The hacker said his attack was mounted in revenge for the Stuxnet virus attack on his country's nuclear programme.

The boast follows a major security breach at Comodo Group, a “certification authority” which acts as an independent third party to ensure communications between users and websites are properly encrypted. The integrity of such encryption is a fundamental part of web security, foiling attackers who could otherwise easily monitor emails or steal online banking details.

Comodo last week admitted it had been forced to revoke nine digital certificates for web service providers including Google, Microsoft, Skype and Yahoo after it emerged they had been fraudulently issued by someone who broke into its systems. The attack was traced to Iran, and now an individual has come forward to claim responsibility.

Messages posted online on Saturday claimed that a lone 21-year-old hacker was able to hack into Comodo “very, very fast”. “Comodohacker”, as he named himself, said he used his “experience of 1,000 hackers” to defend Iran’s leadership and nuclear scientists against international and domestic opponents.

In **one lengthy message** , in flawed English, he boasted: “I know you are really shocked about my knowledge, my skill, my speed, my expertise and entire attack. That's okay, all of it was so easy for me.”

Comodohacker railed especially against Stuxnet, a highly sophisticated virus that last year disrupted centrifuge control systems at Iran’s uranium enrichment site at Natanz. Forensic investigations of the attack have strongly indicated it was a **joint operation by US and Israeli secret intelligence services**
.

“When USA and Israel creates Stuxnet, nobody talks about it, nobody blamed, nothing happened at all, so when I sign certificates nothing should happen, I say that, when I sign certificates nothing should happen,” Comodohacker said.

“If you was doing a dirty business in internet inside Iran, I suggest you to quit your job, listen to sound of most of people of Iran, otherwise you'll be in a big trouble, also you can leave digital world and return to using abacus.”

The break-in was first revealed on 22 **March by Jacob Appelbaum** , a security researcher at the Tor Project, a non-profit organisation based in the US that makes software used by dissidents in Iran and elsewhere to avoid internet surveillance. It relies on digital certificates to guarantee security.

On 16 March Mr Appelbaum noticed that Mozilla and Google had quietly updated their Firefox and Chrome web browsers to revoke digital certificates that had apparently issued by Comodo. The firm was then forced to publicly admit that it had been breached on 15 March - via systems used by one of its European partners to issue digital certificates - and said it suspected government involvement.

“Taken together with other recent attacks against other targets, both reported and unreported it appears likely that this incident forms part of a pattern of attacks on Internet authentication infrastructure and that it is at least highly likely that the perpetrator(s) are highly sophisticated and government directed,” **Comodo said in a blog post** .

“It does not escape notice that the domains targeted would be of greatest use to a government attempting surveillance of internet use by dissident groups.”

Comodohacker’s messages implicitly denied any government involvement, but threatened dissidents.

“Anyone inside Iran with problems, from fake green movement to all MKO [an armed dissident group] members and two faced terrorists, should afraid of me personally,” he claimed.

“As I live, you don't have privacy in internet, you don't have security in digital world, just wait

and see.”

Mikko Hypponen , chief research officer at the computer security firm F-Secure, said that while the technical information Comodohacker posted to prove to he was behind the attack “looks convincing”, “whether they were posted by a 21-year old lone gunman or Iran government PR department, I don't know”.

Source: Telegraph.co.uk