SNWOnline
A VIRTUAL CONFERENCE
Tools and techniques for working with storage.
LIVE ONLINE EVENT: February 27, 2008, 11 am – 6 pm EST
REGISTER NOW for this free, 100% online event

COMPUTERWORLD
Security

Russian hosting network running a protection racket, researcher says

Gregg Keizer

February 19, 2008 (Computerworld) The Russian Business Network, a notorious hacker and malware hosting network, runs a protection racket that extorts as much as $2,000 a month in fees for "protective Web services" from borderline sites, a researcher alleged today.

The RBNExploit blog -- which is authored by one or more anonymous researchers -- spelled out the racket run by the group, which is thought to be headquartered in St. Petersburg, Russia, and has been pegged by security professionals as a major source of malware and cybercriminal activity.

"The business model RBN uses is quite simple and effective," said a post published today on the blog. "Its affiliates and resellers comb various niche market forums and discussion areas for Web masters using or discussing protective web services, i.e. DDoS [Distributed Denial of Service] prevention. Carry out a DDoS attack on the Web site and then provide a third-party sales approach to the Web master to 'encourage' a sign-up for their DDoS prevention services."

The price for "protection:" $2,000 per month.

The DDoS attacks are, like almost all such mass attacks, conducted by a botnet, an army of previously-compromised computers that can be told to hammer a site one day and spew huge quantities of spam the next. Numerous researchers, for example, have linked the RBN to the Storm botnet, an amorphous collection of PCs that have been infected with a Trojan by the same name. Some security experts have put the blame for a massive series of DDoS attacks against Estonian government sites last year on the RBN.

RBNExploit noted that the domains that have recently shifted to RBN's hosting services included sites involved in pornography, online pharmaceutical sales and what it calls "HYIP," for High Yield Investment Programs -- a term that's become synonymous with investment scams, often in the form of traditional Ponzi schemes. "RBN is successful, as most of these Web masters are not about to publically complain," noted the blog.

It also posted a link to an HYIP forum where discussions of RBN DDoS extortions appeared several times. "Paid very fast. A very good return from a ddos attack," wrote one users on the scam's message board in early December 2007.

"Very good support work while ddos!" added another. "I am very happy with your fast payments! THx!"

The blog traced the anti-DDoS hosting services to an IP address it had previously fingered as a "core replacement server" for RBN in St. Petersburg. It also listed several domains, including the HYIP "Golden Pig" and several drug-selling sites, that have recently moved to the RBN servers handling anti-attack hosting. Among the latter: TheCanadianMeds.com and OfficialMedicines.com. Both those sites are now hosted on RBN servers based in Turkey, said the blog, and they have previously been blacklisted by SpamHaus.org, a well-known antispam organization.

Phone numbers listed in the domain registration records for those sites were either incomplete, and thus unusable, or rang through to a fax machine.