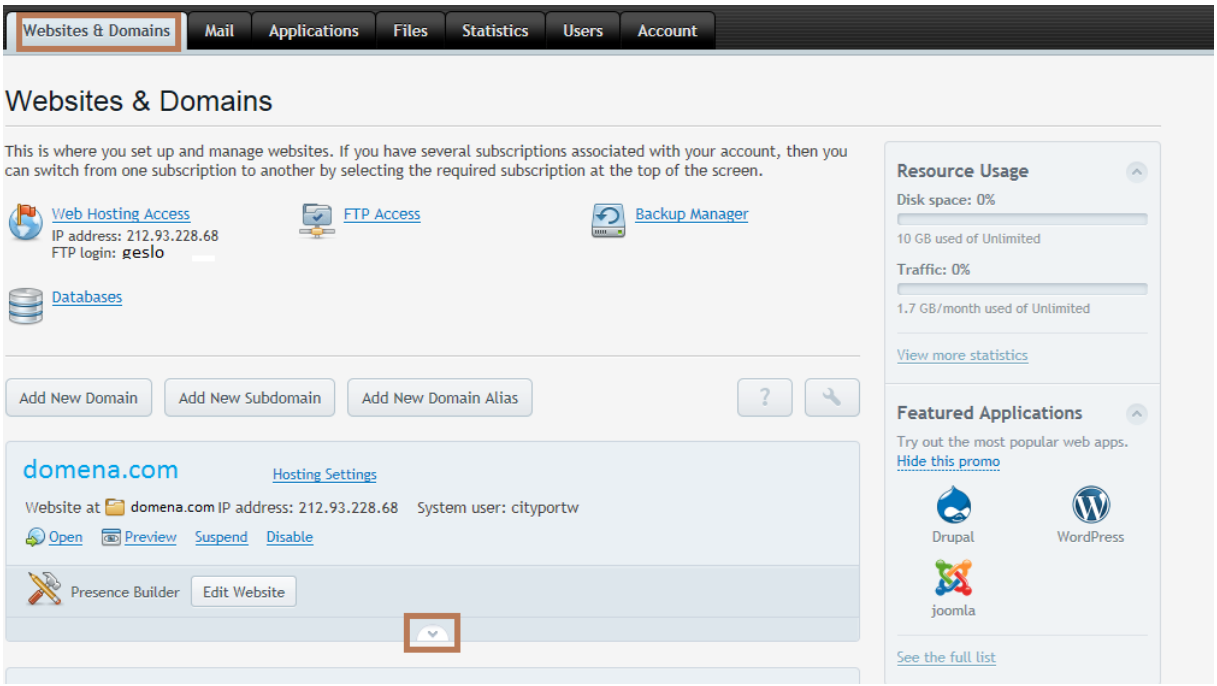
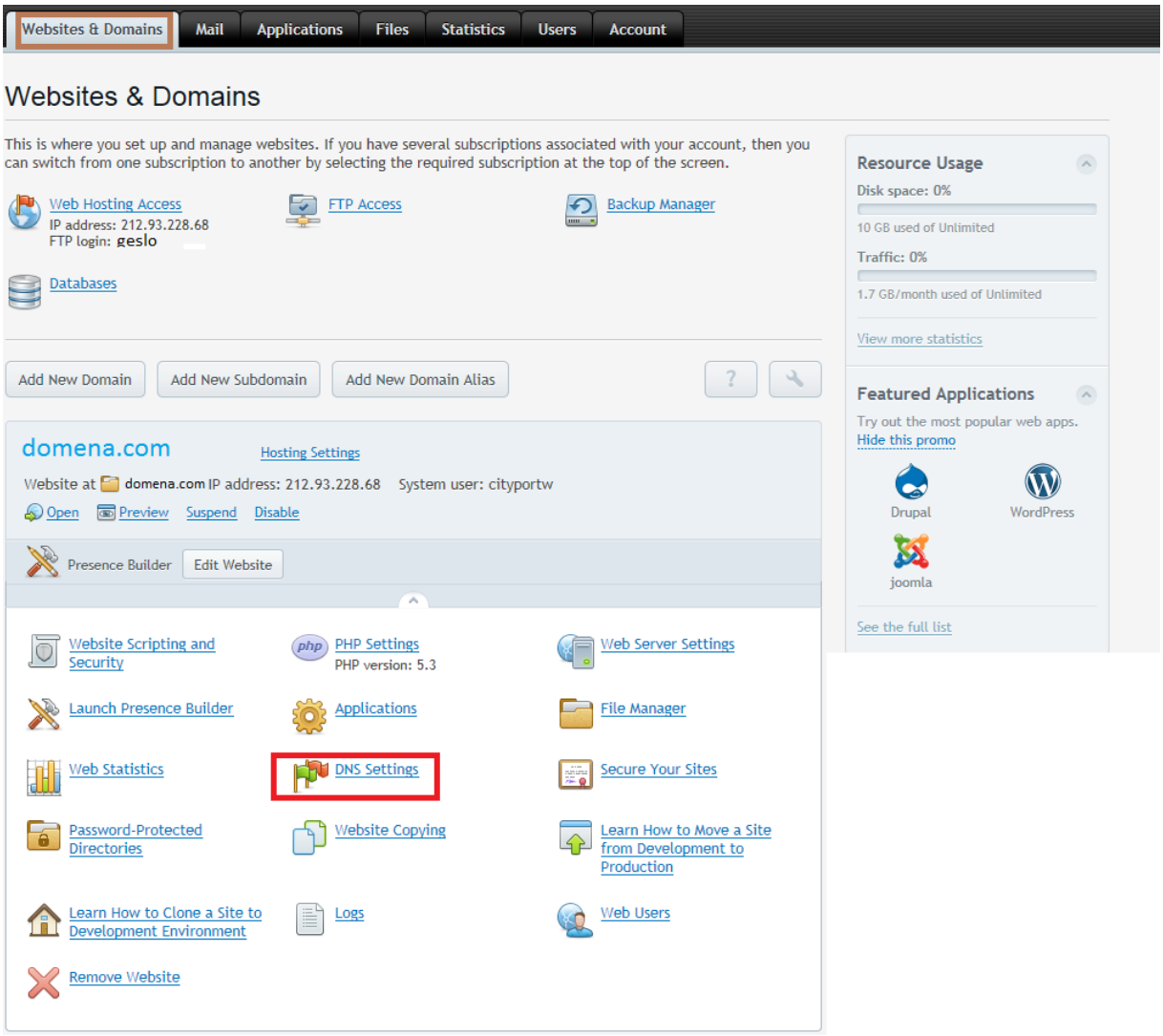
**Kako spremenim DNS zapise za mojo domeno?**

