The Washington Post

Hackers Break Into Virginia Health Professions Database, Demand Ransom

Hackers last week broke into a Virginia state Web site used by pharmacists to track prescription drug abuse. They deleted records on more than 8 million patients and replaced the site's homepage with a ransom note demanding $10 million for the return of the records, according to a posting on Wikileaks.org, an online clearinghouse for leaked documents.

Wikileaks reports that the Web site for the **Virginia Prescription Monitoring Program** was defaced last week with a message claiming that the database of prescriptions had been bundled into an encrypted, password-protected file.

Wikileaks has published a copy of the ransom note left in place of the PMP home page, a message that claims the state of Virginia would need to pay the demand in order to gain access to a password needed to unlock those records:

"I have your [expletive] In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh :(For $10 million, I will gladly send along the password."

The site, along with a number of other Web pages related to Virginia Department of Health Professions, remains unreachable at this time. **Sandra Whitley Ryals**, director of Virginia's Department of Health Professions, declined to discuss details of the hacker's claims, and referred inquires to the FBI.

"There is a criminal investigation under way by federal and state authorities, and we take the information security very serious," she said.

A spokesman for the FBI declined to confirm or deny that the agency may be investigating.

Whitley Ryals said the state discovered the intrusion on April 30, after which time it shut down Web site site access to dozens of pages serving the Department of Health Professions. The state also has temporarily discontinued e-mail to and from the department pending the outcome of a security audit, Whitley Ryals said.

"We do have some of systems restored, but we're being very careful in working with experts and authorities to take essential steps as we proceed forward," she said. "Only when the experts tell us that these systems are safe and secure for being live and interactive will that restoration be complete."

She added that the department does have a page online at www.dhp.virginia.gov that lists the phone and fax numbers for various state health boards, and that the state would continue issuing health care licenses and investigating violations of the law or regulations of state health licensees.

This is the second major extortion attack related to the theft of health care data in the past year. In October 2008, Express Scripts, one of the nation's largest processors of pharmacy prescriptions, disclosed that extortionists were threatening to disclose personal and medical information on millions of Americans if the company failed to meet payment demands. Express Scripts is currently offering a $1 million reward for information leading to the arrest and conviction of the individual(s) responsible for trying to extort money from the company.

By Brian Krebs | May 4, 2009; 6:39 PM ET
Categories: Fraud , Latest Warnings , Misc. , U.S. Government , Web Fraud 2.0
| Tags: defacement, extortion, hack, state of virginia