

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

UNITED STATES OF AMERICA	:	CRIMINAL NUMBER: 07-
v.	:	DATE FILED:
RYAN GOLDSTEIN,	:	CHARGES:
a/k/a "Digerati"	:	18 U.S.C. § 371 (Conspiracy to
	:	commit computer fraud - 1 count)
	:	

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES THAT:

At all times material to this indictment:

1. Defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, resided within the Eastern District of Pennsylvania, and was a student at School A, an institution of higher learning, located within the Eastern District of Pennsylvania.;
2. School A had computers that were protected computers within the meaning of Title 18, United States Code, Section 1030(e)(2);
3. TAUNET, LCIRC, and CENSOREDNET hosted Internet Relay Chat networks that operated on computers that were protected computers within the meaning of Title 18, United States Code, Section 1030(e)(2);
4. The Internet website, www.ssgroup.org was a website that operated on computers that were protected computers within the meaning of Title 18, United States Code, Section 1030(e)(2).

GLOSSARY

5. The following is a glossary of terms regarding the Internet and computers that are relevant to this indictment:

- a. **IRC.** IRC stands for Internet Relay Chat. It is an instant communication medium over the Internet in which people type messages to each other. IRC is mainly designed for group communication in discussion forums called channels. A channel is the basic means of communication in an established IRC session. An IRC network can contain many channels.
- b. **Trojan.** A Trojan, also called a Trojan horse, is a software program in which harmful or malicious code is contained within another seemingly harmless program. When this harmless program executes, it causes the Trojan to perform a set of actions, usually working toward the goal of allowing itself to persist on the target system. Trojans can allow “hackers” to open “back doors” into the target system, giving them access to files and the ability to connect to a network.
- c. **Botnet.** A botnet is a collection of compromised computers (referred to as “bots,” short for “robots”), that have been infected with malicious computer software, such as Trojans. Using the malicious code in the Trojans, the botnet's controller (known as a “botherder”) controls the group of compromised computers, commonly through IRC. The term “botnet” is shorthand for “robot network.”
- d. **Distributed Denial of Service Attack.** A Distributed Denial of Service Attack (DDoS) is a form of attack on another computer on the Internet that overloads the

victim computer. A person attempting a DDoS attack enlists other computers, without the knowledge of the owners, to assist in the attack by causing other computers to bombard the target computer with requests or commands at the same time. This increases the number of messages that can be directed to the victim computer and increases the chances of slowing the victim computer and crashing it. Botnets are frequently used to perform DDoS attacks.

THE CONSPIRACY

6. From on or about January 30, 2006, up to and including, on or about July 14, 2006, defendant

RYAN GOLDSTEIN, a/k/a/ Digerati,

conspired with Person A, an individual whose full identity is unknown to the grand jury, and other persons unknown to the grand jury, knowingly to cause the transmission of codes and commands, with the intent that as a result of such transmission, they would cause damage, without authorization, to protected computers; and further, as a result of such conduct, defendant **GOLDSTEIN**, Person A, and other persons unknown to the grand jury caused a loss of more than \$5,000 to School A; in violation of Title 18, United States Code, Section 1030(a)(5)(A)(i).

HOW THE CONSPIRACY WORKED

7. From a time unknown to the grand jury, until in or about the early part of 2006, defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, was a member of the IRC group known as TAUNET.

8. In or about January 2006, the administrators of TAUNET banned the defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, from TAUNET.

9. In or about January 2006, defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, was involved in on-line disputes with other persons on the Internet.

10. Defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, used an IRC channel to discuss with Person A means of punishing the TAUNET IRC, for banning him, including the launching of DDoS attacks on TAUNET.

11. Defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, also requested Person A to launch DDoS attacks against other computers on the Internet that hosted IRC networks, including LCIRC and CENSOREDNET, and against a website, www.ssgroup.org.

12. Person A is an individual who controlled at least one botnet.

13. Person A updated his botnets by directing them to a server on the Internet from which they were directed to download the latest malicious code files to conduct DDoS attacks.

14. To perform the DDoS attacks that defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, requested, Person A needed to update the computers in his botnet with new malicious code.