Za spremembo DNS zapisov za vašo domeno se morate prijaviti z uproabniškim imenom in geslom za administracijo vaše domene na naslov https://pleskb.mojk2.net:8443/.

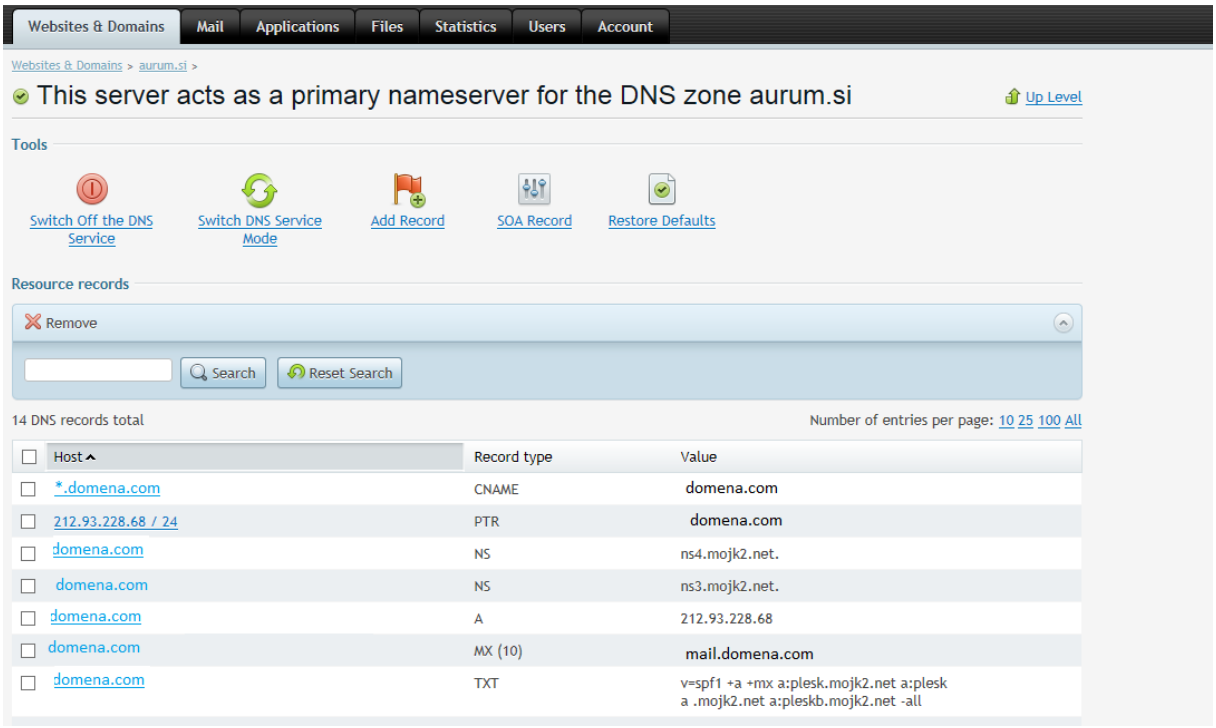
Ko ste na nadzorni plošči, kliknite na Websites&Domains, odpre se vam okno (primer spodaj).




