

By JORDAN ROBERTSON, AP Technology Writer Jordan Robertson, AP Technology Writer – Thu Jan 28, 2:24 pm ET

http://news.yahoo.com/s/ap/20100128/ap_on_hi_te/us_tec_hacking_critical_infrastructure

SAN FRANCISCO – More than half of the operators of power plants and other "critical infrastructure" say in a new study that their computer networks have been infiltrated by sophisticated adversaries. In many cases, foreign governments are suspected.

The findings come in a survey being released Thursday that offers a rare public look at the damage computer criminals can do to vital institutions such as power grids, water and sewage systems and oil and gas companies. Manipulating the computer systems can cause power outages, floods, sewage spills and oil leaks.

The report was based on an survey completed by 600 executives and technology managers from infrastructure operators in 14 countries. The report was prepared by McAfee Inc., which makes security software, and the Center for Strategic and International Studies in Washington, which analyzed the data and conducted additional interviews. The respondents aren't named and specifics aren't given about what happened in the attacks.

The report comes as concerns are growing about state-sponsored hacking and threats to critical infrastructure.

In November, CBS's "60 Minutes" reported that several Brazilian power outages were caused by hackers — a report that Brazilian officials have played down. Last April, U.S. government officials said that spies hacked into the U.S. electric grid and left behind computer programs that would let them disrupt service. The intrusions were discovered after electric companies gave the government permission to audit their systems.

In the new report, 54 percent of respondents acknowledged that they had been hit by "stealthy infiltration" of their networks. In such break-ins, criminals can plant malicious software to steal files, spy on e-mails and do even scarier things like remotely controlling equipment inside a utility.

Utilities are increasingly using mainstream software and connecting parts of their operations to the Internet so technicians can service problems remotely. Both factors heighten the danger of a hacker break-in.

The same percentage of respondents also said they have experienced large-scale "denial-of-service" attacks, in which a computer network is knocked out of service because of it is flooded with bogus Internet traffic. The infrastructure operators frequently said they believed representatives of foreign governments were involved.

Perhaps even more alarming: Many intruders have apparently done something harmful with the access they've stolen. Operators who had experienced denial of service attacks often said the incidents had at least some effect, from minor service interruptions to sustained damage and critical breakdowns.

Extortion is a common motivation, with hackers demanding money to end or agree not to carry out an attack. The power and oil and gas sectors were the most frequently targeted.

Identifying the culprits in such attacks can be next to impossible, because computer attacks are typically routed through multiple layers of infected computers to disguise the source. However, researchers can often learn clues about the attackers' country of origin by studying the language and other signs in the malicious software's programming.