Russia's Extradition Wars Are Not What You Think They Are

By Tom Uren

Published: 2023-09-14 · Archived: 2026-04-05 16:17:35 UTC

Your weekly dose of Seriously Risky Business news is written by Tom Uren, edited by Patrick Gray with help from Catalin Cimpanu. It's supported by the Cyber Initiative at the Hewlett Foundation and this week's edition is brought to you by runZero.

Authorities in Kazakhstan have detained Nikita Kislitsin, a Russian cyber security executive, following an international arrest warrant issued by the United States.

This newsletter's sister publication, *Risky Business News*, described how this has triggered a "diplomatic tug-of-war" between the US and Russia, because Russian authorities are now also seeking to extradite Kislitsin.

The US government alleges Kislitsin stole and sold information, including logins from former social media site Formspring. Kitslitsin subsequently worked for Group-IB, a cyber security company once headquartered in Russia, and is now employed by FACCT, a company that spun out of Group-IB's Russia-based operations company in April this year.

Risky Business News has more detail on Kislitsin's case, but also points out that this isn't the first time that Russians accused of cyber crime have been the subject of competing extradition processes. Cimpanu's article lists *five* previous examples dating back to as early as 2012:

> We've seen this before many times. Every time a big Russian hacker gets arrested outside Russia's borders, Russian authorities hocus-pocus some charges out of a hat and try to get him back home like the suspects are some sort of national treasure.

Gavin Wilde, Senior Fellow at the Carnegie Institute and expert on Russian cyber operations, told *Seriously Risky Business* he thinks Russia's actions are primarily motivated by its desire to be viewed as an equal to the US.

Extradition efforts require a response because, historically, the law in Russia is used as "a tool to enable the powers that be, lending a veneer of credibility to crude authoritarianism". Given that world view, US indictments of Russian hackers are viewed "as mere coercive bullying and lawfare by the West — against which, naturally, Moscow wants to posture itself as a counterweight on the international stage".

Wilde also thinks there *might* be some government concern that Russian cyber criminals "have some degree of insight" into links between security services and cyber criminals that the government would want to keep quiet.

Wilde pointed out that there were indications, such as in the Conti leaks, for example, "of some degree of give and take" between the FSB and Russian cyber criminals. However, he cautioned about "drawing too firm a link… between the command and control of the Russian State and any and all Russian cybercriminals".

"I think by and large it's something that they tolerate rather than have… orchestration or control over," he said.

"If anything, there is probably a degree of shame or embarrassment about how permissive [the Russian cybercrime] environment is and what a lack of control the Russian security services, the interior ministry and the police forces have," he continued.

Although the extradition hijinks following Kislitsin's arrest are perhaps expected, that his arrest occurred in *Kazakhstan* may actually be good news — it may signify fewer countries are happy to act as safe havens for cybercriminals.

Dmitry Smilyanets, director of product management at Recorded Future and formerly involved in Russia's cybercrime scene, told *The Record* "Kislitsin's arrest is a clear indication of the shift in Kazakhstan geopolitics".

"Some hackers called it 'betrayal' and 'backstabbing' in the private chats on Telegram", Smilyanets continued.

Earlier this year Georgia, another former Soviet republic, arrested and extradited to the US a Russian national accused of creating and selling NLBrute, a tool to brute force RDP login credentials.

Russia losing these extradition battles at an increased rate is definitely on the cards. That some of these battles will be lost in former Soviet republics is just the cherry on top.

The purported Ukrainian hacking group Cyber Anarchy Squad has been on a tear lately, causing a severe, albeit short-term impact on two Russian telecommunications providers. These operations illustrate both the potential — and the limits — of disruptive hacktivist actions.

In the first incident, in early June, *Cyber Anarchy Squad* wiped routers and networking devices belonging to Russian telco Infotel JSC. On Telegram, the group wrote that "all their infrastructure is destroyed, nothing alive is left there" (translated with Google services). Infotel JSC operates the Automated Electronic Interaction System for Russia's central bank, so the attack *did* actually cause serious disruption to Russia's financial system, which was unable to process electronic payments for more than a day.

In late June, the group also hit Russian satellite telecommunications operator DoZoR-Teleport. Cyber Anarchy Squad claimed to have destroyed network servers, bricked some of the company's satellite modems, and stolen and leaked documents. This was later confirmed by the company, per *Risky Business News*:

> The company says the incident impacted infrastructure hosted with one of its cloud service providers, but did not name the operator. Dozor-Teleport general director Alexander Anosov says it may take up to two weeks to restore affected services. The company provides satellite connectivity to some of Russia's largest organizations, such as Gazprom, Rosatom, the FSB, and Moscow's regional government.

