UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. Susan D. Wigenton
	:	
v.	:	Crim. No. 11-470
	:	
ANDREW AUERNHEIMER, a/k/a "Weev" a/k/a "Weevlos" a/k/a "Escher"	: : : :	18 U.S.C. §§ 371 & 1028(a)(7), & § 2

S U P E R S E D I N G I N D I C T M E N T

The Grand Jury, in and for the District of New Jersey, sitting at Newark, charges:

COUNT ONE

(Conspiracy to Access a Computer Without Authorization)

1. At all times relevant to this Indictment:

a. Defendant ANDREW AUERNHEIMER resided in Arkansas, and was a member of an organization called Goatse Security ("Goatse").

b. Co-conspirator Daniel Spitler resided in California, and was a member of Goatse.

c. Goatse described itself as a "security research" company, and was comprised of Internet hackers (individuals who accessed sites and information to which they did not have authorized access) and so-called "trolls" (individuals who intentionally, and without authorization, disrupt services and content on the Internet). The Goatse website

provided a hyperlink to the website of an organization referred to as the "GNAA."

d. The GNAA website states that "[t]his website is maintained by the GNAA, world-famous trolling organization." The GNAA website provided hyperlinks to the Goatse website, as well as to defendant AUERNHEIMER's LiveJournal weblog.

e. The iPad, introduced to the market on or about January 27, 2010, was a device developed and marketed by Apple Computer, Inc. It was a touch-screen tablet computer, roughly the size of a magazine. The iPad allowed users to, among other things, access the Internet, send and receive electronic mail, view photographs and videos, read electronic books, word-process, and create spreadsheets and charts.

f. The "3G" model of the iPad ("iPad 3G") allowed users to access to the Internet using either Wi-Fi or the 3G wireless network hosted by AT&T Services, Inc. ("AT&T").

g. AT&T was an interexchange carrier and long distance telephone company, located in Bedminster, New Jersey, among other places.

h. AT&T's servers and individual iPads were

"protected computers" as defined in Title 18, United States Code, Section 1030(e)(2).

i. Title 18, United States Code, Section 1030(e)(2)(B)(2) provides, in relevant part, that "the term 'protected computer' means a computer -- . . . (B) which is used in or affecting interstate or foreign commerce or communication."

j. Among other things, AT&T provided certain iPad users with Internet connectivity via AT&T's 3G wireless network.

k. iPad 3G users who wished to subscribe to the AT&T 3G network had to register with AT&T. During the registration process, the user was required to provide, among other things, an e-mail address, billing address, and password.

l. The iPad 3G user e-mail addresses, billing addresses, and passwords were not available to the public and were kept confidential by AT&T.

m. At the time of registration, AT&T automatically linked the iPad 3G user's e-mail address to the Integrated Circuit Card Identifier ("ICC-ID") of the user's iPad, which was a 19 to 20 digit number unique to every iPad (specifically, unique to the Subscriber Identity Module ("SIM") card in the

iPad).

n. Due to this feature, each time a user accessed the AT&T website, the user's ICC-ID was recognized and, in turn, the user's e-mail address was automatically displayed. This allowed the user speedier and more user-friendly access to the network.

o. The ICC-IDs and iPad user e-mail addresses were not available to the public and were kept confidential by AT&T.

GOATSE SECURITY

2. Defendant AUERNHEIMER, as the self-professed spokesman for Goatse, has previously been public and outspoken about his trolling activities.

3. According to the Goatse Security website, the Goatse "Team" included approximately eight members, among whom were defendant AUERNHEIMER, who was also known as "weev," and Spitler.

4. The Goatse website described defendant AUERNHEIMER as having "[e]xtensive offensive web app[lication] vuln[erability] and business logic exploitation experience. . . . Representing antisec, Bantown and Encyclopedia Dramatica. President of the GNAA." Spitler was described as an "embedded and mobile devices engineer. PPC assembly. GNAA, obviously."

THE CONSPIRACY

5. From on or about June 2, 2010 through on or about June 15, 2010, in the District of New Jersey, and elsewhere, defendant

ANDREW AUERNHEIMER

knowingly and intentionally conspired with Spitler and others to access a computer without authorization and to exceed authorized access, and thereby obtain information from a protected computer, namely the servers of AT&T, in furtherance of a criminal act in violation of the Constitution and laws of the State of New Jersey, namely, N.J.S.A 2C:20-31(a), contrary to Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii).

