
- Registrant name: Rose R Rose
- Street: xianggang

<sup>12</sup> https://www.facebook[.]com/profile.php?id=100001291250438

<sup>13</sup> https://vk[.]com/wall-23398184\_57

<sup>14</sup> https://community.riskiq[.]com/search/gormonx.com/whois

<sup>15</sup> https://community.riskiq[.]com/search/newwinta.com/whois

<sup>16</sup> https://community.riskiq[.]com/search/opera-browser.us/whois

<sup>17</sup> https://ag.anabolicshops[.]me/threads/128/page-3



- City: xianggangdiqu
- State: xianggang
- Country: hong kong
- Telephone: 8520121234567

The domain newwinta[.]com is no longer active.

- Domain: opera-browser[.]us
- Name: Ian Colin
- Street: Alder Street 15-9
- City: orangeville
- Postal code: ON L9W 3T7
- Country: ?land islandslax
- Telephone: 17177599152

The domain opera-browser[.]us is no longer active.

Email address vladimirdj90@gmail[.]com is associated with the name “Tesla DJ” according to a Google-ID search. Data aggregator Pipl associates the email address with the following information:

- Name: Alexey Doguziev
- Email address: sykt.support@gmail[.]com
- Telephone: 79635560496
- Address: Sofrino, Rose 67-2
- Domain: sykt[.]su

Leak data associated with 79635560496 and 79031075270 provided the following information that is likely not the POI:

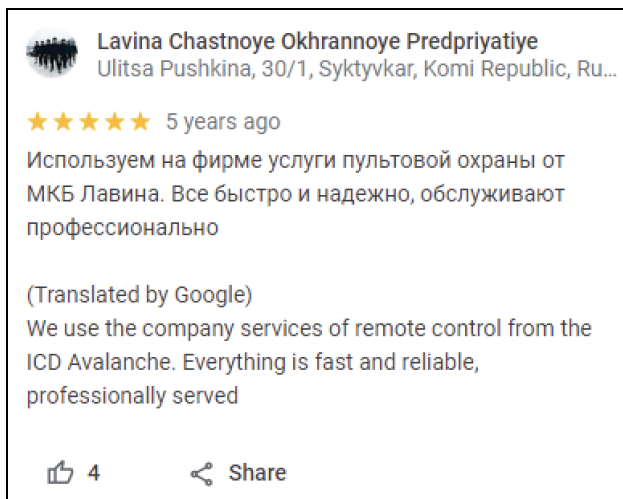
- 79635560496 is linked to an **Отмахова Светлана Владимировна** (Otmakhova Svetlana Vladimirovna) and associated with OK profile: [https://ok\[.\]ru/profile/517588431042](https://ok[.]ru/profile/517588431042) but tagged as “Vladimir Filippov” in Russian contact data
- 79031075270 is linked to a "Robert" with no associated social media accounts. No Russian contact data was associated with this selector

Email address cp.regname@googlemail[.]com under the name “Max Stoykovih” posted a review for the Lavina Private Security Company (Лавина Частное Охранное Предприятие), stating “We” used the company for remote control services.<sup>18</sup> Email address vladimirdj90@gmail[.]com using the name “Tesla DJ” also reviewed the company in 2017, stating the company offered a wide range of services.<sup>19</sup> According to its website, Interregional Security Corporation “LAVINA” (INN 1102053927) provides “services for monitoring objects, responding to alarm messages, maintaining video surveillance

<sup>18</sup> [https://www.google\[.\]com/maps/contrib/115418893585294085929](https://www.google[.]com/maps/contrib/115418893585294085929)

<sup>19</sup> [https://www.google\[.\]com/maps/contrib/108045373549778542202](https://www.google[.]com/maps/contrib/108045373549778542202)

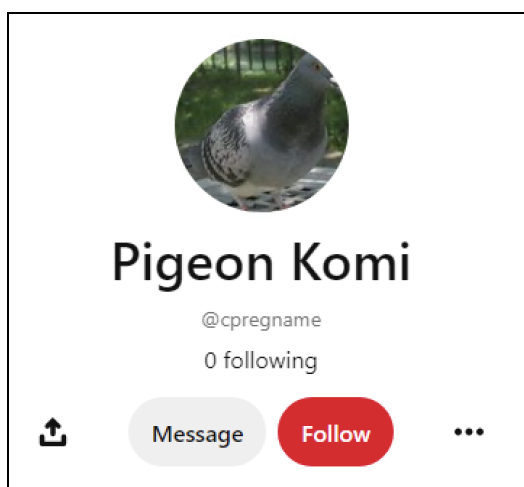
systems and technical security equipment for a whole network of security companies that are part of the partner network of console security in the North-West region.”<sup>20</sup>



**Graphic 2: Max Stoykovih’s Google review of Lavina**

The following social media pages are associated with user “Pigeon Komi”:

