Issued 7/26/18

Russian Hackers used Phishing Tools in 2017 Attack on Grid

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 said Wednesday. 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. 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 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. 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.