# Exomind

Exomind is a tool designed to deliver targeted phishing attacks through social networks. In order to do this we must first retrieve information from them in an OSINT fashion, this information is then used to impersonate key individuals whose fake online profiles can be used as the delivery medium for links into handcrafted webpages.

From the Corelabs site:

The most sophisticated attack that we have implemented so far is a sub-network replication attack, this means we are not only impersonating one individual, but also creating fake profiles for a big-enough part of his subnetwork. This lets us detach from profiles of real people who may perceive the attack, and also gives us more control on the topology of the network. # gutes is our attack target gutes = Graph.TwitterProfile("<http://twitter.com/gutes>")

# exomind is the user that will impersonate gutes. # cloneProfile clones the look and feel (theme, image, colors, etc...) exomind = Graph.ControlledTwitterProfile("<http://twitter.com/exomindtest1>", "password") exomind.cloneProfile(gutes)

# Test cloneFollowingStealth # We first instantiate the bots for the profiles Exomind controls exoclone = Graph.ControlledTwitterProfile("<http://twitter.com/exomindclone>", "password") exoclone1 = Graph.ControlledTwitterProfile("<http://twitter.com/exomindclone1>", "password") exoclone2 = Graph.ControlledTwitterProfile("<http://twitter.com/exomindclone2>", "password") exoclone3 = Graph.ControlledTwitterProfile("<http://twitter.com/exomindclone3>", "password") exoclone4 = Graph.ControlledTwitterProfile("<http://twitter.com/exomindclone4>", "password") exoclone5 = Graph.ControlledTwitterProfile("<http://twitter.com/exomindclone5>", "password")

#  Then for each user of the real sub-network we want to clone and follow, a bot # is assigned to that user. That can be done using the id or the screen-name of # the target user. followersTest = { 17157238 : exoclone, "axelbrz":exoclone1,                  "MarioVilas":exoclone2, "eglinsky":exoclone3,                  "tutterr":exoclone4, "whead":exoclone5,} exomind.cloneFollowingStealth(gutes, followersTest)

http://static.typepad.com/.shared:v03b8f01:typepad:en_us/tiny_mce/3.5.10/themes/advanced/img/trans.gif

**Warranty Disclaimer:** The FBI, InfraGard, and its affiliates provide information, including but not limited to software, documentation, training, and other guidance to be known as “materials”. The materials are provided as-is and we expressly disclaim any and all warranties, express or implied, including, and without limitation, the implied warranties of merchantability, fitness for a particular purpose, non-infringement, quiet enjoyment, and integration, and warranties arising out of course of dealing or usage of trade. You agree that, as between you and the FBI, InfraGard, and its affiliates, you are responsible for the outcome of the use of materials made available, including but not limited to adherence to licensing requirements, and taking legal and regulatory considerations into account. There is no guarantee of accuracy, completeness, timeliness, or correct sequencing of the information provided.