In both cases, the disruption was severe and was confirmed by data from the IODA internet monitoring system.

These attacks have been far more effective than the vast majority of actions that have very involved DDoS or data breaches. However, in both cases, the incidents were relatively short-term, and the networks were restored within days to a week.

In general, this newsletter is sceptical that disruptive hacktivist action will make a significant difference when it comes to conventional military conflicts such as the ongoing war in Ukraine. There are several reasons that it is difficult for state cyber services to coordinate with hacktivist groups, one particularly significant one being that it

is risky to trust unvetted activists with information that reveals significant plans and targets. This makes it difficult for hacktivist actions to be well coordinated and so enable or enhance other state action which could take advantage of the cyber-enabled interruption.

From what we know so far, these attacks haven't enabled any kind of significant Ukrainian success. They certainly caused significant disruption, so if launched at the right time and place and combined with other actions, it is *possible* they could have enabled some significant and enduring outcome. But at this stage, it looks like that coordination with other types of state power is missing, and these attacks are merely an embuggerance.

The Grugq and this author discussed how Ukraine could use its volunteer Ukraine IT Army in this edition of the Between Two Nerds podcast.

Listen to Patrick Gray and Tom Uren discuss this edition of the newsletter in the Seriously Risky Business podcast:

1. **Akira ransomware decryptor:** Cybersecurity firm Avast has released a free decryptor for the Akira ransomware strain. The Akira strain emerged in March of this year, has both Windows and Linux versions and has attacked companies across a wide range of sectors.

2. **FTC to ban fake reviews:** The US Federal Trade Commission has proposed a rule banning fake reviews and testimonials.

3. **CISA's CyberSentry launched:** The US Cybersecurity and Infrastructure Security Agency has launched CyberSentry, a new threat detection and monitoring platform. CyberSentry is free to all critical infrastructure operators and will allow CISA to monitor networks for potential threats

This week's sponsor is runZero, the fastest and easiest way to get to a full asset inventory with actionable insights. In this Risky Business News sponsor interview Tom Uren talks to runZero's CEO Chris Kirsch about how the company has evolved from offering an active scanning product to one that can now discover assets on OT and cloud environments using both active and passive scanning approaches:

Last week Australia's financial regulator, APRA, announced that it will require Medibank Private to set aside an additional AUD$250m to cover potential future losses.

Medibank Private was victim of a major cyber incident in October 2022 that resulted in data from *all* Medibank's customers being stolen. This was a big deal in Australia and triggered a whole-of-government response.

APRA is aiming its action squarely at Medibank's infosec practices, saying the capital adjustment reflected "weaknesses identified in Medibank's information security environment" and "will remain in place until an agreed remediation program of work is completed by Medibank to APRA's satisfaction".

Blockchain security firm SlowMist reports that in the first half of 2023 there were 185 crypto asset-related security incidents that led to losses of up to USD$920m. In the first half of 2022 there were a similar number of incidents, 187, but approximately USD$2bn in losses.

Debate over the UK's proposed Online Safety Bill has heated up recently as tech experts and civil society groups issued an open letter to Technology Minister Chloe Smith expressing concerns about the bill's implication for end-

to-end encryption. Apple also issued a statement asking the government to "amend the bill to protect strong end-to-end encryption for the benefit of all", joining encrypted messaging service providers Signal and WhatsApp in expressing concern about the bill.

Ciaran Martin, former head of the UK's NCSC has weighed in to the debate, essentially saying that rather than being about breaking encryption, the bill is all about client-side scanning (Apple proposed its implementation back in August of 2021, but it was shelved after pushback from privacy and security advocates). The problem for the Online Safety Bill, Martin says, is that the UK government hasn't set out how client-side scanning would work securely and he calls for further amendments to the bill:

> Surely then, parliamentarians should be shown the details of a workable draft regulation before voting? If not, this controversial power will be driven through, but likely never used. Cue another bitter and damaging row about Britain's perceived hostility to encryption, but with no actual benefit to those fighting online harms. If peers do not ask the government to think again, parliament will be legislating for a unicorn — and not the billion-dollar tech company kind.

You can find the audio edition of this newsletter and other fine podcasts and interviews in the Risky Biz News feed (RSS, iTunes or Spotify).

In our last "Between Two Nerds" discussion Tom Uren and The Grugq look at European Union efforts to make laws to protect journalists from spyware.

