

Re: Can't update running process binary in Solaris?

Source: <http://unix.derkeiler.com/Newsgroups/comp.unix.programmer/2007-07/msg00532.html>

- *From:* James Carlson <james.d.carlson@xxxxxxx>
 - *Date:* 27 Jul 2007 09:00:21 -0400
-

Eric Sosman <esosman@xxxxxxxxxxxxxxxxxxxxxxxx> writes:

You may also run afoul of a feature of present-day Solaris: it can verify the digitally-signed checksum of an executable file or library before permitting it to run. The verification is optional, by default, but can be made mandatory for specific user accounts if the sysadmin is security-conscious. Usage of this

In addition to that, there's pkgchk, bart, tripwire, and any number of intrusion-detection systems. This modified binary will stand out like a sore thumb if the administrator tries to verify that his system hasn't been tampered with.

That's essentially what it sounds like the original poster will be accomplishing -- making the system appear to have been tampered with. Sane administrators will wipe the damaged binary from the system and perhaps restore everything from backup at that point.

I'm sure the objection to this will be something like, "but our documentation says that we do this!" So what? It doesn't scale. Maybe I could put up with having one or two binaries on the system that are known to mutate over time. I don't think I could stand it if there were dozens or hundreds of them. Is this application really so special that the user will never want to install another bit?

feature does not seem to be widespread as yet, but as malware continues to spread it would not surprise me to find verification enabled at more and more sites. And since your self-modifying executable cannot maintain a constant checksum, you will find no customers, nor even any trial users, at those sites ...

As with many schemes that appear to assume customers are crooks, it sounds like a self-solving problem to me. ;-}

Re: Can't undate running process binary in Solaris?

James Carlson, Solaris Networking <james.d.carlson@xxxxxxx>
Sun Microsystems / 1 Network Drive 71.232W Vox +1 781 442 2084
MS UBUR02-212 / Burlington MA 01803-2757 42.496N Fax +1 781 442 1677