Service Sells Access to Fortune 500 Firms

Published: 2012-10-22 · Archived: 2026-04-05 21:13:45 UTC

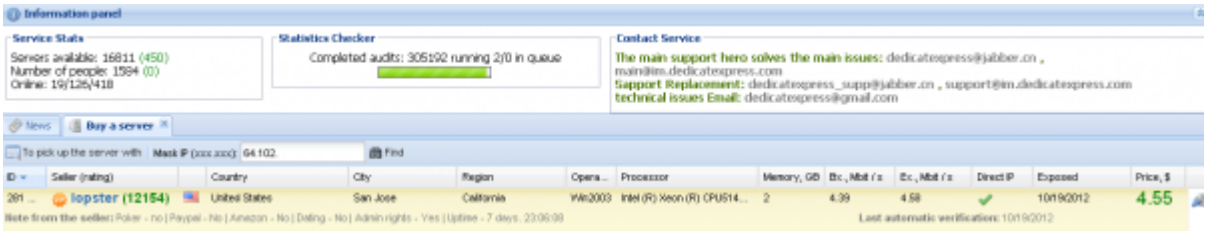
An increasing number of services offered in the cybercrime underground allow miscreants to purchase access to hacked computers at specific organizations. For just a few dollars, these services offer the ability to buy your way inside of Fortune 500 company networks.

The service I examined for this post currently is renting access to nearly 17,000 computers worldwide, although almost 300,000 compromised systems have passed through this service since its inception in early 2010. All of the machines for sale have been set up by their legitimate owners to accept incoming connections via the Internet, using the Remote Desktop Protocol (RDP), a service built into Microsoft Windows machines that gives the user graphical access to the host PC's desktop. Businesses often turn on RDP for server and desktop systems that they wish to use remotely, but if they do so using a username and password that is easily guessed, those systems will soon wind up for sale on services like this one.

Pitching its wares with the slogan, "The whole world in one service," **Dedicatexpress.com** advertises hacked RDP servers on several cybercrime forums. Access is granted to new customers who contact the service's owner via instant message and pay a $20 registration fee via WebMoney, a virtual currency. The price of any hacked server is calculated based on several qualities, including the speed of its processor and the number of processor cores, the machine's download and upload speeds, and the length of time that the hacked RDP server has been continuously available online (its "uptime").

Though it is not marketed this way, the service allows users to search for hacked RDP servers by entering an Internet address range, an option that comes in handy if you are looking for computers inside of specific organizations. For instance, I relied on a list of the IP address ranges assigned to the companies in the current Fortune 500 listing (special thanks to online banking security vendor Greenway Solutions for their help on this front).

I made it about halfway through the list of companies in the Fortune 100 with names beginning in "C" when I found a hit: A hacked RDP server at Internet address space assigned to networking giant **Cisco Systems Inc.** The machine was a Windows Server 2003 system in San Jose, Calif., being sold for $4.55 (see screenshot below). You'll never guess the credentials assigned to this box: Username: "Cisco,"; password: "Cisco". Small wonder that it was available for sale via this service. A contact at Cisco's security team confirmed that the hacked RDP server was inside of Cisco's network; the source said that it was a "bad lab machine," but declined to offer more details.



A hacked Win 2003 Server installation at Cisco Systems was on sale for $4.55.

Dedicatexpress works directly with hackers who earn commissions for selling the RDP machines to the service (see screenshot below). The number beside each seller's name indicates how many servers he has sold to dedicatexpress.com. The service says it will not buy RDP servers from Russia, probably because its proprietors are from that country and do not wish to antagonize Russian law enforcement officials (the site is in Russian but the images pictured here are from Google-translated versions of the pages).

Top vendors of hacked RDP servers.

Sellers can specify how the servers that they contribute may be used, and very often state that their RDP servers may not be used for particular activities, such as online gambling, PayPal or dating scams. Buyers may also be limited to running regular user accounts on the hacked systems, barring them from installing many types of software (the Cisco server sold above granted the buyer administrative rights).

Before a server can be purchased, the service prompts buyers to use its built-in system for checking the reputation of the hacked RDP installation. I ran a check on the Cisco box and found that it had already been blacklisted by 10 out of 15 popular services that track malicious activity online, such as spam and malware hosting. Not to worry, though: The service's operators assure buyers that "if you have any problems with the remote server you have just purchased, you will always be able to file a ticket with technical support and we will be happy to assist you."
