

# US oil industry hit by cyberattacks: Was China involved?

MONITOR EXCLUSIVE: Breaches show how sophisticated industrial espionage is becoming. The big question: Who's behind them?



By Mark Clayton Staff writer

posted January 25, 2010 at 2:02 pm EST

Houston —

At least three US oil companies were the target of a series of previously undisclosed cyberattacks that may have originated in China and that experts say highlight a new level of sophistication in the growing global war of Internet espionage.

The oil and gas industry breaches, the mere existence of which has been a closely guarded secret of oil companies and federal authorities, were focused on one of the crown jewels of the industry: valuable “bid data” detailing the quantity, value, and location of oil discoveries worldwide, sources familiar with the attacks say and documents obtained by the Monitor show.

The companies – Marathon Oil, ExxonMobil, and ConocoPhillips – didn’t realize the full extent of the attacks, which occurred in 2008, until the FBI alerted them that year and in early 2009. Federal officials told the companies proprietary information had been flowing out, including to computers overseas, a source familiar with the attacks says and documents show.

The data included e-mail passwords, messages, and other information tied to executives with access to proprietary exploration and discovery information, the source says.

While China’s involvement in the attacks is far from certain, at least some data was detected flowing from one oil company computer to a computer in China, a document indicates. Another oil company’s security personnel privately referred to the breaches in one of the documents as the “China virus.”

“What these guys [corporate officials] don’t realize, because nobody tells them, is that a major foreign intelligence agency has taken control of major portions of their network,” says the source familiar with the attacks. “You can’t get rid of this attacker very easily. It doesn’t work like a normal virus. We’ve never seen anything this clever, this tenacious.”

Neither Marathon Oil, ExxonMobil, nor ConocoPhillips would comment on the attacks or confirm that they had happened. But the breaches, which left dozens of computers and their data vulnerable in those companies' global networks, were confirmed over a five-month Monitor investigation in interviews with dozens of oil industry insiders, cybersecurity experts, former government officials, and by documents describing the attacks

"We've seen real, targeted attacks on our C-level [most senior] executives," says one oil company official, who, like others familiar with various aspects of the attacks, spoke only on condition of anonymity. "I was at a meeting with the FBI earlier this year [2009] that was pretty eye-opening."

The new type of attack involves custom-made spyware that is virtually undetectable by antivirus and other electronic defenses traditionally used by corporations. Experts say the new cyberburglary tools pose a serious threat to corporate America and the long-term competitiveness of the nation.

"We've had friends in the petroleum industry express grave concern because they've spent hundreds of millions of dollars finding out where the next big oil discovery will be," says Ed Skoudis, cofounder of InGuardians, a computer security firm, who was called last year to help a big oil and gas company secure its bid data after its computer network was infiltrated. He wouldn't name the company. "The attacker would be saving huge expenses for himself by stealing that data."

**Not so long ago**, computer hacking was mainly the handiwork of individuals with overactive imaginations and good programming skills, and they often broke into computers for sport. More recently, people with more sinister motives – including organized criminal gangs – have made an industry out of stealing credit-card information and personal identities for quick cash.

But lurking in the cybershadows is a far more insidious and sophisticated form of computer espionage that, until the recent exposure by search-engine titan Google, was little publicized and often went undetected. Such attackers represent the elite – a dark army of cyberspies targeting the heart of corporations around the world where trade secrets, proprietary data, and cutting-edge technologies lie locked away in digital fortresses.

Some of these attacks are believed to be carried out by foreign governments or their surrogates. "Any country that wants to support and develop an indigenous industry may very well use cyberespionage to help do that," says Greg Garcia, assistant secretary for cybersecurity at the Department of Homeland Security under the Bush administration.

While most major nations, including the United States, are conducting Internet espionage, experts say two traditional US adversaries, China and Russia, are among the most aggressive and adept at carrying out such attacks. Both countries are known to have large communities of hackers and a deep base of computer security expertise.

"China, more so than Russia, has a large number of hacker clubs watched closely by the government," says O. Sami Saydjari, a former Department of Defense employee who runs Cyber Defense Agency, a Wisconsin-based security firm. "These talent pools are all potential recruits for China's professional cyberwarfare units. We strongly suspect they encourage their hacker groups to go out and attack foreign entities and get practice."

