

Re: Worm forcing reboots.

## Re: Worm forcing reboots.

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.misc/2008-03/msg00027.html>

---

- *From:* "[shrike@xxxxxxxxxxxxxxxx](mailto:shrike@xxxxxxxxxxxxxxxx)" <[shrike@xxxxxxxxxxxxxxxx](mailto:shrike@xxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 21 Mar 2008 18:42:35 -0700 (PDT)
- 

On Mar 21, 12:58 pm, Unruh <[unruh-s...@xxxxxxxxxxxxxxxx](mailto:unruh-s...@xxxxxxxxxxxxxxxx)> wrote:

"[shr...@xxxxxxxxxxxxxxxx](mailto:shr...@xxxxxxxxxxxxxxxx)" <[shr...@xxxxxxxxxxxxxxxx](mailto:shr...@xxxxxxxxxxxxxxxx)> writes:

Howdy,

I happened to notice several Win32 boxen, spontaneously have problems with the shift key. When rebooted all installed automatic updates and the problem went away. Basically the shift key functioned in reverse making typing irritating.

Somebody hit the caps lock key. Hit it again and the typing will be back to normal.  
No reboot needed.

It occurred to me that this would be an effective way to force a reboot and subsequent installation of a root kit without drawing a lot of attention.  
Anybody else experience this? Does this fit the profile you know of?

And they say security people have no sense of humor...

No, the capslock function is reversed, and it effects punctuation as well as characters. It shows up like a driver bug or something, but since I've experienced it across multiple hardware/software versions that seems unlikely.

I run a fairly fascist security policy and periodically analyze snapshots of traffic with Ethereal. Every time I get an automated update I'm wondering whether it is legit or not. I've disabled about half the services windows runs by default, renamed crap that periodically gets turned back on by microsoft updates (without my permission). I try to insure my box only runs only what I want it to run. I understand the concept of a user actually configuring a machine is fairly alien in the Win32 world, but there it is.

I chose to run Cygwin to get most of my Unix tools. It isn't a

Re: Worm forcing reboots.

Re: Worm forcing reboots.

complete replacement for Linux, but it is easier than hauling around a second box. It is also pickier than Linux. If something builds with gcc on cygwin compiling on linux is easy.

My point here, is that I'm not a noob. There is some flaky code here. If I wanted to force a reboot quietly, I would make it look like a typical windows bug. If I wanted to relay data, I would encap it in HTTP, or DNS traffic so it would be innocuous to the average firewall. So when I see something that looks hank