

The New York Times Reprints

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers [here](#) or use the "Reprints" tool that appears next to any article. Visit www.nytreprints.com for samples and additional information. [Order a reprint of this article now.](#)

January 19, 2011

E.U. Closes Emissions Trading System After Thefts

By **JAMES KANTER**

BRUSSELS — The [European Commission](#) suspended trading in greenhouse gas emissions permits on Wednesday for at least a week after the theft of permits worth millions of euros via online attacks.

The Emissions Trading System was a target of “recurring security breaches” over the last two months, the commission, the executive agency of the [European Union](#), announced on its Web site Wednesday.

The commission said it needed to shut the system down until at least Jan. 26 because “incidents over the last weeks have underlined the urgent need” for enhanced security measures.

The attacks raised new questions about the viability of Europe’s main tool to combat a rise in greenhouse gases in the atmosphere.

The stolen permits are part of Europe’s effort to cap the amount of carbon dioxide, the main greenhouse gas, that companies may emit each year. Europe’s system is the world’s largest market for greenhouse gas emissions credits.

Companies exceeding their emissions quotas buy certificates from companies that succeeded in shrinking their carbon footprint by, for example, adopting lower-emission technology or modifying production in other ways.

Some of the thefts of credits early this week were from electronic registries in Austria, Greece, the Czech Republic, Poland and Estonia, said Maria Kokkonen, a spokeswoman for Connie Hedegaard, the Europe’s commissioner for climate action.

“It could be a concerted action by fraudsters to get access and steal permits from legitimate accounts to sell on spot markets before the thefts were discovered,” Ms. Kokkonen said.

The permits stolen from the Czech registry were worth about 7 million euros (\$9.3 million), she said. She was unable to comment on the value of the allowances stolen in other countries.

Analysts said the thefts added up to a serious challenge to the system, which Europe wants other

parts of the world — the United States included — to emulate.

“Although such incidents are negligible in terms of actual market impact, they will over time undermine the credibility of carbon trading as a policy measure to reduce emissions in Europe,” said Kjersti Ulset, a manager at Point Carbon, a company that reports on emissions markets and provides consultancy services.

Europe issued security guidelines after a similar attack in early 2010, but the latest case will almost certainly force the authorities to invest in new and more secure hardware.

“By investing tens of thousands of euros to upgrade their I.T. systems, member states could prevent losses on the scale of millions of euros,” Ms. Kokkonen said, referring to information technology systems.

Europe’s system has had a rocky ride since trading began six years ago, including extreme volatility, tax fraud, recycling of used credits and suspicions of profiteering, in addition to online attacks.

One year ago, swindlers used fake e-mail messages to obtain access codes for individual accounts on the national registries that make up Europe’s system.

Traders and companies who fell for that ploy were directed to a rogue Web site and invited to enter their security codes — a practice known as phishing.

The swindlers used the stolen codes to gain access to electronic certificates that represent quantities of greenhouse gases. They then sold the certificates through trading accounts registered in Denmark and Britain. That attack was estimated to have netted the swindlers as much as \$4 million from Germany alone.

Ms. Kokkonen said Wednesday that it was still unclear what methods were used to steal the permits in the latest attacks and that authorities still were looking into the matter.