Malware continues to be a challenge to computer security

February 5 2010

(PhysOrg.com) -- Identity theft continues to be a serious problem nationwide, and according to the nonprofit Identity Theft Resource Center, (ITRC) the economic recession may be a cause in the rise in scams, thievery and hacking. According to the center, confirmed breaches in the United States in 2009 resulted in 222,477,043 records containing personally identifiable information being exposed to potential identity theft. Breaches have hit virtually everywhere, including the federal government, major credit card companies, businesses and higher education institutions.

Penn State has experienced computer breaches due to malware, as previously reported on Penn State Live. Malware is short for malicious software and refers to any software designed to cause damage to a single computer, server, or computer network, whether it's a virus, spyware, worm or other destructive program.

The most recent breach occurred in the Student Aid Office in January, when malware exposed 5,600 records containing Social Security Numbers. These records represent a combination of current and former students. Letters are going out today (Feb. 5) to those affected by the breach, in line with the Pennsylvania Breach of Personal Information Notification Act, which mandates that the University notify anyone whose personally identifiable information is potentially disclosed when a computer is lost or compromised.

At this time, the University has no evidence that the information was accessed by unauthorized individuals, but those affected should be alert in the event that an individual attempts to use their identity. "Even when theft is only a remote possibility, we alert anyone who may have been affected, and arm them with information and steps to take to mitigate their risk," said Sarah Morrow, chief privacy officer for the University.

Hackers are getting increasingly creative in their ploys to get computer users to unwittingly download malware onto their computers by clicking on seemingly innocent links.

The latest scam as reported by the ITRC involves an IRS Form W-2 spoof, coming from the e-mail address update(at)irs.com. According to the ITRC site, "A couple of days after the United States Internal Revenue Service (IRS) kicked off the 2010 tax filing season on Jan. 4, Trend Micro researchers received samples of spammed email messages informing recipients that there have been some important changes in the IRS Employers W-2 forms. … The message also comes with an attachment, which is supposed to be a copy of the updated version of the W-2 form. The attached file (Update.doc) contains an embedded file named W-2update.pdf, which is actually a malicious EXE file."

This is just one example of how easy it is to infect a computer with malware. "The scary part is, you don't have to do anything wrong anymore to infect your computer," said Kathy Kimball, senior director in Penn State's Security Operations and Services Office. "The threat has changed such that you do not need to click on anything, just visit a compromised page. That's the game changer -- the user does not have to do anything active at all, not even a click. Just visiting the infected site is sufficient if active content (scripting) is allowed at all. Legitimate Web browsing can compromise a computer, if the site you browse to has been compromised. That's the big 'wow.' It means we don't have a great way to make sure your computer won't be taken over."

Once infected, a computer is susceptible to being controlled remotely by unauthorized users for anything from being used as a host to send spam e-mails or share copyrighted files such as music or movies, to stealing information from the computer. If the infected computer - or any computer networked with the infected computer - contains sensitive information such as Social Security Numbers or other personally identifiable information, the possibility of identity theft exists.

The key, therefore, is making sure sensitive data is secured so if a computer is compromised, no sensitive data is exposed. That's no easy task, explains Michael Spinney, a senior privacy analyst at the Ponemon Institute. The institute conducts independent research on privacy, data protection and information security policy.

"One of the things we found in terms of protecting information at a large university is that you're dealing with a computer network that's a hybrid. You've got different organizations within the university structure that operate independently, different colleges and even different campuses within a single university," Spinney said. "They each have their own network, their own set of information, and yet they're also tied into other networks in other parts of the university."

Spinney said what people need to understand is that while a university is a place people go to learn, ultimately it's a business. "It has employees for whom there is health insurance and payroll information on file. It has students who also may have health insurance through the school, along with work-study payroll information and student aid information. This is the kind of information cyberthieves are dying to get their hands on," he said. "That's why schools are just as attractive - if not more attractive - to cyberthieves as other businesses, based on the information they have and the challenges IT people have in securing it all. It's important for people to understand the scope of the problem, so they can take steps to help prevent it," he said.

Kimball said Penn State's data protection efforts include a scanning procedure done using software that searches for strings that could possibly be Social Security Numbers or other personally identifiable information. If such strings are identified, steps are taken to verify what information is on the computer, and then if there is personally identifying information found it can be moved to a more secure server. "Some units have completed the initial scanning process, but with 24 campuses, there are many, many University-owned computers so it's a slow process," Kimball said.

More information: More information about the process can be found at sos.its.psu.edu/ online.

Provided by Pennsylvania State University

Citation: Malware continues to be a challenge to computer security (2010, February 5) retrieved 24 April 2024 from https://phys.org/news/2010-02-malware.html