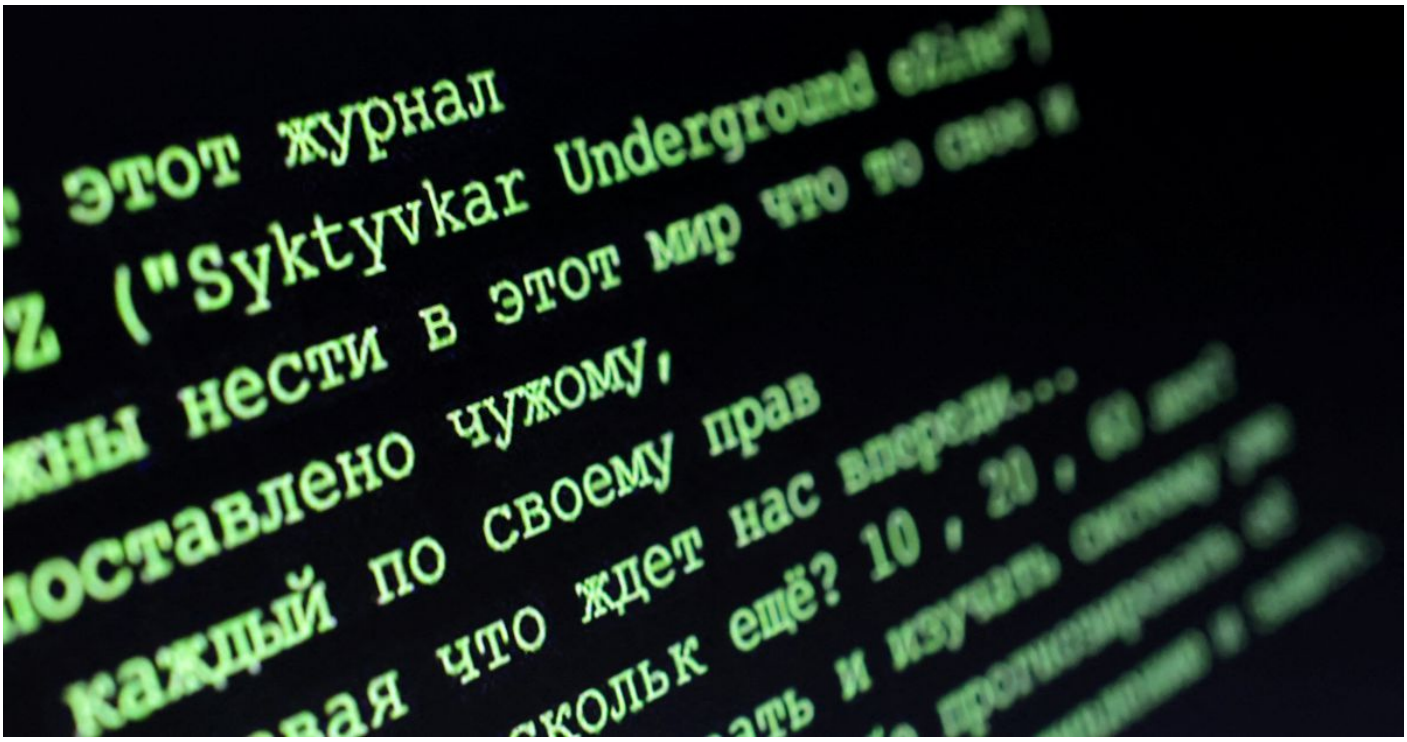
Exclusive: Russian hackers targeted U.S. nuclear scientists

James Pearson, Christopher Bing ⋮⋮ 1/6/2023



Russian hacking underground newsletter is seen in this illustration taken, December 19, 2022 REUTERS/Dado Ruvic/Illustration

LONDON/WASHINGTON, Jan 6 (Reuters) - A Russian hacking team known as Cold River targeted three nuclear research laboratories in the United States this past summer, according to internet records reviewed by Reuters and five cyber security experts.

Between August and September, as President Vladimir Putin indicated Russia would be willing to use nuclear weapons to defend its territory, Cold River targeted the Brookhaven (BNL), Argonne (ANL) and Lawrence Livermore National Laboratories (LLNL), according to internet records that showed the hackers creating fake login pages for each institution and emailing nuclear scientists in a bid to make them reveal their passwords.

Reuters was unable to determine why the labs were targeted or if any attempted intrusion was successful. A BNL spokesperson declined to comment. LLNL did not respond to a request for comment. An ANL spokesperson referred questions to the U.S. Department of Energy, which declined to comment.

Cold River has escalated its hacking campaign against Kyiv's allies since the invasion of Ukraine, according to cybersecurity researchers and western government officials. The digital blitz against the U.S. labs occurred as U.N. experts entered Russian-controlled Ukrainian territory to inspect Europe's biggest atomic power plant and assess the risk of what both sides said could be a devastating radiation disaster amid heavy shelling nearby.

