The New York Times
Bits The Business of Technology

OCTOBER 3, 2012, 8:34 PM

Hackers Breach 53 Universities and Dump Thousands of Personal Records Online

By NICOLE PERLROTH

Hackers published online Monday thousands of personal records from 53 universities, including Harvard, Stanford, Cornell, Princeton, Johns Hopkins, the University of Zurich and other universities around the world.

The group of hackers, calling themselves Team GhostShell, claimed responsibility for the attack on Twitter and published some 36,000 e-mail addresses and thousands of names, usernames, passwords, addresses and phone numbers of students, faculty and staff, to the Web site Pastebin.com. In most cases the data was already publicly available, but in some instances the records included additional sensitive information such as students' dates of birth and payroll information for university employees.

Typically, hackers seek such information because it can be used to steal identities, crack bank accounts or can be sold on the black market. Universities make ripe targets because they store vast numbers of personal records, often in decentralized servers. The records can be a gold mine because students often have pristine credit reputations and do not monitor their account activity and credit scores as vigilantly as adults.

Dozens of universities have been plagued by breaches recently. Last August alone, the University of Rhode Island warned that students and faculty that their information may have been exposed. And at the University of Arizona, a student discovered a breach after a Google search exposed her personal information - and that of thousands of others at the university. Smaller computer breaches at Queens College and Marquette University were also reported.

In this case, the hackers said they were not motivated by profit but to "raise awareness towards the changes made in today's education." In a message accompanying the stolen data, they bemoaned changing education laws in Europe and spikes in tuition fees in the United States. But they also noted that in many cases, the servers they breached had already been compromised.

"When we got there, we found that a lot of them have malware injected," the hackers wrote on Pastebin.

To breach servers, the hackers used a technique known as an SQL injection, in which they exploit a software vulnerability and enter commands that cause a database to dump its contents. In the case of some universities, the hackers breached multiple servers. In several cases, hackers breached student and alumni blogs-- which contained things like usernames and passwords--not the university servers themselves. At Princeton, for instance, hackers breached a Wordpress blog for Princeton alums based in the United Kingdom which contained several usernames and encoded passwords.

IdentifyFinder, a firm that works to prevent identify theft from security breaches, analyzed the published data and said it appeared to be legitimate. The company analyzed the data and found 36,623 unique e-mail addresses and tens of thousands of student, faculty and staff names as well as thousands more usernames and passwords, some encrypted but many stored in plain text.

Aaron Titus, a spokesman for IdentityFinder, said that in analyzing the hackers' attack methods, there was evidence that in many cases they had been inside the universities' systems for "at least four months."

Lisa Ann Lapin, a spokeswoman for Stanford University, said that the university discovered the breach Tuesday evening. She confirmed that two departmental Web sites belonging to the university had been accessed, but said the servers "have been secured."

"Our information security officers consider the breaches to be minor in nature," Ms. Lapin said. "No restricted or prohibited data was compromised, nor was any sensitive or other personal information that could lead to identity theft."

At colleges across the country, some students set up sites that allowed students and faculty to search the leaked data for their information. For instance, at the University of Pennsylvania, Matt Parmett, a junior, created a Web site that made it possible for classmates to search the leaked data by name.

http://bits.blogs.nytimes.com/2012/10/03/hackers-breach-53-universities-dump-thousands-of-personal-records-online/?elq=3c0a7e78ad19446eac41cc0334bf6d74&elqCampaignId=269