Exclusive: Russian spies hacked UK government data and emails earlier this year

By Alexander Martin

Published: 2024-08-08 · Archived: 2026-04-05 15:37:54 UTC

Updated August 9 with comments from a government spokesperson about the incident.

Cyber spies working for Russia's foreign intelligence service accessed corporate emails and data on individuals from the British government earlier this year, according to an official description of the incident obtained by Recorded Future News.

The breach, which has not previously been reported, followed the Russian hackers initially targeting Microsoft, which supplies corporate services to the Home Office, before the hackers exploited this access to also compromise data from several of Microsoft's clients.

Following publication, a government spokesperson stressed that the Russian spies had not accessed the Home Office's own systems. It is understood the hackers compromised corporate email data shared between Microsoft and the Home Office that was held by Microsoft.

"There is no evidence that Home Office systems were compromised. We take data security very seriously, with robust reporting mechanisms in place, and continuous monitoring to ensure data is protected," the spokesperson said.

Microsoft first disclosed in January that the hacking group tracked as Midnight Blizzard — which the U.K. attributes to Russia's SVR intelligence agency — had accessed the email accounts of senior leaders at the company, later confirming the hackers had also accessed customers' emails as well as Microsoft's own "source code repositories and internal systems."

The Home Office reported the incident to Britain's data protection regulator on May 2, almost four months after Microsoft's initial disclosure. Under British data protection laws, organizations are required to report personal data breaches to the regulator within 72 hours of becoming aware of the breach.

A description of this report obtained under the Freedom of Information Act said the incident was a "nation state attack on [a] supplier" of the department's corporate systems, and linked the hack to Microsoft's January announcement.

A spokesperson for the ICO said: "We can confirm that we are aware of this incident, have assessed the information provided and concluded that no further action is required."

It is likely that most of Microsoft's government customers may have discovered being impacted by the breach much later than when Microsoft became aware of the initial incident affecting its senior staff.

It wasn't until April that the U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned that federal government data had also been affected by the hack.

At that time, CISA said Microsoft had pledged to assist the U.S. government's investigation into the incident by providing "metadata for all exfiltrated federal agency correspondence," and warned that this stolen correspondence "presents a grave and unacceptable risk to agencies."

The breach of British government data comes as Russia's intelligence services have been especially active in supporting Moscow's war aims as it continues its invasion of Ukraine, including by targeting those countries providing support to Kyiv.

"Since February 2022, the rules of the game have changed for the Kremlin, which now acts in the cyber realm as if it were already at war with the UK," said Christopher Steele, the director of Orbis Business Intelligence and a former British intelligence officer focusing on Russia.

James Sullivan, the director of cyber research at the RUSI think tank, said: "It's not a surprise that this may have happened. We know that Russia conducts campaigns like this and the British public is sadly used to it now, rather than outraged.

"But we must take these incidents seriously. They can undermine trust and confidence in public services and public officials. We do need to understand the impact a bit more in terms of the damage that has been done, what the risks are to the country, what kind of strategic advantage the adversary might be pursuing, and respond accordingly."

Measuring the effect of intelligence-gathering operations is extremely challenging. Steele said that the SVR's "motivations may be manifold — such as finding personal information of key individuals, or simply disrupting the functions of the British state — but their tactics are consistently more brazen and less cautious than in the past."

Just the day after the data breach report was filed with Britain's data protection regulator, the U.K. and allies issued a joint statement condemning malicious cyber activity by the Russian intelligence services — although this specifically focused on the activity of a different Russian agency, the GRU, which was blamed for attacks on the German Social Democratic Party.

RUSI's Sullivan told Recorded Future News: "Official attributions are a tool we have, but attribution needs to come as a package of measures — it needs to be coupled with other interventions like sanctions, or with cyber operations against the adversary — to have an impact. I'd be very interested to see what the actual response would be to an incident like this, or even if the UK Government thinks a response is needed."

Sullivan said the incident highlighted pressing questions about the accountability of the private-sector organizations involved in selling services to governments: "Similar to Crowdstrike, this incident affecting Microsoft shows how our use of just a few providers for critical services sets us up for single points of failure when there are breaches or outages. We may need to think about greater vendor diversity to spread the risk out and give organizations more resilience."

Following publication, a spokesperson for Microsoft said: "We have found no evidence that any Microsoft-hosted customer-facing systems have been compromised as a result of the attack against Microsoft that we shared in

January. As we shared at the time, the threat actor accessed a very small percentage of Microsoft corporate email accounts. We provided notifications to customers who corresponded with the impacted Microsoft corporate email accounts."

Alexander Martin

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and a fellow at the European Cyber Conflict Research Initiative, now Virtual Routes. He can be reached securely using Signal on: AlexanderMartin.79
