M. Mandl

Hackers expose defence and intelligence officials in US and UK

1/10/2012

Thousands of British email addresses and encrypted passwords, including those of defence, intelligence and police officials as well as politicians and Nato advisers, have been revealed on the internet following a security breach by hackers.

Among the huge database of private information exposed by self-styled "hacktivists" are the details of 221 British military officials and 242 Nato staff. Civil servants working at the heart of the UK government – including several in the Cabinet Office as well as advisers to the Joint Intelligence Organisation, which acts as the prime minister's eyes and ears on sensitive information – have also been exposed.

The hackers, who are believed to be part of the Anonymous group, gained unauthorised access over Christmas to the account information of Stratfor, a consultancy based in Texas that specialises in foreign affairs and security issues. The database had recorded in spreadsheets the user IDs – usually email addresses – and encrypted passwords of about 850,000 individuals who had subscribed to Stratfor's website.

Some 75,000 paying subscribers also had their credit card numbers and addresses exposed, including 462 UK accounts.

John Bumgarner, an expert in cyber-security at the US Cyber Consequences Unit, a research body in Washington, has analysed the Stratfor breach for the Guardian. He has identified within

the data posted by the hackers the details of hundreds of UK government officials, some of whom work in sensitive areas.

Many of the email addresses are not routinely made public, and the passwords are all encrypted in code that can quickly be cracked using off-the-shelf software.

Among the leaked email addresses are those of 221 Ministry of Defence officials identified by Bumgarner, including army and air force personnel. Details of a much larger group of US military personnel were leaked. The database has some 19,000 email addresses ending in the .mil domain of the US military.

In the US case, Bumgarner has found, 173 individuals deployed in Afghanistan and 170 in Iraq can be identified. Personal data from former vice-president Dan Quayle and former secretary of state Henry Kissinger were also released.

Other UK government departments have been affected: seven officials in the Cabinet Office have had their details exposed, 45 Foreign Office officials, 14 from the Home Office, 67 Scotland Yard and other police officials, and two employees with the royal household.

There are also 23 people listed who work in the houses of parliament, including Jeremy Corbyn, Labour MP for Islington North, Lady Nicholson and Lord Roper. Corbyn said he had been unaware of the breach, adding that although his email address was public he was disturbed by the idea that his password could be cracked and used to delete or write emails in a way that "could be very damaging".

Nicholson, speaking on a phone from Iraq, said she had no idea that her personal information had been hacked. She said she was very unhappy that private individuals had had their fundamental right to privacy violated. "To expose civil servants is monstrously unfair," she said. "Officials in sensitive areas like defence and the military could even be exposed to threats. Guarding data like this is extremely difficult, but it's not impossible, and we should do a great deal more."

The hacking has had a big impact because Stratfor offers expert analysis of international affairs, including security issues, and attracts subscribers from sensitive government departments.

The British victims include officials with the Joint Intelligence Organisation (JIO) responsible for assessing intelligence from all sources, including MI6 secret agents.

A former deputy head of Whitehall's strategic horizons unit is listed. The unit is part of the JIO based in the Cabinet Office and was set up four years ago to give early warning of potential serious problems that might have an impact on Britain's security or environment.

The extent of the security risk posed by the breach is not known. Bumgarner said officials who did not take extra precautions in securing passwords through dual authentication or other protection systems could find email and other databases they use being compromised. "Any foreign intelligence service targeting Britain could find these emails useful in identifying individuals connected to sensitive government activities," he said.

British officials, speaking on condition of anonymity, said they were aware of the hacking but it did not pose a risk to national security. Passwords for their communications within Whitehall would be different from any used to access the Stratfor sites. Whitehall communications would also be protected by extra security walls, officials said.

However, they added that their personal communications could be at risk if individuals used the same password as they used to access Stratfor for their bank accounts and other personal communications.

A government spokesman said: "We are aware that subscriber details for the Stratfor website have been published in the public domain. At present, there is no indication of any threat to UK government systems. Advice and guidance on such threats is issued to government departments through the Government Computer Emergency Response Team."

Stratfor has taken down its website while it investigates the security breach. The company says it is "working diligently to prevent it from ever happening again".

This is just the latest action to hit the headlines by hackers associated with Anonymous. The group, whose loose collection of members are scattered around the world and linked through internet chatrooms, has previously targeted Visa, MasterCard and PayPal in protest at the companies' refusal to accept donations for the WikiLeaks website.