Če se vam odpre okno podobnemu zgoraj, pritisnite na puščico na spodnjem robu, da se vam prikažejo dodatni meniji za nastavitve.




Izberite DNS Settings. Prikažejo se vam nastavitve za vpis DNS zapisov.




Spletni portali CMS (Joomla, Drupal, Wordpress ipd.) pa tudi druge spletne aplikacije se pogosto uporabljajo kot tarča hekerskih napadov in zlonamernih skript. Okužite se lahko tudi samo z obiskom okužene spletne strani, ki izkoristi luknje v programski opremi vašega brskalnika (flash, pdf, brskalnik ...). Hekerji poznajo luknje v programih in skriptah in preko njih običajno namestijo zlonamerno kodo na vašo spletno stran oz. računalnik. Avtorji aplikacij redno izdajajo popravke za luknje (napake) v kodi, vendar pa jih uporabniki ponavadi redko nameščajo -- ali pa jih sploh ne. V primeru, da brskalnik zazna tak primer zlonamerne kode na spletni strani, opozori, da je stran sumljiva in dostop do nje onemogoči. Opozorilo se pojavlja toliko časa, dokler se zlonamerne kode ne odstrani.

Vsi Ciyport strežniki imajo nameščene aplikacije, ki preprečujejo ali zmanjšujejo možnost vdorov na strežnik. Vendar **pa ni možno preprečiti spreminjanja vaše spletne strani, če ima vaša spletna aplikacija luknjo v skripti (bug).**

Rešitev za omenjen problem je sprotno nameščanje popravkov oz. zadnjih verzij vaše spletne in PC aplikacije ter ustrezne nastavitve. Če se vam je primer zgodil, najprej odstranite zlonamerno kodo in nato nadgradite portal oz. zaščitite spletno stran.

Okvirni postopek odstranjevanja je sledeč:
- najprej spremenite vsa gesla za dostop do upravljanja z gostovanjem (predvsem pa FTP dostop)
- to uredite z računalnika, ki je zagotovo dobro zaščiten in neokužen.
- prijavite se preko FTP dostopa in poiščete sumljive datoteke in si zabeležite datume teh datotek
- datoteke lahko prenesete na lokalni računalnik in odprete urejevalniku besedila in poskusite ugotoviti kaj datoteke izvajajo, kar je lahko v pomoč
- nato se prijavite na plesk kontrolno ploščo in preverite LOG (dnevnike) datoteke
  Iščete vzorec ob uri, ko so bile datoteke nameščene/spremenjene, kar ste ugotovil preko FTP dostopa
- ko ugotovite, preko česa so vam dostopali do vašega gostovanja, vzrok odpravite (nadgradite portal, dodatke, zaščitite mape ...) in počistite zlonamerno kodo.

V pomoč pri preverjanju je lahko http://www.google.com/webmasters/tools, kar pomaga tudi pri hitrejšem odpravljanju opozorila v brskalniku.

Vse to urejate z računalnika, ki ima urejeno in posodobljeno antivirusno zaščito.

Če uporabnik ne ukrepa in ne odpravi napake, Lahko Ciyport onemogoči dostop do spletne strani z geslom. V primeru da se zadeva ponavlja, lahko spletno stran ukinemo zaradi kršenja Splošnih pogojev gostovanja.