The New York Times | https://nyti.ms/2tRVPNq

TECHNOLOGY

Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say

By NICOLE PERLROTH JULY 6, 2017

Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries.

Among the companies targeted was the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kan., according to security consultants and an urgent joint report issued by the Department of Homeland Security and the Federal Bureau of Investigation last week.

The joint report was obtained by The New York Times and confirmed by security specialists who have been responding to the attacks. It carried an urgent amber warning, the second-highest rating for the sensitivity of the threat.

The report did not indicate whether the cyberattacks were an attempt at espionage — such as stealing industrial secrets — or part of a plan to cause destruction. There is no indication that hackers were able to jump from their victims' computers into the control systems of the facilities, nor is it clear how many facilities were breached.

Wolf Creek officials said that while they could not comment on cyberattacks or security issues, no “operations systems” had been affected and that their corporate network and the internet were separate from the network that runs the plant.

In a joint statement with the F.B.I., a spokesman for the Department of Homeland Security said, “There is no indication of a threat to public safety, as any potential impact appears to be limited to administrative and business networks.”

The hackers appeared determined to map out computer networks for future attacks, the report concluded. But investigators have not been able to analyze the malicious “payload” of the hackers’ code, which would offer more detail into what they were after.

John Keeley, a spokesman for the Nuclear Energy Institute, which works with all 99 electric utilities that operate nuclear plants in the United States, said nuclear facilities are required to report cyberattacks that relate to their “safety, security and operations.” None have reported that the security of their operations was affected by the latest attacks, Mr. Keeley said.

In most cases, the attacks targeted people — industrial control engineers who have direct access to systems that, if damaged, could lead to an explosion, fire or a spill of dangerous material, according to two people familiar with the attacks who could not be named because of confidentiality agreements.

The origins of the hackers are not known. But the report indicated that an “advanced persistent threat” actor was responsible, which is the language security specialists often use to describe hackers backed by governments.

The two people familiar with the investigation say that, while it is still in its early stages, the hackers’ techniques mimicked those of the organization known to cybersecurity specialists as “Energetic Bear,” the Russian hacking group that researchers have tied to attacks on the energy sector since at least 2012.

Hackers wrote highly targeted email messages containing fake résumés for control engineering jobs and sent them to the senior industrial control engineers who maintain broad access to critical industrial control systems, the government report said.

The fake résumés were Microsoft Word documents that were laced with malicious code. Once the recipients clicked on those documents, attackers could steal their credentials and proceed to other machines on a network.

In some cases, the hackers also compromised legitimate websites that they knew their victims frequented — something security specialists call a watering hole attack. And in others, they deployed what are known as man-in-the-middle attacks in which they redirected their victims' internet traffic through their own machines.

Energy, nuclear and critical manufacturing organizations have frequently been targets for sophisticated cyberattacks. The Department of Homeland Security has called cyberattacks on critical infrastructure "one of the most serious national security challenges we must confront."

On May 11, during the attacks, President Trump signed an executive order to strengthen the cybersecurity defenses of federal networks and critical infrastructure. The order required government agencies to work with public companies to mitigate risks and help defend critical infrastructure organizations "at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

The order specifically addressed the threats from "electricity disruptions and prolonged power outages resulting from cybersecurity incidents."

Jon Wellinghoff, the former chairman of the Federal Energy Regulatory Commission, said in an interview last week that while the security of United States' critical infrastructure systems had improved in recent years, they were still vulnerable to advanced hacking attacks, particularly those that use tools stolen from the National Security Agency.

"We never anticipated that our critical infrastructure control systems would be facing advanced levels of malware," Mr. Wellinghoff said.

In 2008, an attack called Stuxnet that was designed by the United States and Israel to hit Iran's main nuclear enrichment facility, demonstrated how computer attacks could disrupt and destroy physical infrastructure.

The government hackers infiltrated the systems that controlled Iran's nuclear centrifuges and spun them wildly out of control, or stopped them from spinning entirely, destroying a fifth of Iran's centrifuges.

In retrospect, Mr. Wellinghoff said that attack should have foreshadowed the threats the United States would face on its own infrastructure.

Critical infrastructure is increasingly controlled by Scada, or supervisory control and data acquisition systems. They are used by manufacturers, nuclear plant operators and pipeline operators to monitor variables like pressure and flow rates through pipelines. The software also allows operators to monitor and diagnose unexpected problems.

But like any software, Scada systems are susceptible to hacking and computer viruses. And for years, security specialists have warned that hackers could use remote access to these systems to cause physical destruction.

A version of this article appears in print on July 7, 2017, on Page B5 of the New York edition with the headline: Hackers Are Targeting Nuclear Plants, U.S. Says.
