PHYS.ORG

Linux B-day celebrations rattled by break-in

September 4 2011, by Nancy Owano

(PhysOrg.com) -- Just days after celebrations marking the 20th birthday of Linux, the operating system revered around the globe as a rock-solid open source triumph, news surfaced that key servers used to maintain and distribute the operating system were hacked. Malware had gained root access. System software had been modified. The attack was confirmed in a note on Wednesday, August 28, posted on the Linux Kernel Archives www.kernel.org , the main distribution site for the Linux kernel. Though discovered on the 28th, the security breach possibly took place some time before, possibly no later than August 12. By Sunday, the 28th, it was obvious to admins of the web site that things had gone wrong. Files belonging to ssh (openssh, openssh-server and openssh-clients) were modified. A trojan startup file had been added to startup scripts.

The intruders initially gained root access on a server called hera, and compromising other servers. The administrators think they may have slipped in with a compromised user account. In an e-mail to kernel.org users, chief administrator John "Warthog" Hawley indicated he was definitely not in a party mood. The subject line: *Master back-end break-in*. "Afternoon everyone," he wrote,"as you can guess from the subject line, I've not had what many would consider a 'good' day." He said that a trojan had been discovered and he named "some boxes" on kernel.org that had been hit.

With the news of such a break-in, it might easily appear as if the event spells calamity, as this is all about a break-in of a repository hosting site of source code, and for an operating system that runs the engines of banks, businesses, and governments. What could be worse news than this? In fact, Linux being Linux signifies that the August break-in, while unwelcome, rattling, and burdensome, appears to have also given Linux keepers the opportunity to remind the world that its construct has built-in safeguards.

The strength of Linux, admins quickly pointed out, lies in its change-tracking system, where a secure hash of each of 40,000 files hosted on the site makes signs of tampering transparent. The hashes are stored in multiple servers. On confirmation of the break-in on the 28th, each of the site's 448 users were told to change their passwords and Secure Shell keys. Boxes were promptly taken off-line and re-installs were set in motion. Authorities in the U.S. and Europe were notified and asked to help in the investigation.

Source code does not appear to have been altered, according to the kernel maintainers, but the posting stated the administrators were doing an analysis to confirm that nothing has been modified.

More information: www.kernel.org/

Citation: Linux B-day celebrations rattled by break-in (2011, September 4) retrieved 18 April 2024 from https://phys.org/news/2011-09-linux-b-day-celebrations-rattled-break-in.html