Comodo has confirmed that two other resellers have been compromised since the "Comodogate" attacks which saw an attacker generate forged certificates for login.live.com, mail.google.com, www.google.com, login.yahoo.com, login.skype.com and addons.mozilla.org. According to Comodo's CTO, Robin Alden, no further certificates were issued as a result of these compromises at the two RAs (Registration Authorities). The disclosure will do little to reduce the worry that other forged certificates could be in circulation.

Alden was responding to queries in the mozilla.dev.security.policy Usenet group. He also confirmed that Comodo was reinstating a "high value target check" on all certificate orders noting that "regrettably it had been disabled for a small number of RA accounts" and that the company was "removing the aspects of our back-end system that allow this check to be optional".

The company had assumed that the threat would come from an RA which was not performing validation properly or avoiding doing validation. Alden says the RA in this case was carrying out those duties correctly. He says that the underlying problem was that "what we had not done was adequately consider the new (to us) threat model of the RA being the subject of a targeted attack and entirely compromised".

Source: H-Online.com