

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

CRIMINAL NO. 07-20284

v.

HON. NANCY EDMUNDS

D-1 JASON MICHAEL DOWNEY,

Defendant.

GOVERNMENT'S SENTENCING MEMORANDUM

The United States, by and through its attorneys, STEPHEN J. MURPHY, United States Attorney, and TERRENCE BERG, Assistant United States Attorney, hereby submit this Sentencing Memorandum.

Defendant Jason Michael Downey pleaded guilty to Computer Intrusion, in violation of Title 18, United States Code, Section 1030(a)(5)(A)(I), on June 20, 2007.

Downey operated a "botnet," a network of computers that he infected with a virus program giving him control over several thousand computers. Downey used this program to direct the botnet to "attack" several Internet companies, resulting in a loss of approximately \$21,000. In order to create a botnet, it is necessary to design a virus program that, when successfully installed in a victim computer, will cause that victim computer to "phone home" to a command and control computer that is being operated by the "bot-herder" or "bot-master." Once infected, the victim computer will connect to the command and control computer over the Internet and will await instructions. The bot-master will then send commands to the army of infected computers through the command and control computer.

In this case, Downey operated a bot-net of over 6000 infected computers. This means that the defendant succeeded in causing over 6000 computers to download his bot virus, and that these computers were all compromised and under his control. Downey told the FBI that he obtained the bot virus called "Agobot" and had his friend program the bot virus to cause the infected computers to connect to a computer with the domain name of "yotta-byte.net." Downey would change the location of his command and control computer by changing the IP address that was assigned to the yotta-byte.net domain name. Downey registered the domain name of yotta-byte.net using false information. Downey used his botnet to send floods of data to other networks that he wanted to knock off-line. To do this, Downey had to know the correct commands to give to the infected computers that were logged into his command and control computer. This is called a "distributed denial of service" attack, or "DDOS" attack. This caused significant problems for his victims, but only approximately \$21,000 in quantifiable damages to three victims who provided damage information to the FBI: Southo.net, B2NetSolutions, and Ingeneria. In some cases, companies were charged for bandwidth usage caused by the defendant's flooding their network with data, but these charges were later reversed when it was learned the reason for the increase in bandwidth usage.

Defendant is being held accountable only for the quantifiable losses of three victims. Defendant is not being held accountable for costs that may have been incurred by the thousands of individual computer owners who were infected with his bot virus and who unwittingly participated in his various denial of service attacks.

Defendant has objected to the inclusion of both the 2-point increase in the offense characteristics for the offense involving "sophisticated means" under U.S.S.G. 2B1.1(b)(9) and

the 2-point role in the offense adjustment for “special skill” under U.S.S.G. 3B1.3. The plea agreement reserves defendant’s right to object to the two points for special skill.

The government believes that the defendant’s conduct warrants inclusion of both the increases for sophisticated means and use of special skill. Even a cursory glance at the nature of the defendant’s conduct reveals that controlling thousands of computers by means of a customized virus is to commit a crime using sophisticate means. As the Probation Department points out, the defendant possesses specialized training in computer networking. At the time of his arrest, Downey told the FBI that he was operating his own Internet Relay Chat (or “IRC”) network or service called Rizon.net, and had 44,000 users on this network. This was not an illegal enterprise, but an Internet business that he owned, involving 42 servers linked in his network, three of which were servers he owned. Downey admitted that, to operate his botnet, he used compromised computers, mostly located in Asia, and that he primarily used his bot network to attack and/or retaliate against competing IRC networks.

It is not impermissible double counting to include points for both sophisticated means and special skill because they relate to two separate characteristics of the crime. The crime itself was complicated, technically complex, and involved a large number of methods and means that could only be called “sophisticated.” At the same time, the defendant possessed specialized knowledge, whether self-taught or otherwise, which gave him the necessary skills to commit this crime successfully. If a businessman paid a computer expert to create and launch a botnet, the businessman might be held accountable for using sophisticated means, but not for having any specialized skills. Here, Jason Downey had both.

With respect to computer skills, the complexity and expertise required to deploy a bot

virus and operated a bot network clearly do not fall within the kind of computer skills that can “be learned by the general public with minimal difficulty” which the Sixth Circuit has held insufficient to garner a two-point increase for special skill. *United States v. Godman*, 223 F.3d 320 (6th Cir. 2000)(finding “amateurish . . . common and ordinary computer skills” of desk-top publishing used to manufacture counterfeit not to be special skill). The Guidelines do not prohibit the application of both special skill and sophisticated means when appropriate. *See United States v. Olis*, 429 F. 3d 540, 549 (5th Cir. 2005)(applying both enhancements to tax accountant in complex fraud scheme).

Wherefore, the government respectfully requests the Court to impose a sentence within the guideline range contained in the plea agreement and the Presentence Report.

Respectfully submitted,

STEPHEN J. MURPHY
UNITED STATES ATTORNEY

s/ Terrence Berg
TERRENCE BERG

First Assistant U.S. Attorney
211 W. Fort St., Suite 2001
Detroit, MI 48226
Phone: (313) 226-9160
Email: Terrence.Berg@usdoj.gov
Bar No. P40295

DATED: October 22, 2007

CERTIFICATE OF SERVICE

I hereby certify that on October 22, 2007, I electronically filed the foregoing document with the Clerk of the Court using the ECF system which will send notification of such filing to the following:

Jill L. Price, Esq.
Jill_Price@fd.org

I further certify that I have mailed by United States Postal Service the document to the following non-ECF participants:

N/A

s/ Terrence Berg _____
TERRENCE BERG

First Assistant U.S. Attorney
211 W. Fort St., Suite 2001
Detroit, MI 48226
Phone: (313) 226-9160
Email: Terrence.Berg@usdoj.gov
Bar No. P40295