Russian hackers tricked people into giving their passwords

July 26 2018, by Colleen Long

In this Jan. 31, 2018, file photo, the sun rises beyond power lines in St. Charles Parish, La. Homeland Security officials say that Russian hackers used conventional tools to trick victims into entering passwords in order to build out a sophisticated effort to gain access to control rooms of utilities in the U.S. The victims included hundreds of vendors that had links to nuclear plants and the electrical grid. (AP Photo/Gerald Herbert, File)

Russian hackers who penetrated hundreds of U.S. utilities,

manufacturing plants and other facilities last year gained access by using the most conventional of phishing tools, tricking staffers into entering passwords, officials say.

The Russians targeted mostly the energy sector but also nuclear, aviation and critical manufacturing, Jonathan Homer, head of Homeland Security's industrial control system analysis, said during a briefing Wednesday.

They had the capability to cause mass blackouts, but chose not to, and there was no threat the grid would go down, the officials said. Instead, the hackers appeared more focused on reconnaissance.

The 2017 attack prompted a rebuke from the Trump administration earlier this year.

The victims ranged from smaller companies with no major budget for cybersecurity to large corporations with sophisticated security networks, Homer said. Vendors were targeted because of their direct access to the utilities—companies that run diagnostics or update software or perform other tasks to keep the systems running. The victims were not identified.

"This is a situation where they went in and said this is what they're looking for, and found weaknesses there," Homer said.

The newly disclosed details of the 2017 hack come amid growing concerns over Russia's efforts to interfere in the November midterm elections and the recent indictments of a dozen Russian military intelligence officers accused of infiltrating the Clinton presidential campaign and the Democratic Party and releasing tens of thousands of private communications.

U.S. national security officials previously said they had determined that

Russian intelligence and others were behind the cyberattacks. They said the hackers chose their targets methodically, obtained access to computer systems, conducted "network reconnaissance" and then attempted to cover their tracks by deleting evidence of the intrusions. The U.S. government said it had helped the industries expel the Russians from all systems known to have been penetrated.

It wasn't clear if more had been compromised since news of the attack was made public earlier this year. Wednesday's briefing was intended to help businesses defend themselves from future attacks.

Homer said the attack began in 2016 with a single breach that stayed dormant nearly a year before other infiltrations occurred in concentric circles closer and closer to the U.S. systems.

Hackers used a mix of real people downloading open-source information from company websites like photos and other data, and attacks that trick employees into entering passwords on spoofed websites. Hackers then use the passwords to compromise corporate networks. It's possible some of the companies are unaware they were compromised, because hackers used credentials of actual employees to get inside, which could make it harder to detect, officials said.