

Computer hacking proliferating with highly networked society, expert says

August 18 2011, By Xinming

Google, the International Monetary Fund and Sony represent major names in the world economy. But the three share another distinction -- recently disclosed attacks by computer hackers that have compromised sensitive information.

A Kansas State University computer security expert says the impact of hacking is increasing and evolving with technological advances.

Xinming "Simon" Ou, assistant professor of computing and [information sciences](#), attributes levels of Internet usage to the changed dynamics of computer hacking. The first large-scale Internet worm was released in 1988. The Morris worm essentially brought down the Internet, according to Ou. Considerable media attention accompanied the release though the techniques used by the worm had long been known. The increased usage of networks and computing in all aspects of life has turned hacking into a trophy-driven activity, Ou said.

"In the earlier days of hacking, talented hackers gained fame by creating clever exploits of [software vulnerabilities](#) resulting in viruses and worms that propagate rapidly through various media that often create large-scale impact in a short period of time," Ou said.

Recent targets show a new focus on profit-driven hacking. Profit-driven hacking occurs when computers are intruded for the purpose of monetization, according to Ou. Spam emails for advertisements are a common source of revenue for hackers. They also can scramble the data

stored on a hard disk and request a ransom to release the key to decrypt the data.

Other methods include tricking users into believing their computers are infected with malware and that purchasing an anti-malware program is necessary. BotNet -- a large number of zombie computers controlled by hackers who coordinate further attacks -- is the most pronounced hacking phenomenon today, Ou said.

Many valuable assets now have an online presence, and that helps hackers worldwide.

"Thanks to the rapid advancement of computing/networking power, the effects of successful hackings can generate large damage in a very short period of time," Ou said.

Corporate responses to successful hacking vary by the organization. In many instances external security firms are brought in to analyze the scope of the damage and to understand what happened. On a personal level, several preventive measures can be taken, Ou said.

* Always turn on your operating system and application's automatic update function. A better-patched system has fewer holes a hacker can utilize.

* Always turn on the firewall on your personal computer. Some operating systems do not turn on the firewall by default so you will have to do it the first thing after you take it out of the box before plugging it in to the network.

* Think twice before you click. Most hackings' first step is a user accidentally clicking a malicious link on a web page or email. If you are not sure of the true origin of the content, do not view it. Try not to open

a spam email in your email client or browser window. Just delete it directly if the title suggests it is obviously spam.

* Having an anti-malware product can help, although it can only capture a portion of the malware so do not think you are safe if you have one of those products installed.

Greater visibility has been afforded to computer hacking through the news media in recent cases, Ou said. Increased media interest and recent regulations and laws requiring companies to disclose data breaches to customers are the likely causes.

Successful [computer hackers](#) must have a deep and comprehensive understanding of computer and network systems, as well as strong coding and operating system capabilities, according to Ou. Skilled hackers are highly sought after by employers because of the emerging market in security solutions and consulting businesses.

Society's responses to [hacking](#) will determine the evolution of the issue, Ou said.

"Many problems are actually not technical but economical problems that can only be solved by providing the right incentives for the people best placed to improve security to take actions," Ou said.

Provided by Kansas State University

Citation: Computer hacking proliferating with highly networked society, expert says (2011, August 18) retrieved 20 April 2024 from <https://phys.org/news/2011-08-hacking-proliferating-highly-networked-society.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.