

## Anti-hacking firm RSA gets hacked

by Lawrence Latif via reed - The Inquirer *Friday, Mar 18 2011, 8:06am*

international / mass media / commentary

### Hunter turns into the hunted

*It seems the elite (anonymous) hacker underground is targeting IT Corporates and teaching them a lesson in SKILL and STRATEGY. [A widely known fact in the hacker community but little known in the general community, is that Corporatists are only able to enlist 5th rate hackers/security staff, as elite crewz and skilled hackers possess ideological integrity and would never assist the enemy. Also, elite hackers cannot be tempted with toilet paper dollars, as money is no problem for hackers - LOL!]*

*The USAF was actually reduced to advertising for hackers in the mass media, how revealing and embarrassing, hilarious!*

*The attack on EMC/RSA was a classic co-operative assault by elite teams, few are able to initially defend against or withstand such attacks -- have you read Dickens, my Lovelies? Seems like the 'artful hacker' and his crew have been busy and methinks it's only the beginning.*

*Never forget, suckers, we own the wire; we took it before you lamers were even aware it was a battlezone. You are light years behind -- have a nice LAME day; game over (before it's begun!)*

**SECURITY VENDOR** RSA admitted that its internal anti-hacking technologies have been hacked.

Parent company EMC, which is one of the largest enterprise storage vendors, stated in a Securities and Exchange Commission (SEC) filing that its RSA division was the victim of an "advanced persistent threat", which the Associated Press claims is "industry jargon for a sophisticated computer attack".

EMC did not divulge details of the attack, however it did say it discovered an "extremely sophisticated" attack against its networks with attackers making off with confidential data on RSA's SecurID products.

In the SEC filing by EMC, RSA said that it is "confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers". Nevertheless, the company warned that "this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack".

For EMC, the RSA break-in and theft is deeply [embarrassing](#), as RSA is one of the best known security vendors in the market. Many large firms, government organisations and medical organisations use RSA's two-factor authentication software for access control.

The procedure generates a passcode using a secondary device, meaning that if the user's password is compromised, access will not be granted without the device generated passcode. The fear is that hackers got hold of the algorithms used to generate the

passcodes.

For its part, RSA was quick to say that it was taking "immediate remediation steps" for its customers.

EMC hopes that the fall-out from this attack will be limited and said the RSA break-in won't have an affect on its financial results.

While EMC might not be expecting any financial blowback, its customers must be eager to find out whether and how badly their RSA based security might have been compromised.

Copyright applies to external article.

<http://www.theinquirer.net/inquirer/news/2035368/anti-hacking-firm-rsa-hacked>

---

Cleaves Alternative News. <http://cleaves.lingama.net/news/story-2392.html>