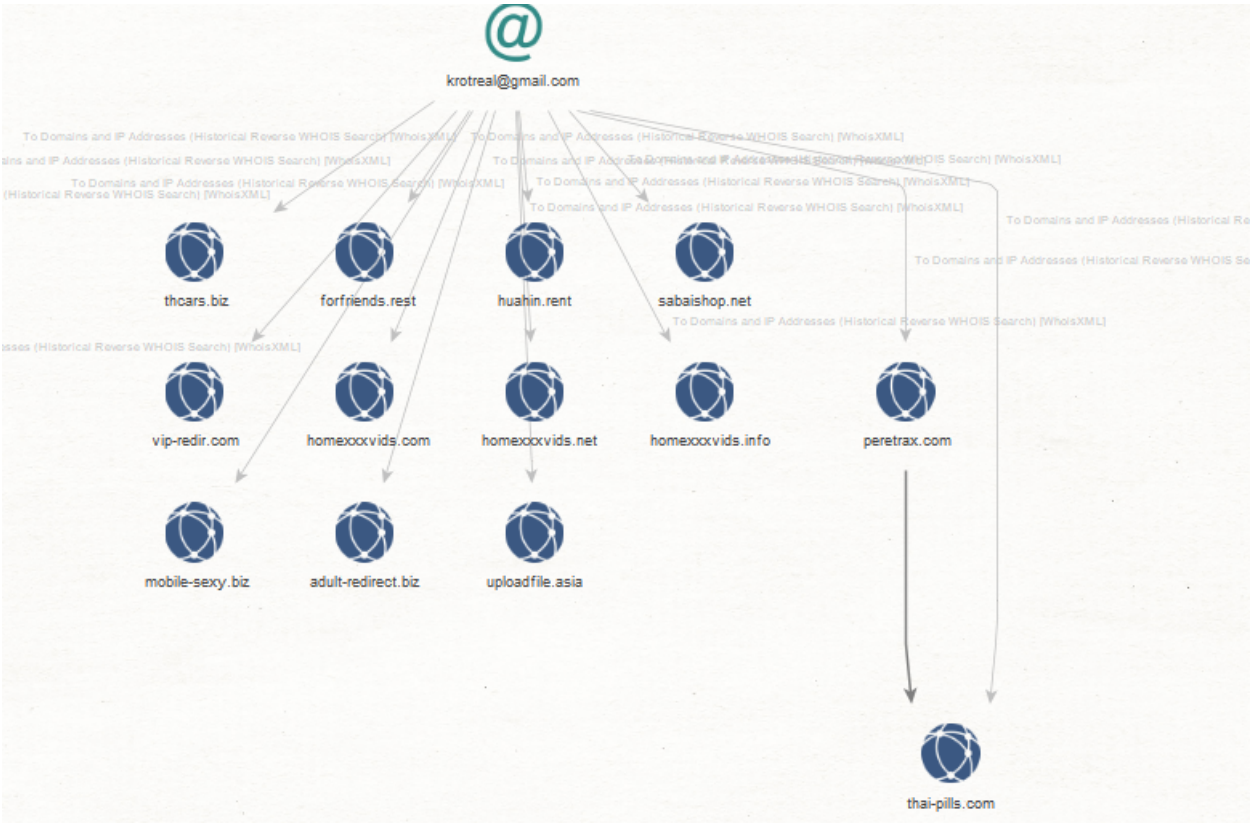
Is Koobface Botnet's Master KrotReal Back in Business? Try the Adult Entertainment Industry First!



Dancho Danchev decided to dig a little bit deeper into Koobface's Botnet Master KrotReal using his own techniques and methodology and actually attempt to find additional information on KrotReal's online whereabouts as of 2022 in terms of malicious and fraudulent activities. He found evidence of several new domain registrations using the original krotreal@gmail.com personal email which Danchev originally profiled and exposed in his original OSINT analysis back in 2012.

Sample domains known to have been involved in the campaign include:

hxxp://mob-vids.com

hxxp://mob-dating.net

hxxp://xerotic-mob.com

hxxp://kinozal3d.com

hxxp://xmob-erotic.com

hxxp://uploadfile.asia

hxxp://mljsprivate.biz

hxxp://xmusic-mp3.com

hxxp://tube4mob.com

hxxp://mob-ka-next.com

hxxp://mobcelebrity.net

hxxp://mobcelebrity.org

hxxp://mob-dating.com

hxxp://mob-dating.org

hxxp://forfriends.rest

hxxp://xxxfreewebcams.com

hxxp://huahin.rent

hxxp://vrwebcam.site

hxxp://peretrax.com

hxxp://thcars.biz

hxxp://mobile-sexy.biz

hxxp://adult-redirect.biz

hxxp://homexxxvids.net

hxxp://homexxxvids.info

hxxp://vip-redir.com

hxxp://homexxxvids.com

hxxp://sabaishop.net

hxxp://holopoker.online

hxxp://thai-pills.com

hxxp://searches.online

hxxp://android-igru.biz

hxxp://rusx.mobi

hxxp://horomob.org

hxxp://erotic-mobile.com

hxxp://horomob.com

hxxp://horomob.net

hxxp://mob-ka.com

hxxp://salosbros.com

hxxp://horomob.biz

hxxp://mtswapservice.com

hxxp://online-kinoteatr.biz

hxxp://mobile-vista.org

hxxp://mp3prosto.com

hxxp://prostofiles.com

hxxp://eromfpre.com

hxxp://x-onlinekino.com

hxxp://z-erovideo.com

hxxp://z-kinozal3d.com

hxxp://getgdz.net

hxxp://v2mlcelery.com

hxxp://good-erotic.org

hxxp://nice-erotic.org

hxxp://super-erotic.org

hxxp://amazing-erotic.org

hxxp://perfect-erotic.org

hxxp://cool-erotic.org

Sample personal email address accounts known to have been involved in the campaign:

arkano@arkano.ru

contact@biddx.com

tinnakorn_khu@hotmail.com

mrpinkesq@yahoo.com

krotreal@gmail.com

inf@outlook.co.th

2@2220.com

We'll continue monitoring the campaign and post updates as soon as new developments take place.