15. Person A needed a server on which to place his malicious code files.

16. School A gave to each of its students, including defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, an account and access privileges on a protected computer.

17. Defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, gained unauthorized access to the account of another student (hereafter "Student B").

18. Defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, offered to place Person A's malicious code files in the account of Student B on the computers of School A.

19. Defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, then obtained the malicious code files from Person A and uploaded them into the computer account of Student B. These files included Trojans.

20. Defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, then directed Person A to employ his botnet to access the account of Student B on the protected computer at School A, and to download the files that defendant **RYAN GOLDSTEIN, a/k/a/ Digerati** had loaded onto the account of Student B.

21. At the direction of defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, Person A employed his botnet to launch DDoS attacks against other IRC networks, including TAUNET, LCIRC and CENSOREDNET, and against a website, www.ssgroup.org.

OVERT ACTS

To further the conspiracy and to achieve its objects, the following overt acts were committed in the Eastern District of Pennsylvania and elsewhere:

1. On or about January 30, 2006, defendant **RYAN GOLDSTEIN, a/k/a/ Digerati**, in a conversation in an IRC channel, wrote to Person A, "i can get you some good private stuff, i can also pay you, to take taunet down..... i have access to a lot of stuff you might want..... www.findnot.com/servers.html - i have a legit login/pass for that, guaranteed to work through 2007 at least... undetected, unreleased bifrost (trojan) beta with 100% av (antivirus) and fw (firewall) bypass."

2. On or about January 31, 2006, defendant **RYAN GOLDSTEIN, a/k/a Digerati**, again wrote to person A, urging him to launch a computerized attack against TAUNET.

3. On or about February 2, 2006, and February 3, 2006, defendant **RYAN GOLDSTEIN, a/k/a Digerati**, wrote to person A, urging him to launch a DDoS attack against CENSOREDNET.

4. On or about February 9, 2006, February 15, 2006, February 17, 2006, and February 19, 2006 defendant **RYAN GOLDSTEIN, a/k/a Digerati**, wrote to person A, urging him to launch a DDoS attack against LCIRC.

5. On or about February 19, 2006, defendant **RYAN GOLDSTEIN, a/k/a Digerati**, wrote to person A, urging him to launch a DDoS attack against www.ssgroup.org.

6. On or about February 19, 2006, defendant **RYAN GOLDSTEIN, a/k/a Digerati**, wrote to Person A and told him to send him the malicious code that he wanted to use to update the computers in his botnet.

7. On or about February 19, 2006, defendant **RYAN GOLDSTEIN, a/k/a Digerati**, uploaded this code to the account of Student B on the protected computers of School A and gave the Internet address to Person A, so that Person A could update the computers in his botnet.

8. On or about February 19, 2006, Person A caused the computers in his botnet to update their files by having each computer log into the account of Student B and download the files that defendant **RYAN GOLDSTEIN, a/k/a Digerati**, had placed there. The large number of computers downloading from this protected computer slowed the response time of the computer.

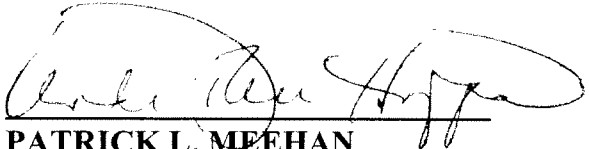
9. On or about February 23, 2006, Person A caused the computers in his botnet to update their files by having each computer log into the account of Student B and download the files that defendant **RYAN GOLDSTEIN, a/k/a Digerati**, had placed there. The number of requests for these files was larger than the protected computer could handle and, as a result, the computer ceased functioning (“crashed”). School A spent more than \$5,000 restoring the protected computer.

10. On or about On March 13, 2006, defendant **RYAN GOLDSTEIN, a/k/a Digerati** wrote to Person A, “i want taunet taken down, they are starting to annoy me again.... they must stay down for at least a week or so.”

All in violation of Title 18, United States Code, Section 371.

A TRUE BILL

GRAND JURY FOREPERSON

Pol


PATRICK L. MEEHAN
UNITED STATES ATTORNEY