Cold River, which first appeared on the radar of intelligence professionals after targeting Britain's foreign office in 2016, has been involved in dozens of other high-profile hacking incidents in recent years, according to interviews with nine cybersecurity firms. Reuters traced email accounts used in its hacking operations between 2015 and 2020 to an IT worker in the Russian city of Syktyvkar.

"This is one of the most important hacking groups you’ve never heard of," said Adam Meyers, senior vice president of intelligence at U.S. cybersecurity firm CrowdStrike. "They are involved in directly supporting Kremlin information operations."

Russia's Federal Security Service (FSB), the domestic security agency that also conducts espionage campaigns for Moscow, and Russia's embassy in Washington did not respond to emailed requests for comment.

Western officials say the Russian government is a global leader in hacking and uses cyber-espionage to spy on foreign governments and industries to seek a competitive advantage. However, Moscow has consistently denied that it carries out hacking operations.

Reuters showed its findings to five industry experts who confirmed the involvement of Cold River in the attempted nuclear labs hacks, based on shared digital fingerprints that researchers have historically tied to the group.

The U.S. National Security Agency (NSA) declined to comment on Cold River's activities. Britain's Global Communications Headquarters (GCHQ), its NSA equivalent, did not comment. The foreign office declined to comment.

'INTELLIGENCE COLLECTION'

In May, Cold River broke into and leaked emails belonging to the former head of Britain's MI6 spy service. That was just one of several 'hack and leak' operations last year by Russia-linked hackers in which confidential communications were made public in Britain, Poland and Latvia, according to cybersecurity experts and Eastern European security officials.

In another recent espionage operation targeting critics of Moscow, Cold River registered domain names designed to imitate at least three European NGOs investigating war crimes, according to French cybersecurity firm SEKOIA.IO.

The NGO-related hacking attempts occurred just before and after the October 18 launch of a report by a U.N. independent commission of enquiry that found Russian forces were responsible for the "vast majority" of human rights violations in the early weeks of the Ukraine war, which Russia has called a special military operation.

In a blog post, SEKOIA.IO said that, based on its targeting of the NGOs, Cold River was seeking to contribute to "Russian intelligence collection about identified war crime-related evidence and/or international justice procedures." Reuters was unable independently to confirm why Cold River targeted the NGOs.

The Commission for International Justice and Accountability (CIJA), a nonprofit founded by a veteran war crimes investigator, said it had been repeatedly targeted by Russian-backed hackers in the past eight years without success. The other two NGOs, the International Center of Nonviolent Conflict and the Centre for Humanitarian Dialogue, did not respond to requests for comment.

Russia's embassy in Washington did not return a request seeking comment about the attempted hack against CIJA.

Cold River has employed tactics such as tricking people into entering their usernames and passwords on fake websites to gain access to their computer systems, security researchers told Reuters. To do this, Cold River has used a variety of email accounts to register domain names such as "goo-link.online" and "online365-office.com" which at a glance look similar to legitimate services operated by firms like Google and Microsoft, the security researchers said.

DEEP TIES TO RUSSIA

Cold River made several missteps in recent years that allowed cybersecurity analysts to pinpoint the exact location and identity of one of its members, providing the clearest indication yet of the group's Russian origin, according to experts from Internet giant Google, British defense contractor BAE, and U.S. intelligence firm Nisos.

Multiple personal email addresses used to set up Cold River missions belong to Andrey Korinets, a 35-year-old IT worker and bodybuilder in Syktyvkar, about 1,600 km (1,000 miles) northeast of Moscow. Usage of these accounts left a trail of digital evidence from different hacks back to Korinets' online life, including social media accounts and personal websites.

Billy Leonard, a Security Engineer on Google's Threat Analysis Group who investigates nation state hacking, said Korinets was involved. "Google has tied this individual to the Russian hacking group Cold River and their early operations," he said.

Vincas Ciziunas, a security researcher at Nisos who also connected Korinets' email addresses to Cold River activity, said the IT worker appeared to be a "central figure" in the Syktyvkar hacking community, historically. Ciziunas discovered a series of Russian language internet forums, including an eZine, where Korinets had discussed hacking, and shared those posts with Reuters.

Korinets confirmed that he owned the relevant email accounts in an interview with Reuters but he denied any knowledge of Cold River. He said his only experience with hacking came years ago when he was fined by a Russian court over a computer crime committed during a business dispute with a former customer.

Reuters was able separately to confirm Korinets' links to Cold River by using data compiled through cybersecurity research platforms Constella Intelligence and DomainTools, which help identify the owners of websites: the data showed that Korinets' email addresses registered numerous websites used in Cold River hacking campaigns between 2015 and 2020.

It is unclear whether Korinets has been involved in hacking operations since 2020. He offered no explanation of why these email addresses were used and did not respond to further phone calls and emailed questions.

Reporting by James Pearson and Christopher Bing Additional reporting by Polina Nikolskaya, Maria Tsvetkova, and Anton Zverev; and Zeba Siddiqui in San Francisco and Raphael Satter in Washington Editing by Chris Sanders and Daniel Flynn