guardian.co.uk

Oil companies targeted by hacking attack

Bobbie Johnson, San Francisco

guardian.co.uk, Wednesday 27 January 2010 07.00 GMT

Just two weeks after Google said it was the victim of an organised hacking attack, details of a similar sting that targeted three of the world's biggest oil companies have emerged.

Documents obtained by US newspaper the Christian Science Monitor show that the computer systems of three major energy companies – ExxonMobil, Marathon and ConocoPhillips – were hit by a string of attacks in 2008 aimed at stealing valuable information.

The strikes, which used precision phishing attacks to fool executives into bypassing security procedures, focused on "bid data", the valuable information collected by the companies on new oil deposits and potential sites for future operations.

According to the Monitor's investigation, the three companies – which are all based in

Texas – were only made aware of the extent of the attacks following an FBI investigation.

None of the companies involved in have made a public comment, but security experts have warned in the past about the growing importance of cybersecurity.

A report late last year by US defence company Northrop Grumman suggested that American systems were being targeted by the Chinese government – which has invested heavily in its 'informationised' army.

"First, the values of information systems and networks have never been greater," said Northrop Grumman's chief technology officer Robert Brammer in December. "Second, cybersecurity threats have never been greater."

Though precise details of the Texan attacks remain unclear, they bear similar hallmarks to those used in the strike on Google and more than 30 other American companies, which is now being dubbed Operation Aurora by internet security experts.

Aurora used a vulnerability in Microsoft's Internet Explorer web browser to access some confidential information, while the Financial Times reported earlier this week that the hackers responsible had also used instant messaging programs to pose as the friends of Google employees in order to obtain protected data such as passwords.

As a result of the attacks, which are said to have originated in China, Google has threatened to protest by uncensoring its search engine in the country - a move that has threatened to escalate relations between Beijing and Washington towards a diplomatic standoff.

The origins of the oil company hackers are not known, but the newspaper said that at least some of the information was sent to computers in China.

It is far from the first time that major companies or systems have been the victim of hacking attacks. According to reports that emerged last year, hackers have targeted a number of major computer networks belonging to governments, private companies or other important schemes.

The $300bn Joint Strike Fighter project - a collaboration between countries including the United States, Britain, the Netherlands and Israel - is said to have been compromised, while the US electrical grid was also an apparent target.

News of the attacks on ExxonMobil and others also throws into relief comments made

last week by Microsoft chief executive Steve Ballmer.

In a speech to oil industry executives in Houston, Ballmer scoffed at Google's stance over the hacking attacks and suggested that information warfare was incredibly common.

"People are always trying to break into other people's data," he said. "There's always somebody trying to break into Microsoft."

Such attempted break-ins are part of the reason Barack Obama recently suggested that defending from internet attacks was "one of the most serious economic and national security challenges we face".

That realisation led to the White House to appoint a new head of cybersecurity last month, while the British government is also planning to institute its own national cyber security centre to combat the growing threat of online warfare and criminal activity.

Comments in chronological order (Total 12 comments)

Comments are now closed for this entry.

- Staff
- Contributor

-  **selfdetermination**

  27 Jan 2010, 7:54AM

  There is a serious danger from Mainland China which has to be faced. While Beijing has introduced some economic reforms, the political stance remains the same as that of the old Eastern Bloc before the Berlin Wall came down. Just as scientists in the USSR stole much of their technology from the west, so Chinese scientists are doing the same.
  I believe this calls into question the wisdom of allowing Chinese students and technicians access to high-level areas of universities ans companies outside Mainland China. hopefully the Google affair has been a wake-up call to the West, and our political leaders will thoroughly re-assess their policy towards Mainland China.

- - Recommend? (9)
  - Report abuse
  - Clip |
  - Link

-  **dianbang**

  27 Jan 2010, 8:03AM

  > A report late last year by US defence company Northrop Grumman suggested that American systems were being targeted by the Chinese government ? which has invested heavily in its 'informationised' army.

  Never mind the "war on terror," this is a war which is happening in our own homes and offices every day organised by the largest and most powerful enemy of the western world in the world today.

- Recommend? (8)
- Report abuse
- Clip |
- Link

-  **laogai**

  27 Jan 2010, 9:02AM

  > The origins of the oil company hackers are not known, but the newspaper said that at least some of the information was sent to computers in China.

  It is high time this evil and mendacious regime was made to realise that it cannot extend its system of "gangster capitalism" to the rest of the world. Why worry about "rogue states" like North Korea when China is the biggest one of all.

- Recommend? (5)
- Report abuse
- Clip |
- Link

-  **Swedinburgh**

  27 Jan 2010, 9:54AM

  China and 'the West' are headed for armed conflict of some kind, somewhere, eventually. There is no point denying or wishing this away just because it doesn't suit your global capitalist view ("hey, it's only business, no-one gets hurt") or your naive pacifist view ("we can all get along").
  A lot of British, French, Dutch and American businessmen and politicians undoubtedly had the same attitude to Japan in the 1920s.