Spying on other countries' defense agencies and diplomatic corps undoubtedly remains a focus of Internet espionage. But cyberspies are increasingly targeting strategically important businesses, both because of the information to be gleaned and because their defenses are often easier to penetrate.

Google has said it found evidence of at least 20 companies in an array of US industries that had been infiltrated by attacks from China. Was the Chinese government involved? China adamantly says "no." Whether it was or not, the Google breach reveals how pervasive the new espionage war is becoming and how sophisticated the tools are with which it is being waged.

But before Google there was Marathon.

**On Nov. 13, 2008**, a senior executive at Marathon Oil in Houston looked at a strange e-mail on her screen. It appeared to be a response to a message she had sent a corporate colleague overseas. The only problem was, according to a source familiar with the incident who asked for anonymity, she hadn't sent the original e-mail.

Yet there, on her screen, was a "reply" to what looked like her request for a comment on the "Emergency Economic Stabilization Act" – the

federal bailout of US banks. And the original e-mail contained something else: an embedded Internet link. Recognizing the danger, the executive alertly sent out an internal warning that the e-mail was fake and may contain a computer virus.

But, according to the source and documents obtained by the Monitor, her response was too late. The fake had already been forwarded to other people – and someone had clicked on the link it contained. Instantly, an unseen spy program started spreading stealthily across Marathon's global computer network.

Nearly identical fake e-mails that appeared to come from senior executives were also sent to colleagues in key posts at ExxonMobil and ConocoPhillips – all containing a request for them to analyze the Economic Stabilization Act noted on the subject line, a source familiar with the attacks says.

How successful the cyberspies ultimately were – whoever they were – isn't publicly known.

"Marathon does not comment on security matters due to the confidential nature of such issues," the company said in a statement to the Monitor. "Our Company recognizes the critical importance of ensuring the security of all aspects of our operations and to accomplish this we continually monitor and review the security systems and processes we have in place to protect our facilities, employees and the communities in which we operate."

**The attacks that infiltrated** Marathon, ExxonMobil, and ConocoPhillips penetrated their electronic defenses using a combination of fake e-mails and customized spyware programs to target specific data, according to multiple sources and documents.

Such customized attacks first began infiltrating corporate computer networks in low numbers around 2004, but have become far more common in the past year. An estimated \$1 trillion in intellectual property was stolen worldwide through cyberspace in 2008, according to a study last year by the antivirus company McAfee.

"We've seen across many industries in recent months a very targeted type of attack," says Rob Lee, a computer forensics expert and director at Mandiant, a cybersecurity company in Alexandria, Va. "These are professionals [working in teams], not people doing this at night."

Many experts say the theft of this kind of information – about, for instance, the temperature and valve settings of chemical plant processes or the source code of a software company – can give competitors an advantage, and over time could degrade America's global economic competitiveness.

"Identity theft is small potatoes compared to this new type of attack we've been seeing the past 18 months," says Scott Borg, who heads the US Cyber Consequences Unit, a nonprofit that advises government and the private sector. "This is a gigantic loss with significant economic damage."

Yet it's often hard to prove – or even know – if outsiders have infiltrated a network or pilfered any information. Many companies are unwilling to tell shareholders or law enforcement that they've been attacked.

Even more basic, many corporate executives aren't aware of how sophisticated the new espionage software has become and cling to outdated forms of electronic defense.

"Antivirus software misses more than 20 percent of the Trojans in my testing," says Paul Williams, a cybersecurity expert who spoke at a recent oil and gas industry conference in Houston.

One new type of intruder, for instance, is customized "zero-day" spyware – so-called because its digital signature is so new that it has not yet been catalogued by antivirus companies. "Phishing," trying to acquire sensitive information through fraudulent e-mails or instant messages, is a common criminal technique. A more insidious variant, "spear-phishing," customizes the fake e-mail for a company in the hope of fooling key personnel into introducing the spyware throughout a computer network.

Once a bogus link is clicked on, a single intruding piece of advanced spyware can change digital signatures to evade detection, spin off decoys, and lie low while waiting to pilfer targeted information. It gives clandestine control of a network over to the outside attackers. When the program finds data, it encrypts the information and sends it back to the cyberthieves.

"I can confirm for you that this type of advanced attack is happening to companies across the US today," says Daniel Geer, chief information security officer for In-Q-Tel, a nonprofit venture capital firm funded by the Central Intelligence Agency.

