

RBN - 76service, Gozi, HangUp Team, and US hosting

The recent detailed and fascinating reports within CIO written by By Scott Berinato in conjunction with SecureWorks researcher Don Jackson was focused on the technical analysis of form-grabbing software, via access to 76service (dot)com. Subscribers to 76 service could log in, pull down the latest drops, i.e. data deposits from the Gozi-infected machines they subscribed to sent to the servers, like the 3.3 GB one Jackson had found containing more than 10,000 online credentials (ID theft) taken from 5,200 PCs.

Within the analysis and articles there is reasonable logic as to the 76service servers being based in Panama, but unfortunately they are or were based within the US. The Mpack DIY exploit package involving the "HangUp Team" which Jackson had found a coder who posted the news of 76service's demise, all of these players have connections to the Russian Business Network (RBN), according to several researchers, including Jackson, ref: CIO.

In a long term watch analysis of DNS for 76service (dot) com (66.232.122.239) and related, reveals a detailed hosting history and CBL / SBL blacklisting (see below), but apparently is still currently hosted by "coolservecorp (dot) net" i.e. Noc4hosts Inc, with their servers stated as being in Lykes Building, Tampa, FL, USA. Although 76service appears closed, they may still be dwelling the hive of associated domains i.e. Key related domains @ 66.232.122.239 - carbon coolservecorp net: 76service.com, gamesboard.ru, newpulses.com, odeku.net, putany.net, sosnovsky.net (see below for further domains for interested researchers).

This is similar to another RBN retail outfit "iFrame Cash", where hosting was shown until recently by another US based web host Layered Technologies. The "carbon coolservecorp net" server is not the only one involved also; host33.coolservecorp.net, and aa.18.1343.static.theplanet.com.

Any reasonable conclusion again asks the question; are the RBN's "bullet proof" servers operating with apparent impunity from within large low cost shared and dedicated hosting services within the US at coolservecorp / Noc4Hosts, Global Net Access (GNAX), The Planet or similar?

Even more concerning is the fact that there are reports of website hacking, iFrame exploits and hijacking at these hosts, not quite reported yet on the scale of the recent iPower (10,000+ sites exploited) problem but significant and growing. However the potential "internal" target for the RBN here is staggering, if correlating the potentially "infectable" IP domains from AS29802, AS3595, and AS29802 is a total of 1,296,640 IP addresses.

For the authors here, this analysis similarly proves the color of the credit card is more important than any due diligence concerning the activities of the client webmaster to most hosting outfits. Perhaps when hacked webmasters or those individuals who have been subject to ID theft eventually sue the hosts responsible for housing the cause, perhaps some due diligence may ensue.

The final conclusion is it would appear the RBN does not have to hack into servers to gain access to websites and a major hosts legitimate customers, they are already inside.

(Authors note: thanks to Scott Berinato, Don Jackson, and CIO for publishing the core information.)

Specific details:

BAD Listed on : 2 dnsbl services:

66.232.122.239 YES - LISTED BY cbl.abuseat.org

66.232.122.239 YES - LISTED BY t1.dnsbl.net.au

Further potentially related domains:

76 service domains sharing nameservers

5ballov.net, adulthosting.ru, alnar.net, alt.by, anemia-working-group.net, anemia-working-groups.net, anemiaworkinggroup.net, anemiaworkinggroup.net, anonymous-service.com, apps4.net, aspmedia.net, azgar.by, beldrug.org, belpatent.net, belreferatov.net, beltorg.com, bvf.by

carbon.coolservecorp.net

charadziej.org, chukov.net, contour-lamn.com, coolservecorp.net, coolwebserve.net, daugiasaigon.net, fromby.net, gamesboard.ru, glamoura.net, gomeloboi.com, goro.by, greentrans.net, hope-casadue.net

host33.coolservecorp.net

iiseys.org, jewelry-fashion.net, k6tv.com, krimea.net, lysandrasoft.com, magomedov.net, maltofer.ru, medprom.com, multydom.crimea.ua, newpulses.com, odeku.net, pegasas.net, pogotski.com, priceby.net, priceru.net, priceua.net, putany.net, respekt-plus.com, sexbomba.ru, shemalesru.net, sit93.com, sosnovsky.net, syabry.com, venofer.ru, vodkaescort.com, wdl.ru, webmoney-hosting.net, znaesh.net

AS29802

Number of unique AS-peers:1 - Number of prefixes:7 -Number of ip numbers:28,928

AS3595 AS GNAXNET AS Global Net Access

Number of unique AS-peers:7 - Number of prefixes:35 -Number of ip numbers:145,920

AS21844 THEPLANET AS2 ThePlanet com

Number of unique AS-peers:5 -Number of prefixes:22 - Number of ip numbers:1,121,792

Total = 1,296,640