- Pinterest: [https://www.pinterest\[.\]com/cpregname](https://www.pinterest[.]com/cpregname) (Page is not active)
- Livejournal: [https://ext-1667185.livejournal\[.\]com](https://ext-1667185.livejournal[.]com) (No recent entries)
  - The Livejournal profile for Pigeon Komi lists the user location as Syktyvkar, Ukhta, and lists the user’s website as [http://komi\[.\]eu](http://komi[.]eu), which no longer exists.
- Foursquare: [https://ru.foursquare\[.\]com/pigeon\\_komi](https://ru.foursquare[.]com/pigeon_komi) (Last activity 2017)
  - List of locations and check-ins is retail and bars around Syktyvkar



**Graphic 3: Pigeon Komi Pinterest profile image**

<sup>20</sup> [https://lavina-mkb\[.\]ru/about](https://lavina-mkb[.]ru/about)



Korinets is currently employed by Trustlink<sup>21</sup>, an SEO exchange that has been operating in the internet marketing and SEO industry since 2008, while still residing in Syktyvkar. The email address used by his VK account was used as the contact email address for an ezine published by the hacker underground in Syktyvkar.<sup>22</sup> He is currently employed by Trustlink[.]ru. This organization is an “exchange of trusted links and unique articles,” used for sharing links between web site owners and advertisers and is built on top of the SEOPult[.]pro marketing platform. It is possible that the Coldriver group is using Trustlink infrastructure or the SEOPult platform to build out their phishing infrastructure.<sup>2324</sup>

## Andrey Georgievich Yushkov

Researchers identified the following information for Andrey Georgievich Yushkov (Юшков Андрей Георгиевич) in leak data:

- Telephone: 78212391241
- Telephone: 79121284823
- Telephone: 79129627144
- Email Address: andrey\_usk@mail[.]ru
- Email address: hearer80@mail[.]ru
- INN: 110102282353
- Address: Komi Republic
- Possible DOB: 12-Dec-1978
- Possible DOB: 30-Nov-1977
- Possible passport: 8703878169, Issued 11-Oct-2003

Telephone number 78212391241 is the contact number for “Print-S,” a company located at Syktyvkar, Pervomayskaya, 70 that sells and repairs office equipment and refills print cartridges.<sup>25</sup> Russian corporate data related to Yushkov’s INN confirms he is involved in computer repair and sales.<sup>26</sup>

Telephone number 79121284823 is associated with the name Андрей Юшков in a mobile data aggregator.

Leak data provided leaked passwords “280872t” and “7788dd” for the email address hearer80@mail[.]ru. Additionally, a MyWorld page for hearer80@mail[.]ru lists location as Syktyvkar, Komi, Russia, and DOB as 01-Dec-1980.<sup>27</sup>

---

<sup>21</sup> [https://facebook\[.\]com/e1eet](https://facebook[.]com/e1eet)

<sup>22</sup> [https://museum.netstalking\[.\]ru/xaknotdie/index-27.htm](https://museum.netstalking[.]ru/xaknotdie/index-27.htm)

<sup>23</sup> [https://trustlink\[.\]ru](https://trustlink[.]ru)

<sup>24</sup> [https://www.facebook\[.\]com/Trustlinkru](https://www.facebook[.]com/Trustlinkru)

<sup>25</sup> [https://syktyvkar.moyaspravka\[.\]ru/company/print-S-1](https://syktyvkar.moyaspravka[.]ru/company/print-S-1)

<sup>26</sup> [https://rusprofile\[.\]ru/ip/308110125600041](https://rusprofile[.]ru/ip/308110125600041)

<sup>27</sup> [https://my.mail\[.\]ru/mail/hearer80](https://my.mail[.]ru/mail/hearer80)

# Alexey Valerievich Doguzhiev

Researchers identified the following information for Alexey Valerievich Doguzhiev (Догужиев Алексей Валерьевич) in leak data:

- DOB: 24-Nov-1984
- Address: Russia, Moscow Region, Pushinsky district, Chelyuskinsky settlement, Sadovaya St., 25/1, Apt. 96
- Passport: 4699275896
- Passport: 4606872023 issued 07-Jul-2005
- Email address: doguzhiev@mail[.]ru
- Telephone: 79250304548, also associated with Kristina Viktorovna Ulyanova (Ульянова Кристина Викторовна) according to leak data
- Telephone: 79263079088
- Possible Employment: Federal State Unitary Enterprise “Moscow Railway” of the Ministry of Communications of the Russian Federation (ФГУП "МЖД")
- Vehicle: 2009 Ford Focus, plate number K977AK190
- ICQ: [https://icq\[.\]im/doguzhiev@mail.ru](https://icq[.]im/doguzhiev@mail.ru)

Doguzhiev, INN 503808695264, is listed as the co-founder of ООО “HELMET” (КЕЛЬМЕТ), INN 7708314303. The company, liquidated on 08-Oct-202, is listed as wholesale trade in metals and metal ores. Alexey Alexandrovich Lakin (Лакин Алексей Александрович), INN 330704005820, is listed as the other co-founder.<sup>28</sup>

Leak data provided leaked passwords “2879837” and “287a98137x” for email address doguzhiev@mail[.]ru.

---

<sup>28</sup> [https://audit-it\[.\]ru/contragent/1177746334952\\_ooo-khelmet](https://audit-it[.]ru/contragent/1177746334952_ooo-khelmet)