OBJECTS OF THE CONSPIRACY

6. The objects of the conspiracy were for defendant AUERNHEIMER, Spitler, and others to steal and disclose the personal identifying information of thousands of individuals, to cause monetary and reputational damage to AT&T and to create monetary and reputational benefits for themselves.

MANNER AND MEANS OF THE CONSPIRACY

A. The Account Slurper

7. Prior to mid-June 2010, when an iPad 3G communicated with AT&T's website, its ICC-ID was automatically displayed in the Universal Resource Locator, or "URL," of the AT&T website in plain text. Seeing this, and discovering that each ICC-ID was connected to an iPad 3G user e-mail address, defendant AUERNHEIMER and Spitler conspired to write, and did write, a

script termed the "iPad 3G Account Slurper" (the "Account Slurper") and deployed it against AT&T's servers.

8. The Account Slurper attacked AT&T's servers for several days in or around June 2010, and was designed to harvest as many ICC-ID/e-mail address pairings as possible. It worked as follows:

a. The Account Slurper was designed to mimic the behavior of an iPad 3G so that AT&T's servers were fooled into believing that they were communicating with an actual iPad 3G and wrongly granted the Account Slurper access to AT&T's servers.

b. Once deployed, the Account Slurper utilized a process known as a "brute force" attack - an iterative process used to obtain information from a computer system - against AT&T's servers. Specifically, the Account Slurper randomly guessed ranges of ICC-IDs. An incorrect guess was met with no additional information, while a correct guess was rewarded with an ICC-ID/e-mail pairing for a specific, identifiable iPad 3G user.

9. From on or about June 5, 2010 through on or about June 9, 2010, the Account Slurper attacked AT&T's servers, gained unauthorized access to those servers, and ultimately stole for its hacker-authors, including defendant AUERNHEIMER and Spitler,

approximately 120,000 ICC-ID/e-mail address pairings for iPad 3G customers. This was done without the authorization of AT&T, Apple, or any of the individual iPad 3G users.

10. Neither defendant AUERNHEIMER, Spitler, nor any other member of Goatse obtained prior authorization from any victim of the breach.

B. Defendant AUERNHEIMER and Goatse Knowingly Disclose Approximately 120,000 ICC-IDs and Corresponding E-Mail Addresses to the Internet Magazine Gawker, and Take Credit for the Breach

11. On or about June 9, 2010, immediately following the theft, the hacker-authors of the Account Slurper knowingly provided stolen e-mail addresses and ICC-IDs to the website Gawker. Gawker was an internet magazine. Gawker proceeded to publish on its website the stolen information, though in redacted form, as well as an article concerning the breach (the "Gawker Article").

12. Also on or about June 9, 2010, defendant AUERNHEIMER made an entry on his LiveJournal weblog, which read, in pertinent part: "Oh hey, my security consulting group just found a privacy breach at AT&T[.]" LiveJournal was a social networking website on which users could set up personal weblogs and post messages. Once a weblog had been created, only the user of that weblog could post messages and content on that weblog. The post further linked to the Gawker Article and stated: "[T]his story has been broken for 15 minutes, twitter is blowing the f[***] up, we are

on the forntpage [sic] of google news and we are on drudge report (the big headline)[.]" The "User Profile" for the LiveJournal weblog, http://weev.livejournal.com, listed the user as "weev" with the name "Escher Auernheimer."

13. On or about June 10, 2010, the website CNET published an article titled, "Hacker defends going public with AT&T's iPad data breach (Q&A)." The article reported: "On Thursday, CNET talked to a key member of Goatse - Escher Auernheimer, also known as 'Weev' - about the group and what motivates them." In the article, a question and answer dialog was presented, including the following:

Q: So, one of your members had an iPad and noticed this strange interaction with the AT&T Web site?
A: He used this AT&T security maintenance app. It was part of the normal user experience that tipped him off to something that would allow him to scrape this data.
Q: Then a script was written to do an automated brute force, right?
A: Correct.

