# US probing cyber attacks on gas pipelines (Update)

May 8 2012

A natural gas pipeline yard in Skokie, Illinois. A series of cyber attacks has been targeting US natural gas pipeline operators, officials acknowledged Tuesday, raising concerns among security experts about vulnerabilities in key infrastructure.

A campaign of cyber attacks has been targeting US natural gas pipeline operators, officials acknowledged Tuesday, raising security concerns about vulnerabilities in key infrastructure.

The Department of Homeland Security "has been working since March 2012 with critical infrastructure owners and operators in the oil and natural gas sector to address a series of cyber intrusions targeting natural gas pipeline companies," DHS spokesman Peter Boogaard said in an email to AFP.

He said the attack "involves sophisticated spear-phishing activities targeting personnel within the private companies" and added that the FBI and other federal agencies are assisting in the probe.

Spear-phishing is a technique used to target a specific company or organization by sending fake emails designed to get employees to divulge passwords or other security information.

The Christian Science Monitor first reported confidential alerts had been made to US energy firms.

A public alert released by an arm of DHS said the activity may date back to December 2011.

The alert from the DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) said the e-mails "have been convincingly crafted to appear as though they were sent from a trusted member internal to the organization."

But the cybersecurity arm said some of the information about the attacks is "sensitive and cannot be disseminated through public or unsecure channels."

Interstate Natural Gas Association of America spokeswoman Cathy Landry told AFP that its member firms had been in contact with investigators.

"We know the nature of the threat but we don't know the intent of the threat," she said. "We have been getting the word out to everyone in the industry, we want to make sure everyone knows this threat is out there."

Joe Weiss, managing partner for the security firm Applied Control Solutions, said the latest attacks highlight the vulnerability of so-called

critical infrastructure systems.

He said control systems vulnerabilities can be found in the electrical grid, water utilities and others as well as pipeline operators.

"Once you get to those systems, really bad things happen," he said. "That's where people die."

But tracking the attacks can be difficult because of a lack of forensics, Weiss said.

"You have your usual list of suspects, nation-states like Iran, radical Muslims, a bunch of radical organizations in the states who don't like anyone they feel is not environmentally friendly," he told AFP

"But you also now have cyber exploit code on the Web for free that any number of people can get to."

Weiss said the motivation was unclear, because the attackers may be unhappy with the companies, may be targeting the infrastructure or may simply be hacking to show it can be done.

He maintained that security is often looser in the field operations than in corporate websites, because most firms do not expect those operations to be accessed by outsiders.

"We don't know if (the target) is the pipelines themselves or the pipeline companies," he said.

Kapil Raina of the security firm Zscaler said the biggest fear "would be a coordinated attack on several facilities that would trigger automatic responses at other facilities, potentially causing a chained effect -- similar to an electrical blackout but with more severe consequences."

Because natural gas prices are low, he said, "the attack could have other affects including driving up the price of natural gas dramatically and creating financial market turmoil."

The news of the attacks comes with the US experiencing a natural gas boom thanks to expanded use of hydraulic fracturing or "fracking" which can unlock shale gas from deposits that had previously been inaccessible.

Brian Contos of the online security firm McAfee, said these types of attacks are increasingly common and that companies are responding with tighter controls.

"What we thought kept us secure the last 20 years won't keep us secure the next. As the enemy matures and adapts so must we," Contos said.