Coldriver Group Research Report

nisos.com/blog/coldriver-group-report/

January 6, 2023

Blog

by Nisos | Jan 6, 2023 | Blog, Research

An Investigative Report – January 2023

The Coldriver Group, also known as Callisto and SEABORGIUM, is a threat actor known to attack government organizations, think tanks, and journalists in Europe and the Caucasus regions through spearphishing 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. Nisos analysts identified his ties to the Russian internet marketing and SEO industry, which historically has been tied to malware and phishing operations in Russia and Eastern Europe.

Nisos also identified connections between Korinets and his business entities to a Russian gas pipeline company that has contracts with Russian government entities. The team further discovered a direct link between Korinets and the underground hacking community in

Syktyvkar, Russia,

In this report, Nisos researchers identified the following:

1. Andrey Stanislavovich Korinets (Коринец Андрей Станиславович), through a company email address, it@ugs[.]center, is linked to LLC UHTAGAZSERVICE (ООО УХТАГАЗСЕРВИС), a Russian company that contracts with Russian governmental entities.
2. Korinets is currently employed by Trustlink[.ru], an SEO exchange that has been operating in the internet marketing and SEO industry since 2008, while still residing in Syktyvkar.
3. 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. 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.
4. Two email addresses 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.
5. Two individuals, Andrey Georgievich Yushkov (Юшков Андрей Георгиевич) and Alexey Valerievich Doguzhiev (Догужиев Алексей Валерьевич), were identified by through email addresses that appear to be shared with Andrey Korinets.
6. The email 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.
7. 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.

In conclusion, 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.

To learn more, download the complete Nisos Research report.

About Nisos®

Nisos is The Managed Intelligence Company®. Our services enable security, intelligence, and trust and safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset

delivering smarter defense and more effective response against advanced cyber attacks, disinformation, and abuse of digital platforms.

Explore Adversary Insights®