- Recommend? (3)
- Report abuse
- Clip |

- Link

-  **LSEscientist**

  27 Jan 2010, 12:29PM

  Bush and Blair will go down history a generation on not for the Iraqi mistake but ignoring and misunderstanding China.

- - Recommend? (2)
  - Report abuse
  - Clip |
  - Link

-  **Eccentrix**

  27 Jan 2010, 12:41PM

  @selfdetermination
  27 Jan 2010, 7:54AM

  "Just as scientists in the USSR stole much of their technology from the west, so Chinese scientists are doing the same."

  IP law and their enforcement in China are virtually non-existent so it should come as no surprise that technology theft is quite common in China. I honestly don't know how companies/governments can deal with this. China is a superpower now and like most superpowers, it only pays attention to what it can benefit from.

  "I believe this calls into question the wisdom of allowing Chinese students and technicians access to high-level areas of universities ans companies outside Mainland China."

  I disagree. It is impossible to have Chinese students and technicians working on high-tech projects and refuse them access to the high-level areas of universities and companies where they would actually carry out the design, testing and assembly of whatever products that they are working on.

You have to accept that some technology will end up being shared in this fashion regardless of the student/technician nationalities. For facilities crucial to national security then it makes to restrict access. If you restrict access to technological research facilities on the basis of nationality then the talent pool shrinks very quickly.

"hopefully the Google affair has been a wake-up call to the West, and our political leaders will thoroughly re-assess their policy towards Mainland China."

Don't be fooled. Technological warfare is a two-way street. Just as there Chinese hackers trying to get into US or European systems so also there are US and European hackers trying to get into Chinese systems. It may come as scant consolation if your personal data is compromised but the idea that systemic hacking is solely practiced by the Chinese is a ridiculous one.

- Recommend? (4)
- Report abuse
- Clip |
- Link

- **conorf**

27 Jan 2010, 1:06PM

"The origins of the oil company hackers are not known"...so why such a focus on China. Are people so naive as to think that hacking comes solely from China and Russia? Though I agree that governments should be be vigilant to attacks from all sources, it seems as though these threads and hacking reports are creating an enemy far greater than any evidence has yet to suggest or prove.

- Recommend? (6)
- Report abuse
- Clip |
- Link

- **Corin**

27 Jan 2010, 1:16PM

I'm with conorf on this. The most likely organisation(s) behind this are other oil companies seeking a competitive advantage.

- Recommend? (4)
- Report abuse
- Clip |
- Link

- **PaPaPeng3**

27 Jan 2010, 7:31PM

The Internet universe is practically run on Microsoft's OS which is known to have many loopholes that require frequent patches to fix. Hackers use these loopholes to illegally access computers. Since MS is an American company it is obvious that the US has both the tools and the means to get right into the fundamental root of the problem to safeguard their data. Trillions of dollars are routed through the same connections by banks across the world every day without anyone being able to hack their network. Surely super sensitive internet users such as the American military and the government should be able to come up with a similar secure system.

I distinctly remember a TIME magazine cover story on cyberwarfare around the time of the First Gulf War where US and Israeli military gummed up Saddam's computers such that the Iraqi military dared not switch on their PCs in case they sent dubious commands or compromised firing instructions to their weapons . These weapons may explode on their mounts or redirect the same weapons into Iraqi installations. Whatever, logic points to MS OS retaining backdoor entrances to computers around the world so that American spy agencies can gain access to target organizations when they want to. Should a hacker discover this backdoor they have a romp around other people's computers until MS comes up with the latest patch that includes a new backdoor entrance. So long as MS has the user market advantage it will keep providing backdoors to US spy agencies. Thus we will forever have hacker attacks and MS patches to close that backdoor and put in another one. Why else is MS OS software so bloated? In the meantime its very

useful to blame China for something no one can prove.

Its time for China to migrate to the Red Flag Linux.

- Recommend? (2)
- Report abuse
- Clip |
- Link

-  **jimmywednesday**

27 Jan 2010, 11:01PM

I taught for for over 8 years in China including business at Huawei and students would regulary admit they would hack into 'western companies' if it helped the mainland, many even saying they would spy and steal in order to make China a more powerful nation.

All countries have hackers but China seems very intent on stealing and distrupting on a much larger scale.

It's a pity the Chinese education system is so poor it cannot produce talented individuals who can create their own cutting edge technology.

China you really must try harder!!

- Recommend? (1)
- Report abuse
- Clip |
- Link

-  **Monkeybiz**

28 Jan 2010, 12:55AM

What's this? Exxon complaining about dirty tricks? ahahahahaha

- Recommend? (2)

- Report abuse
- Clip |
- Link

-  **candleberry**

  28 Jan 2010, 3:17PM

  > The strikes [...] used precision phishing attacks to fool executives into bypassing security procedures.

  Ha. Ha. Ha.

  Idiots.

- - Recommend? (0)
  - Report abuse
  - Clip |
  - Link

Comments are now closed for this entry.

Comments

Sorry, commenting is not available at this time. Please try again later.