

## Re: Trojan ByteVerify Question

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.misc/2007-12/msg00010.html>

---

- *From:* "Sebastian G." <[seppi@xxxxxxxxxx](mailto:seppi@xxxxxxxxxx)>
  - *Date:* Mon, 10 Dec 2007 19:55:02 +0100
- 

george wrote:

Hm? ByteVerify is an exploit for the class format verifier of the Java ClassLoader of super old Sun JavaVM 1.2.4.

That's exactly unhelpful response you could find on Symmantec, but what does byteverify do to your machine?

If you're running Sun's Java VM 1.2.4 or older: it will allow the attacker to execute arbitrary code, which will do about virtually anything.

If you're not so horribly stupid and run a newer version of Sun's JavaVM, a Java VM of another vendor, or simply none at all, the exploit fails and doesn't execute anything malicious. Thus, nothing happens.

It's really a wonder that such super-old exploits are still in use.

.