C. The Internet Relay Chats

14. On or about June 15, 2010, during the execution of a Court-authorized search warrant, defendant AUERNHEIMER agreed to speak with federal law enforcement officers and stated, among other things, that he and the other members of Goatse often communicated with one another using an online medium known as Internet Relay Chat, or "IRC."

i. June 5, 2010: Exploiting the Breach

15. On or about June 5, 2010, co-conspirator Spitler was

chatting with fellow Goatse members "Nstyr" and "Pynchon." The three considered the possible benefits of harvesting ICC-ID/e-mail pairings.

> **Spitler:** if you enter valid ICCIDs in this website you can get iPad subscriber email addresses I dont see the point unless we phish[1] for passes [passwords] even then that's boring
> **Nstyr:** data minig *mining you could put them in a database for spamming for example sell them to spammers. . .
> **Spitler:** tru ipad focused spam
> **Pynchon:** harvest all the emails then expose it publicly
> **Spitler:** hahaha
> **Pynchon:** tarnish at&t
> **Spitler:** true
> **Nstyr:** or sell if for thousands to the biggest spammers

16. Later that day, Spitler reported the following to defendant AUERNHEIMER:

> **Spitler:** I just harvested 197 email addresses of iPad 3G subscribers there should be many more . . . weev: did you see my new project?
> **AUERNHEIMER:** no
> **Spitler:** I'm stepping through iPad SIM ICCIDs to harvest email addresses if you use someones ICCID on the ipad service site it gives you their address
> . . .
> **AUERNHEIMER:** looool[2] thats hilarious HILARIOUS oh man now this is big media news . . . is it scriptable? arent there SIM that spoof iccid?
> **Spitler:** I wrote a script to generate valid iccids and it loads the site and pulls an email
> . . .
> **AUERNHEIMER:** this could be like, a future massive phishing

---

[1] "Phishing" involved sending e-mails to users falsely claiming to be an established, legitimate enterprise in an attempt to scam the users into surrendering private information that would be used for identity theft.

[2] "LOL" and its variants, including "lawlwla," stand for laughing out loud.

operation serious like this is valuable data we have a list a potential complete list of AT&T iphone subscriber emails
Spitler: ipad but yeah

17. When Spitler announced that he was "in a rut" and having difficulty determining additional ICC-ID/e-mail pairings, defendant AUERNHEIMER assisted, offering: "SIM cards may be allocated by geographic region, either for number administration or [] network planning reasons. The method of payment (pre-paid, post-paid) may be allocated on the SIM cards. . . . so sims are definitely preallocated either by geographic region sales channes, service providers or MVNOs question is who allocates them . . . probably AT&T suballocates free IDs to apple hopefully not at random . . . otherwise we have a real big space to search[.]"

18. On or about June 5, 2010, and again the following day, defendant AUERNHEIMER encouraged Spitler to amass as many ICC-ID/e-mail pairings as possible, writing: "if we can get a big dataset we could direct market ipad accessories[.]" Likewise, after learning that Spitler had collected "625 emails," defendant AUERNHEIMER wrote: "takes like, millions to be profitable re: spam but thats a start[.]"

ii. June 6, 2010: Collecting Stolen E-Mails

19. Responding to defendant AUERNHEIMER's encouragement, on or about June 6, 2010, Spitler reported:

Spitler: I hit f[***]ing oil
AUERNHEIMER: looooool nice

Spitler: If I can get a couple thousand out of this set where can we drop this for max lols?
AUERNHEIMER: dunno i would collect as much data as possible the minute its dropped, itll be fixed BUT valleywag i have all the gawker media people on my facecrook friends after goin to a gawker party

20. As Spitler uncovered additional ICC-ID/e-mail pairings, he continued speaking with defendant AUERNHEIMER about releasing the information to the press and the legality of the data breach:

Spitler: do I got to get involved
AUERNHEIMER: no
Spitler: I'd like my anonaminity
AUERNHEIMER: alright
Spitler: sry dunno how legal this is or if they could sue for damages
AUERNHEIMER: absolutely may be legal risk yeah, mostly civil you absolutely could get sued to f[***]
Spitler: D8[3]
AUERNHEIMER: alright i can wrangle the press just get me the codes and whatnot show me how to run this thing

21. Spitler then proceeded to provide the script to defendant AUERNHEIMER, writing: "heres the script you run it php [redacted] . . . ."

22. As the data breach continued, defendant AUERNHEIMER wrote to Spitler: "if we get 1 reporters address with this somehow we instantly have a story . . . the best way to have a leadin on it . . . HI I STOLE YOUR EMAIL FROM AT&&T WANT TO KNOW HOW?"

