Kraken the Botnet: The Ethics of Counter-Hacking

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The Kraken (a 19th century word referring to a giant squid)<http://unmuseum.mus.pa.us/kraken.htm> is a huge network of personal computers that have been infected with software that turns them into zombie systems under the control of a master program – a botnet<http://www.honeynet.org/papers/bots/>. The Kraken botnet is used by criminals to generate spam. Kelly Jackson Higgins, writing for DarkReading, says “...like Storm, Kraken so far is mostly being used for spamming the usual scams – high interest loans, gambling, male enhancement products, pharmacy advertisements, and counterfeit watches, for instance.” The botnet is the largest known; in April 2008 it was estimated to included 400,000 zombies.<http://www.darkreading.com/shared/printableArticle.jhtml?articleID=211201307>

Gregg Keizer of Computerworld reports<http://www.networkworld.com/news/2008/043008-researchers-infiltrate-kraken-botnet-could.html> that in April 2008, TippingPoint researchers Pedram Amini and Cody Pierce “created a fake Kraken command-and-control server by reverse engineering the list of domain names found in a captured sample of the bot, and then registered some of the sub-domains Kraken looks for. The server essentially acted as a command-and-control honeypot that waited for connections from PCs infected with the bot.

As a result, the scientists “monitored the incoming communications from Kraken bots for seven days.” They “listened and collected statistics for a week, and filtered out [for] the IP addresses and then the systems.” Then “Pierce wrote code that would let him redirect infected PCs, or better yet, use the bot’s built-in update mechanism – something most malware includes – to remove Kraken.”

However, management at TippingPoint forbade the researchers from activating the cleaning code. They argued that although it might be nice to interfere with the botnet, the law in the US forbids unauthorized access to anyone’s computers, including zombies. In addition, managers were concerned about the possibility that their code could inadvertently damage the systems of unknowing recipients of their well-intentioned cleaning. “<http://www.theregister.co.uk/2008/04/29/kraken_botnet_infiltrated/>

This case illustrates sound judgement on the part of the managers at TippingPoint. There are two fundamental problems here:

1. Releasing programs that modify other people’s systems without permission, even with the best of intentions, is a prescription for disaster. It’s bad enough getting a poorly tested patch from a major software vendor that screws up the operating system or an application program when we allow it to load; having someone’s bright idea invade our computers without permission – and inevitably, without consideration of particular configurations that will make the program cause damage – is unconscionable.
2. Accessing someone else’s computer without permission is illegal. Period.

Readers should remind over-enthusiastic colleagues who are contemplating counter-hacking that breaking the law to punish bad guys on the ‘Net is not acceptable; corporate policies should be

Policy: Workers must not use Company X information systems to engage in hacking activities that include, but are not limited to: (a) gaining unauthorized access to any other information systems, (b) damaging, altering, or disrupting the operations of any other information systems, and (c) capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access.

In his Commentary for the policy, Wood writes,

The policy is written in such a way that it applies to both internal and external information systems. The policy embraces a wide variety of hacker techniques, including social engineering, and password grabbers. Thus the words —access control mechanism— are deliberately vague. This phrase includes smart cards, dynamic password tokens, and other extended authentication mechanisms. This policy can be used to discipline, and perhaps terminate, a worker who was hacking through Company X information systems.

The final warning is that sometimes the apparent source of trouble may be the result of deception: it is quite possible that the target of counter-hacking could be a completely innocent and totally uninvolved computer (and person) who would suffer harm because of poorly-thought-through vindictiveness.

So get busy kracken the whip! No counter-hacking!

* * *

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Copyright © 2009 M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.