Prigozhin troll farms in limbo following Wagner mutiny: Several Russia-based news outlets are reporting that Yevgeny Prigozhin is shutting down his Patriot media company in the aftermath of his failed mutiny at the head of the Wagner PMC last month.

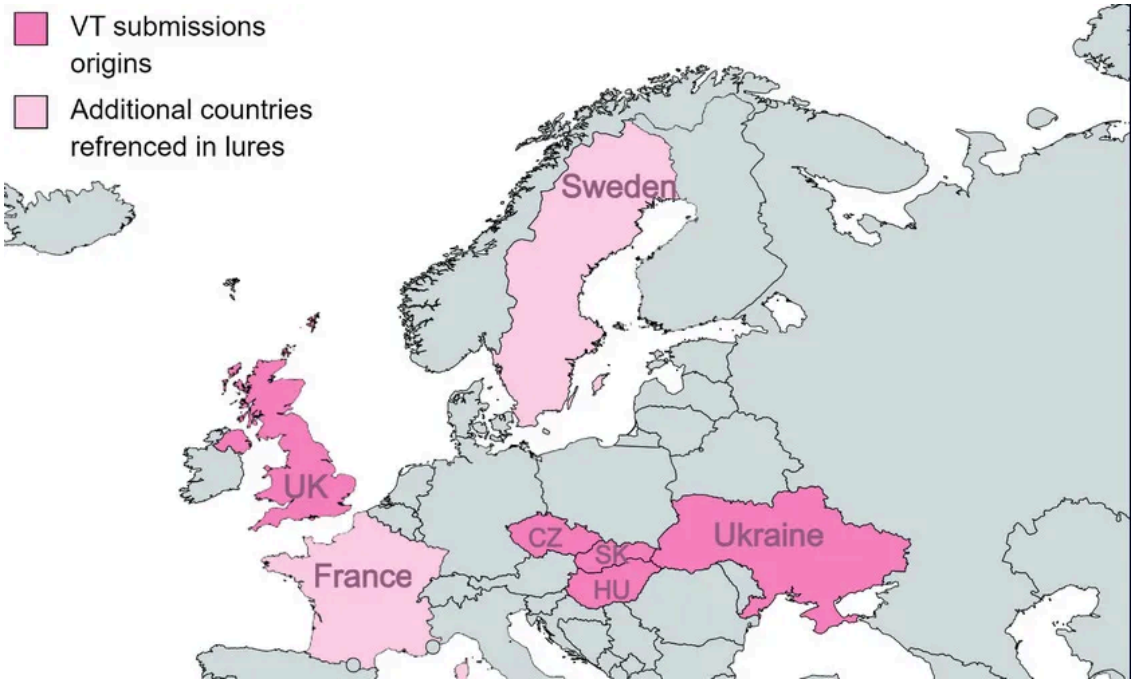
The Patriot media group is a holding company for a dozen of Russian-language propaganda and fake news sites, such as RIA FAN, Politika Segodnya (Politics Today), Ekonomika Segodnya (Economics Today), Nevskiye Novosti (Nevsky News), and Narodnye Novosti (People's News). It is also the holding company for the Internet Research Agency—Russia's infamous "troll farm" linked to multiple instances of election interference across the world.

Prigozhin has allegedly fired all employees and plans to shut down all news sites. All this information comes from Patriot media group insiders, and Prigozhin has not made a formal statement or has been seen or heard from since leaving Russia for Belarus. [more on *Risky Business News*]

UK NCSC first-ever APT response: The UK National Cyber Security Centre (NCSC) says the first-ever state-sponsored cyber-attack that targeted the UK government took place 20 years ago, in June 2003. The agency didn't reveal who was behind the attack but says the operation was a phishing campaign carried out by a foreign state. The incident was investigated by the Communications-Electronics Security Group of the GCHQ and is what eventually led the UK government to form a dedicated cybersecurity arm within the agency years later.

SmugX: Chinese cyber-espionage group RedDelta (Mustang Panda) has continued its persistent targeting of Foreign Affairs ministries and embassies across Europe. Security firm Check Point says the new attack represents a larger trend within the Chinese espionage ecosystem that has been slowly shifting its attention to European entities. The new operations are a continuation of RedDelta campaigns initially reported back in December 2022

by BlackBerry and Recorded Future. The attacks were spotted in countries such as Sweden, France, Ukraine, Czechia, Slovakia, Hungary, and the UK. Just like last year, the final malware payload deployed on infected systems was the good ol' faithful PlugX backdoor—a malware strain used by tens of Chinese APT groups for more than a decade.



Source: https://srslyriskybiz.substack.com/p/russias-extradition-wars-are-not