The new cyberwarfare has become complex enough that specialized teams are used to carry out different operations. Often, an “intrusion team” of professional hackers will work to breach the system. An “exfiltration team” will retrieve the data. Another unit might be dedicated to maintaining an electronic foothold in the network for years. “There are clear lines of responsibility between different actors going on,” says Mr. Lee of Mandiant.

**Fake “phishing” e-mails** are a familiar problem in corporate America and usually easily dealt with. Oil companies employ some of the top computer security talent. But the Nov. 13, 2008, e-mail to the executive at Marathon was not an ordinary phishing e-mail, as company officials found out when the FBI contacted them.

Agents told the companies that their computer networks were being covertly manipulated by outsiders and proprietary information had been flowing out, according to the source and documents. (FBI officials in Washington and Houston refused to comment on the cases or to acknowledge that they were involved in them.)

Once alerted, the Marathon team began finding other e-mail accounts, passwords, and personal computers that were “compromised,” says the source and documents show.

**On Feb. 5, 2009**, a handful of senior oil company executives and key technology people listened as federal officials from the National Cyber Investigative Joint Task Force in Fairfax, Va., – whose partner agencies include the Federal Bureau of Investigation, Secret Service, and members of the US intelligence community – began sharing some of what they had detected, documents show. Federal officials told the companies, for instance, that conventional defenses like antivirus software were not likely to be effective against “state-sponsored attacks,” the documents show.

Further, based on the kind of information that was being stolen, federal officials said a key target appeared to be bid data potentially valuable to “state-owned energy companies,” according to a written summary of the meeting. Marathon and other oil companies spend billions worldwide to locate new deposits. Most oil “lease blocks” produce little of value. But a few yield vast returns, and the estimates of where oil might be found and how much it might yield could give an outside entity a big advantage in bidding wars for prime leases.

China would certainly be interested in this kind of data, experts say. With the country’s economy consuming huge amounts of energy, China’s state-owned oil companies have been among the most aggressive in going after available leases around the world, particularly in Nigeria and Angola, where many US companies are also competing for tracts.

“Knowing which one of those blocks is oil-bearing – and which to go for and which not – is clearly worth something,” says Paul Dorey, former chief information security officer at BP, the world’s third-largest oil company, and now a computer-security consultant in London. “If I was a foreign government, that’s the data I would want to get – and any analysis that reveals [a company’s] intention. Yes, that would be pretty valuable.”

Still, a simple thirst for oil is no proof that a country is conducting corporate espionage. Even the suggestion, contained in one of the documents, that some data had flowed from a ConocoPhillips computer to a computer in China could have been the result of some other nation’s cyberspy unit co-opting Chinese servers to cover their tracks, experts say. Lee and other specialists admit that it will be difficult, and perhaps impossible, to ever determine definitively who was behind the attacks.

Even so, the oil industry breaches coincide with a growing number of coordinated cyberassaults in the US that many experts do blame on the Chinese. The Google allegations are just the most recent.

“What I’m saying to you is that it’s not just the oil and gas industry that’s vulnerable to this kind of attack: It’s any industry that the Chinese decide they want to take a look at,” says an FBI source. “It’s like they’re just going down the street picking out what they want to have.”

Last March, Canadian researchers identified 1,295 computers in 103 countries infected by spyware and operated by someone as a “GhostNet” or cyberspy network. In each case, a Trojan program was downloaded that allowed the attackers control of the computers traceable, the report said, to “commercial Internet accounts on the island of Hainan,” which is the home of the Chinese Army’s intelligence facility.

In October, a report by the US-China Economic and Security Review Commission summarized the threat bluntly. “China is likely using its maturing computer network exploitation capability to support intelligence collection against the US Government and industry by conducting a long term, sophisticated, computer network exploitation campaign.”

Chinese officials refuted the report when it came out, and, more recently, a spokesman for the Chinese Embassy in Washington, Wang Baodong, denied any Chinese involvement in the oil and gas industry attacks, saying the country forbids “all forms of cybercrimes, including hacking activities.”

Others remain skeptical. “The China threat is constant,” says Shawn Carpenter, principal forensics analyst for NetWitness, a cybersecurity company. “If there’s valuable intellectual property out there, there are people in China and elsewhere who want to take it. It’s the new battlefield – low risk and low investment with high gain.”



© The Christian Science Monitor. All Rights Reserved. [Terms](#) under which this service is provided to you. [Privacy Policy](#).