China's 'state-sponsored hackers renew attacks on US'

The Pentagon has accused China's army of carrying out cyber-attacks

State-sponsored hackers have renewed attacks on the US after a three-month hiatus, the New York Times reports.

In February, Unit 61398 of the Chinese army was named as the source of many cyber-attacks on American companies and federal agencies.

The publicity drew denials from the Chinese government, but also prompted the number of attacks launched from China to slow to a trickle.

Now, the newspaper reports, the unit has resumed attacks on US companies.

Cyber-defence company Mandiant told the New York Times the unit, which is believed to operate out of a heavily guarded building in the suburbs of Shanghai, had recently stepped up its activity. It declined to name which agencies and businesses had been attacked.

Earlier this year Mandiant published detailed evidence suggesting Unit 61398 was behind the vast majority of significant attacks on American federal agencies and industrial organisations.

Government documents, intellectual property, blueprints and many other confidential papers had been stolen during the attacks, said Mandiant.

Hide tracks

In the wake of that report and condemnation by the Obama administration, the unit apparently scaled back its activity, uninstalling spying tools and the remote access code it had placed on networks.

But now, Mandiant told the paper, the unit had sprung back into action and was working at about 70% of its former capacity.

In a bid to hide its tracks, the unit had started using different computers to insert its remote access tools, the company said.

China has persistently denied sponsoring the attacks, saying the US is the real cyber-aggressor.

It said Mandiant's report was flawed and did not contain enough proof to back up its accusations.

The cyber-attacks are expected to be one of the main topics of discussion when President Obama's national security adviser visits China for talks in late July.

Fonte: BBC International [Portal]. Disponível em: <http://www.bbc.co.uk/news/technology-22594140>. Acesso em: 20 maio 2013.