Hackers throw campus info caution to the wind

October 4 2012, by Nancy Owano

(Phys.org)—For 53 universities, this was the week that brought a line of enquiry they could well do without: How much damage are we dealing with? Hackers on Monday threw thousands of personal records from 53 universities online, posted to Pastebin. Affected schools included Harvard, Stanford, Cornell, Princeton, Johns Hopkins and University of Zurich. Identity Finder reported the exploit involved e-mail addresses and names of students, faculty and staff along with usernames and passwords. Only some were encrypted while others were in plain text. Although the hackers claim to have posted 120,000 accounts, Identity Finder could confirm less than that.

Numbers vary according to different news accounts; some estimated around 40,000 accounts were exposed while others estimate numbers closer to 36,000.

Team GhostShell, which describes itself as a publisher of sensitive data worldwide, claimed responsibility for the attack Their motive was not data theft for personal gain but winning attention toward problems in today's education system. They criticized tuition costs and other issues.

"We have set out to raise awareness towards the changes made in today's education, how new laws imposed by politicians affect us, our economy and overall, our way of life. How far we have ventured from learning valuable skills that would normally help us be prepared in life, to just, simply memorizing large chunks of text in exchange for good grades."

They spoke against soaring tuitions fees "so much that by the time you finish any sort of degree, you will be in more debt than you can handle and with no certainty that you will get a job, to Asia, where strict & limited teachings still persist and never seem to catch up with the times and most of the time fail to prep you up for a world where foreign affairs are crucial in this day and age."

Some of the servers they breached had already been compromised. They found the servers were already malware injected. According to Identity Finder, there was evidence that in some cases they had been inside the universities' systems for at least four months. The technique they used to gain access to the information is described as SQL injection. Hackers' commands can cause a database to "dump" its contents. The rogue SQL commands result in dumping the database contents to the attacker. An article expressing concern about these types of attacks in *SecurityWee*k earlier this year noted that SQL injection attacks are well known security threats and yet they are growing in prevalence. "The ease of spawning these attacks, paired with the surplus of vulnerable websites and applications available to go after, make this type of data breach a prime choice for hackers."

Reacting to the hacker news, some students set up sites to help those who may be affected go through the leaked data to see if they could spot their information.

© 2012 Phys.org

Citation: Hackers throw campus info caution to the wind (2012, October 4) retrieved 24 May 2024 from https://phys.org/news/2012-10-hackers-campus-info-caution.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.