Expert: Rural US websites easy target for hackers

August 8 2011, By NOMAAN MERCHANT and RAPHAEL G. SATTER , Associated Press

(AP) -- The digital trove of credit card numbers and emails stolen by the group known as Anonymous came from towns across rural America - places like Gassville, Ark. and Tishomingo County, Miss., where officers don't usually have to worry about international hackers.

That may have made them an easy score.

The loosely-knit hacking collective said Saturday that it attacked 70 mostly rural law enforcement websites in the United States in retaliation for the arrests of its sympathizers. Some county sheriffs said they were told about the hacking, but others appeared to learn of the scope of what had happened only when contacted by The Associated Press.

Web security experts said the cyberattack shows that no website is too small to avoid hacking, especially as more law enforcement agencies upload sensitive information about investigations, inmates and officers to their sites.

"It seems to me to be low-hanging fruit," said Dick Mackey, vice president of consulting at Sudbury, Mass.-based SystemExperts. "The smaller the organization, the more likely that they don't think of themselves as potential targets. They're not going to have the protections in place that a larger organization will have."

Many of the sheriff's offices outsourced their websites to the same

Mountain Home, Ark.-based media hosting company, Brooks-Jeffrey Marketing. If Brooks-Jeffrey's defenses were breached, that would give hackers access to every website the company hosted, said Kevin Mitnick, a security consultant and former hacker.

Brooks-Jeffrey declined to comment.

Most of the sheriffs' department sites, if not all, were either unavailable for most of Saturday or had been wiped clean of content. Some had started to reappear online Saturday evening.

The emails were mainly from sheriffs' offices in Arkansas, Kansas, Louisiana, Missouri and Mississippi. Many of the leaked emails appeared to be benign, but some of the stolen material seen by the AP carried sensitive information, including tips about suspected crimes, profiles of gang members and security training. At least one email had material - including pictures of teenage girls in their swimsuits - that Tim Mayfield, the police chief in Gassville, Ark., said was sent to him as part of an ongoing investigation. Mayfield declined to provide more details.

In another email that Anonymous posted, a police tipster wrote that his uncle was a convicted sexual offender who was homeless and hanging around an area Walmart and other places where children were. Another tipster wrote to police that she and her neighbors could smell drugs coming from a house.

The leaked information also included five credit card numbers Anonymous said were used to make "involuntary donations." At least four of the names and other personal details appeared to be genuine. One person confirmed to the AP that his credit card had been used improperly.

In a statement, Anonymous said it leaked "a massive amount of

confidential information that is sure to (embarrass), discredit and incriminate police officers across the US." The group said it hopes its disclosures would "demonstrate the inherently corrupt nature of law enforcement using their own words" and "disrupt and sabotage their ability to communicate and terrorize communities."

The group did not say specifically why these sheriffs' departments were targeted, but Anonymous members have increasingly been pursued by law enforcement in the United States and elsewhere following a string of high-profile data thefts and denial of service attacks - operations that block websites by flooding them with traffic. FBI spokesman Steve Frazier did not return several messages Saturday seeking comment on the latest cyberattack.

The group celebrated its success in several messages posted Saturday to Twitter and hinted that more attacks were to come. In one tweet, it poked fun at local sheriffs: "Time to wake up, boys."

Small agencies often need to do more to protect themselves, even if they don't have as much staff or money as larger cities, Mackey said. One major step is demanding better security from the companies that host their sites.

"I think it behooves anyone who stores sensitive information to basically put the pressure on the vendors who create their websites to do a good job of protecting those sites," Mackey said.

Many sheriffs said they weren't using their sites to store Social Security numbers or other highly sensitive data. John Montgomery, sheriff of Baxter County in northern Arkansas, where Brooks-Jeffrey is located, said his department's website has been used in the past to help track down suspects and get information to the public.

"We are going to continue using the Web," said Montgomery, whose website was taken down. "Are we going to have to be smarter in how we use the Web as far as security? Sure. We'll have to look closely at the security measures that go into place."

Montgomery said the department would also check its internal servers for any weaknesses, and he encouraged other county sheriffs to do the same.