23. Spitler then proceeded to provide defendant AUERNHEIMER

---

[3] The phrase "D8" means "balls deep," *i.e.*, to be deeply involved in an activity or to perform an activity to the fullest extent possible.

with an ICC-ID and e-mail address for a member of the Board of Directors at News Corporation.

24. Defendant AUERNHEIMER sent an e-mail to that board member, which read in relevant part:

> "An information leak on AT&T's network allows severe privacy violations to iPad 3G users. Your iPad's unique network identifier was pulled straight out of AT&T's database . . . . We have collected many such identifiers for members of the media and major tech companies . . . . If a journalist in your organization would like to discuss this particular issue with us[,] I would be absolutely happy to describe the method of theft in more detail."

The e-mail to the board member included the ICC-ID for the board member's iPad.[4]

iii. June 7, 2010: Identifying Information from More Than 100,000 Victims Stolen

25. After Spitler announced that he had stolen over 100,000 ICC-ID/e-mail address pairings, defendant AUERNHEIMER stated: "the more email addresses we get . . . the more of a freakout we can cause if nothing else we can pack these into a [database] . . . and do a mail merge and mail EVERYONE with an ipad 3g 1 o 1[.]" To that, Spitler responded simply: "lawlwla[.]"

---

[4] In addition to the e-mail sent to the board member at News Corporation, defendant AUERNHEIMER sent similar e-mails to an employee of the *San Francisco Chronicle*, an employee of the Washington Post, and to employees of Thomson-Reuters. Defendant AUERNHEIMER later forwarded these e-mails to yet others, including a reporter at Forbes magazine.

iv. June 10, 2010: Destroying Evidence

26. On or about June 10, 2010, defendant AUERNHEIMER and Spitler had the following conversation during which they discussed destroying evidence of their crime:

AUERNHEIMER: i would like get rid of your shit like are we gonna do anything else with this data?
Spitler: no should I toss it?
AUERNHEIMER: i dont think so either might be best to toss
Spitler: yeah, I dont really give a fuck about it the troll is done
AUERNHEIMER: yes we emerged victorious
Spitler: script is going byebye too

OVERT ACTS

27. In furtherance of the conspiracy and to effect its objects, defendant AUERNHEIMER and his co-conspirators, including Spitler, committed and caused to be committed the following overt acts in the District of New Jersey and elsewhere:

a. In or around June 2010, the co-conspirators wrote the Account Slurper.

b. In or around June 2010, the co-conspirators deployed the Account Slurper against AT&T's servers.

c. In or around June 2010, defendant AUERNHEIMER sent a series of e-mails to victims that included the ICC-IDs of the victims' iPads, and described his and his co-conspirators' actions as a "theft."

d. In or around June 2010, defendant AUERNHEIMER and

his co-conspirators disclosed approximately 120,000 stolen ICC-ID/e-mail address pairings for iPad 3G customers -- including thousands of customers who resided in New Jersey -- to the internet magazine Gawker.

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

COUNT TWO

(Fraud in Connection with Personal Information)

1. Paragraphs 1 through 4 and 7 through 27 of Count One of this Superseding Indictment are hereby alleged and incorporated as though set forth in full herein.

2. From on or about June 2, 2010 through on or about June 15, 2010, in the District of New Jersey, and elsewhere defendant

ANDREW AUERNHEIMER

knowingly transferred, possessed, and used, without lawful authority, means of identification of other persons, including means of identification of New Jersey residents, in connection with unlawful activity, specifically, the unlawful accessing of AT&T's servers contrary to Title 18, United States Code, Section 1030(a)(2)(C).

In violation of Title 18, United States Code, Sections 1028(a)(7) and Section 2.

A TRUE BILL

Paul J. Fishman/rah

PAUL J. FISHMAN
UNITED STATES ATTORNEY

CASE NUMBER: 2010R00631

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

ANDREW AUERNHEIMER

SUPERSEDING INDICTMENT FOR

18 U.S.C. §§ 371 and 1028(a)(7)

PAUL J. FISHMAN
UNITED STATES ATTORNEY, NEWARK, NEW JERSEY

MICHAEL MARTINEZ
ZACH INTRATER
ASSISTANT U.S. ATTORNEYS
NEWARK, NEW JERSEY
(973) 645-2728