By John Leyden, TheRegister.co.uk

Cybercrooks are offering hacked domains, including military sites, for sale through underground marketplaces.

Government, defence (.mil) and education sites in the US and Europe are on offer to interested parties from anywhere between $55 and $499 each. The hacker is selling admin login credentials to hacked sites as well as looted personal data from compromised sites, yours for $20 per 1K records.

Database security firm Imperva, which issued an advisory late last week after coming across the illicit trade, reckons SQL injection vulnerabilities are the root cause of the security problems affecting the sites up for sale. It reckons the miscreant behind the sale used a scanner to search for vulnerabilities he knew how to exploit using automated tools.

Such a scenario is credible but by no means proven. Screenshots posted by the hacker show access to the admin interface for the University of Connecticut in a bid to substantiate claims that staff members' details are up for sale.

However the list of domains on offer includes several typos, which raises doubts about whether what is on offer is the real deal or a scam directed at fleecing cybercrooks themselves.

Underground sites more commonly offer access to networks of compromised machines or stolen credit card information. The offer to sell access to compromised websites is unusual, suggesting a further diversification of the goods on offer via black market outlets.

Imperva's advisory on the illicit trades, complete with screenshots, can be found here .