# Russian hackers breach UK MoD data systems in latest cyberattack escalation



In a significant cyber incident that has alarmed the British defence community, Russian hackers reportedly breached UK Ministry of Defence (MoD) data systems, accessing and stealing sensitive information relating to military personnel and operational bases. According to reports from British media, the cybercriminals infiltrated the systems of Dodd Group, a maintenance and construction contractor for the MoD, through a ransomware attack that granted them temporary access to internal networks. While the contractor confirmed the security breach and ongoing forensic investigation, claims emerged that personal data belonging to some 272,000 service members and veterans—including names, bank details, and addresses—were taken and posted online.

The stolen files purportedly included details about key military locations such as RAF Lakenheath, home to US Air Force F-35 jets, and various Royal Navy bases. The British Ministry of Defence acknowledged the incident and stated it was investigating allegations that classified information had been published on the Dark Web. However, to protect operational security, the MoD declined to comment further on specifics.

This attack fits into a broader pattern of escalating cyber threats against UK military infrastructure in recent years. The Defence Gateway portal, a critical platform for British military staff, was targeted in a separate 2024 cyberattack that resulted in nearly 600 employees’ passwords being leaked online. This earlier breach compromised sensitive login credentials and raised concerns among intelligence experts about potential espionage, including recruitment or blackmail attempts connected to these cyber intrusions.

More broadly, state-sponsored cyberattacks have increasingly targeted the UK’s defence sector. In April 2024, a massive data breach involving the third-party payroll system SSCL exposed names and bank information of thousands of military personnel. Although the government did not publicly confirm the perpetrators, media sources speculated that the attack involved a state-backed actor, with allegations pointing towards Chinese hackers.

Other notable incidents include a September 2023 breach by the Russian-linked LockBit hacking group, which accessed substantial data from Zaun, a provider of fencing for high-security sites. Among the compromised information were details related to the UK’s nuclear submarine base at HMNB Clyde, the Porton Down chemical weapons facility, and GCHQ communications infrastructure. LockBit’s administrator, Dmitry Yuryevich Khoroshev, was indicted by US authorities in October 2024, facing charges from multiple international law enforcement bodies. Despite these efforts, the threat posed by such groups remains substantial, especially if actors remain shielded by operating from within Russia.

In October 2025, the UK Ministry of Defence launched another investigation following claims that the Russian hacker group Lynx accessed and leaked hundreds of sensitive military documents. The breach reportedly involved a 'gateway' attack through an MoD contractor, circumventing advanced cyber defences.

Despite these ongoing challenges, the UK government has sought to bolster its cyber resilience. A foiled cyber espionage operation in May 2025, where Russian-linked hackers posing as journalists attempted a spear-phishing attack against MoD staff, highlighted the persistent risks. Subsequently, Defence Secretary John Healey announced steps towards enhancing the UK military’s offensive cyber capabilities, in line with the Strategic Defence Review due for publication in June 2025.

