

RBN - Hijacking via Banner-Ads on Major Web Portals

The Russian Business Network (RBN) in one of its boldest PC hijacking exploits used conventional banner-ads to redirect web visitors to "fake" anti-spyware sites, this is a new attack vector but uses known RBN server routes and exploits. Malware based ads have been spotted on various legitimate websites, ranging from baseball's MLB.com, NHL.com, Canada.com and The Economist. Acting as a conventional Flash file, the exploit is via DoubleClick's DART program, DoubleClick acknowledges the malware, and says it has implemented a new security-monitoring system that has thus far captured and disabled a hundred ads.

How the exploit works, servers and locations (confirm Explabs):

Example for mlb.com ... mlb.com - to - ad.doubleclick.net - to - newbieadguide.com - to - fixthemnow.com - this calls to safetydownload.com for the "fake" download

Example for nhl.com ... nhl.com - to - 2mdn.net - to - ad.doubleclick.net - to - adtraff.com - to - blessedads.com and prevedmarketing.com - to - malware-scan.com, for the "fake" download.

Figure 3 - Secure Hosting Bahamas

As shown above the key servers involved in particular Secure Hosting based in The Bahamas has been utilized on other occasions by RBN. It should also be noted the four specific exploit servers and their AS (Autonomous Server) are:

* AS15146 Cable Bahamas Ltd. (also AS26855 INTERNET BAHAMAS) - SECUREHOST.COM - IP range involved - 190.15.72.0/21

* AS29131 RAPIDSWITCH Ltd - London UK - IP range involved - 87.117.192.0/18

* AS33510 SETUPAHOST - Toronto Canada - IP range involved - 66.244.254.0/24

* AS41947 WEBALTA / Internet Search Company - Moscow Russia - IP range involved - 77.91.224.0/21

Each of these servers houses many other questionable and other exploit based domains within the same specific IP as those specific domains utilized within this PC hijack exploit, figure 4 – shows those domains which include 23 domains as “fake” anti-spyware or rogue software based upon the same RBN exploits as “Winfixer”, “SpySheriff”, etc.

This important exposure is thanks to excellent CYBERINT work within the community, references:

Explabs - Wired.com - Sunbelt