By Kim Zetter, Wired.com

Three U.S. oil companies were targeted in a coordinated hack that sought valuable information about new discoveries of oil deposits and other data, according to a new report in the Christian Science Monitor.

The attacks predated by two years recent intrusions into Google and other companies but shared some similarities to those attacks. Highly targeted malicious e-mails were sent to employees and customized spyware attempted to grab specific data.

The hackers sought “bid data,” which details the location of oil deposits around the world as well as their size and value.

“Knowing which one of those blocks is oil-bearing — and which to go for and which not — is clearly worth something,” Paul Dorey, former chief information security officer at BP, told the Monitor. “If I was a foreign government, that’s the data I would want to get — and any analysis that reveals [a company`s] intention.”

The three companies that were hit — ExxonMobil, ConocoPhillips and Marathon Oil — didn’t confirm the hacks to the Monitor. But according to sources who spoke with the paper, the companies were unaware of the extent of the attacks until authorities disclosed that the hackers had been siphoning e-mail passwords and other data associated with executives who had access to proprietary oil exploration and discovery information.

“We’ve seen real, targeted attacks on our C-level [most senior] executives,” an anonymous oil company official told the Monitor.

In February 2009, federal officials from the National Cyber Investigative Joint Task Force met with oil company executives and their technology teams to discuss what occurred.

Marathon Oil first became suspicious when, on Nov. 13, 2008, a senior executive in the company’s Houston office received an e-mail that appeared to be a reply to a message she had sent a corporate colleague overseas. The original message, which included a URL, related to the U.S. government’s bailout plan for U.S. banks. The executive did not send the original message and warned colleagues to avoid the e-mail if they received one.

Investigators would ultimately learn that similar e-mails had been sent to key executives at ExxonMobil and ConocoPhillips, as well. Some of the data siphoned from the companies went to computers overseas, including one located in China.

The Monitor doesn’t say what vulnerability the malicious e-mails targeted. And it’s unclear whether hackers managed to obtain the “bid data” they sought.

It was an Internet Explorer flaw that allowed hackers to breach Google, Adobe and other companies recently targeted in a coordinated attack that hit 34 U.S. firms in the technology, finance and defense industries. Google has indicated that the intrusion into its network originated in China, though attributing attacks definitively is often impossible to determine, because hackers can control computers in China or anywhere else to launch an attack.

The Financial Times reported Monday that the hackers who hit Google focused on employees who had access to proprietary data, then targeted their friends on social networking sites. The hackers were able to take control of the social network accounts of those friends with the aim of sending the targeted employees malicious e-mails from these trusted sources.