These cumulative events underscore the complex and persistent nature of cyber warfare targeting UK military interests, revealing vulnerabilities in both direct military systems and associated contractor networks. They also highlight the intersecting threats from state-backed hackers and criminal groups, prompting ongoing efforts toward improved cyber security and countermeasures within the defence sector.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://www.kyivpost.com/post/62485), [[4]](https://www.upday.com/uk/uknews/russian-hackers-steal-military-files-mod-investigates/vkn35y9)
* Paragraph 2 – [[1]](https://www.kyivpost.com/post/62485), [[4]](https://www.upday.com/uk/uknews/russian-hackers-steal-military-files-mod-investigates/vkn35y9)
* Paragraph 3 – [[2]](https://www.computing.co.uk/news/2024/security/mod-hit-by-major-cyberattack)
* Paragraph 4 – [[3]](https://www.apnews.com/article/49899b429f138bb2075d9fd6703ac7b0)
* Paragraph 5 – [[5]](https://www.thedefensepost.com/2023/09/05/russian-hackers-uk-military/), [[6]](https://www.cybersecurity-insiders.com/uk-military-data-breach-and-lockbit-admin-identified/)
* Paragraph 6 – [[4]](https://www.upday.com/uk/uknews/russian-hackers-steal-military-files-mod-investigates/vkn35y9), [[7]](https://www.eurointegration.com.ua/eng/news/2025/05/29/7212643/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.kyivpost.com/post/62485> - Please view link - unable to able to access data
2. <https://www.computing.co.uk/news/2024/security/mod-hit-by-major-cyberattack> - In December 2024, the UK's Ministry of Defence (MoD) experienced a significant cyberattack resulting in the theft and leakage of passwords belonging to nearly 600 employees onto the dark web. The breach exposed sensitive information of military personnel, civilian staff, and defence contractors. The stolen data included email addresses and login credentials for the Defence Gateway portal, a critical online platform used by British military personnel. The majority of the affected employees were based in the UK, with some stationed overseas in countries like Iraq, Qatar, Cyprus, and mainland Europe. Intelligence sources warned that such cyberattacks could be precursors to more sophisticated espionage activities, such as recruitment or blackmail.
3. <https://www.apnews.com/article/49899b429f138bb2075d9fd6703ac7b0> - In April 2024, a massive data breach exposed the names and bank details of thousands of British soldiers, sailors, and airmen. The Ministry of Defence stated that this breach, involving up to 272,000 individuals, was likely carried out by a 'malicious actor' with potential state support. The third-party payroll system, SSCL, was taken offline immediately after the discovery, and an investigation was launched. While the government did not have conclusive evidence at the time, media sources alleged possible Chinese involvement. SSCL, formerly co-founded by the UK government, counts among its clients the Home Office, Cabinet Office, and Ministry of Justice. In March, the UK and the US had already accused Chinese hackers of conducting malicious cyberattacks.
4. <https://www.upday.com/uk/uknews/russian-hackers-steal-military-files-mod-investigates/vkn35y9> - In October 2025, the UK Ministry of Defence (MoD) initiated an investigation into claims that Russian hackers had stolen hundreds of sensitive military documents and leaked them on the dark web. The files reportedly contained details of eight RAF and Royal Navy bases, along with MoD staff names and email addresses. The breach was believed to have been orchestrated by Russian group Lynx, who gained access to the sensitive information by hacking a maintenance and construction contractor employed by the MoD in a 'gateway' attack. This method allowed the hackers to bypass the MoD’s strong cyber defences.
5. <https://www.thedefensepost.com/2023/09/05/russian-hackers-uk-military/> - In September 2023, a group of Russian hackers known as LockBit accessed gigabytes of sensitive data related to British military and intelligence sites. The hackers reportedly targeted Zaun, an England-based provider of fences for maximum security sites. Zaun confirmed that the hackers managed to download approximately 10 gigabytes of data from vulnerable computers. Sensitive details about the country’s HMNB Clyde nuclear submarine base, Porton Down chemical weapons laboratory, and a GCHQ communications complex were reportedly compromised. It is believed that the hacked information was posted on the dark web after the incident.
6. <https://www.cybersecurity-insiders.com/uk-military-data-breach-and-lockbit-admin-identified/> - In October 2024, the administrator of the LockBit ransomware group, Dmitry Yuryevich Khoroshev, was identified and indicted by the US Department of Justice. Khoroshev, a Russian national, reportedly amassed nearly $100 million in 2023 through illicit means using LockBit ransomware. He now faces criminal charges from the FBI, Britain’s National Crime Agency, Europol, and the Australian National Cyber Crime Agency. As a result, he is subject to travel restrictions, and his international bank accounts have been frozen. However, if Khoroshev operates from within Russia, he may evade prosecution within his home jurisdiction. The FBI has issued warnings that any company engaging in ransom payments to LockBit or negotiating with the criminal group could face legal repercussions.
7. <https://www.eurointegration.com.ua/eng/news/2025/05/29/7212643/> - In May 2025, a hacker group linked to Russia posed as journalists and carried out a cyber espionage operation against the UK Ministry of Defence. The attack was foiled, and Defence Secretary John Healey announced that the UK military was strengthening its offensive capabilities to carry out cyber attacks against enemy states such as Russia as part of a long-awaited review of the UK’s defence framework. The Strategic Defence Review was expected to be published in June 2025. The National Cyber Security Centre analysed the thwarted hacking attack and stated that the Ministry of Defence detected a spear-phishing campaign targeting staff with the aim of delivering malware.