**Computer Crime**

**Professor Ohm**

In-Class Exercise 1/28/2013: 18 U.S.C. § 1030(a)(2) and (a)(5)

One night, Jon Leibowitz—cosmopolitan chairman of the FTC by day, notorious computer criminal by night—is on a computer crime spree, attacking computers across the country. For all of the following problems, ignore the *attempt* provisions of section 1030.

Target One: FedWatch's Eligible Bachelors server

First, Chairman Leibowitz targets the computer network of the magazine, FedWatch, hoping to gain access to the ultra-secret "government agencies" server housing the statistics used in their annual ranking of most important and effective government agencies.

Inadvertently, he first accesses the magazine's "most eligible bachelors" server, and by guessing passwords gains administrator access. The server displays the message "Welcome to our sirver."

[A-1] Has he violated 1030(a)(2) or (a)(5) at this point?

He has probably violated (a)(2)(C). The "information obtained" is the welcome message. He has probably not violated (a)(5) because he has not caused damage, unless "integrity" is read very broadly (pages 107-108).

A stickler for spelling, Chairman Leibowitz modifies the file containing the greeting to fix the misspelled word sirver.

[A-2] Has he violated 1030(a)(5) at this point?

Probably. Damage is broadly defined.

Assume he doesn't make the change in A-2. Instead, he browses through the confidential files stored on the server, and quickly realizes that he is on the wrong server, so he decides to log out.

[A-3] Has he violated 1030(a)(2) or (a)(5) at this point?

Same answer as [A-1].

Instead of typing the correct command, "end," he accidently types, "rend," which begins to delete all of the files on the server. Not knowing what he has done, he types "end" and successfully logs out.

[B-1] Has he violated 1030(a)(5) at this point?

Probably (a)(5)(C). Damage and loss are probably satisfied. The damage isn't intended, so probably no (A). Is it reckless? Debatable. If so, (B), if not, then no.

As it happens, the Bachelors rankings server was also being under a special contract with the U.S. Government to help rank the effectiveness of leaders in Afghanistan, as part of the military effort. A secret part of the hard drive contained military assessments of each college, including categories like "potential to breed extremism." Chairman Leibowitz's "rend" command deletes that data too.

[B-2] Has he violated a felony 1030(a)(5) at this point?

Yes. Felony enhancement for "administration of justice, national defense, or national security". Probably also $5,000 worth of damage.

Target Two: FedWatch's Agencies server

Second, Chairman Leibowitz correctly identifies the Tech Policy Today server containing the agency evaluation statistics. He tries to guess passwords, but he cannot.

[C-1] Has he violated 1030(a)(5) at this point?

Probably not. Probably no access.

Not being able to gain access, Chairman Leibowitz commands his botnet army to launch a distributed denial of service attack at the agencies server. The attack succeeds, and the agencies server becomes unresponsive.

[C-2] Has he violated 1030(a)(5) at this point? Has he committed a felony or just a misdemeanor?

Probably a violation because of (a)(5)(A) and broad definition of damage. Whether it is a felony turns on loss definition and $5,000.

After learning about the attack, FedWatch executives take the seven steps in response listed on page 119-20, Note 2 (A-G) of your casebook.

[D-1 to D-4] Has Chairman Leibowitz committed a felony under 1030(a)(5) if FedWatch takes response A? B? C? D? (assume for each that this is the only response they undertake)

All of these questions ask whether the specified expense qualifies as loss counted toward the $5,000 felony threshold. So it's hard to know whether this is a felony without knowing how much was spent. So instead of answering whether the Chairman has committed a felony, the answers below answer the question posed in the book—which of these should be considered loss under (e)(11) and cases interpreting it?

[D-1] (Problem A) Probably a reasonable cost included in the loss.

[D-2] (Problem B) Probably not. See Nexans Wires in Note 4.

[D-3] (Problem C) Probably not. But maybe a closer call?

[D-4] (Problem D) Probably not under Nexans Wires and B&B Microscopes (page 122) but because the lost business is due to doubts about security, might be a slightly stronger case than either of those two to include this in loss. Still, probably not.

[E-1 to E-3] Has Chairman Leibowitz committed a felony under 1030(a)(5) if FedWatch takes response E? F? G? (assume for each that this is the only response they undertake)

[E-1] (Problem E) Probably not. And is this really a "loss" to the company, as opposed to the shareholders?

[E-2] (Problem F) Possibly. Assuming that they took the website down to remediate the damage, possible argument that this is a loss.

[E-3] (Problem G) Similar to F, but probably not. Further attenuated.

[E-4] If FedWatch's Chief Security Officer, who makes an annual salary of $100,000, spends 100 hours investigating and fixing the nonresponsive server, has Chairman Leibowitz committed a felony under 1030(a)(5)?

Probably, but it's arithmetically close. First, you can include salary even though it would have been paid even without the hack because the CSO isn't working on other things, per Millot, Note 3. The problem is that depending on how you divide up a $100,000 salary, you might end up just below or just above $50/hour, meaning you are very close to the $5000 line. Still, the FBI agent can probably find a few more things to throw in to get it over the line, regardless.

Target Three: Assembling the botnet

After the successful denial of service, FBI agents begin to investigate the Chairman's botnet. Over the span of a few years, the Chairman has spent his evenings infecting as many computers on the Internet as he can with a virus. The viruses listen for commands from the Chairman but otherwise do not affect the functioning of the infected computer in anyway. The FBI discover at least 100,000 infected computers in the botnet.

[F-1] Has the Chairman violated 1030(a)(5)? Has he committed a felony or just a misdemeanor?

Misdemeanor (A), (B), and (C) are all easy. For felony, first must go through (c)(4)(A)(i)(I) carefully. Aggregating $5000? Probably not. But likely felony anyway under (c)(4)(A)(i)(VI) ten or more protected computers? Sure.

[F-2] The FBI notifies the victims of the botnet that they should wipe their computers clean in order to ensure they have removed the virus. Later, the FBI collects affidavits from a few hundred of the victims stating that they spent as little as two hours and as many as an entire week and paid from $0 to $1000 repairing their systems. Does this help the FBI establish a felony? What kinds of upgrades should count or not?

Probably felony anyway under VI, but this is asking about I. These facts help get to $5000. Security patches should probably count. But upgrades to a newer version of the OS (with better features) probably shouldn't count

[F-3] Can the FBI use the affidavits of cohabitants of the victims of the botnet who also wiped their machines clean and incurred similar costs, because they were afraid that they might have contracted the virus?

Probably not. Not a reasonable cost. Maybe not even a "victim."

[F-4] If the Chairman's botnet consisted entirely of vulnerable Internet-connected refrigerators with tiny, on-board processing units and no traditional computers, has he violated 1030(a)(5)?

Yes. "Computer" and "protected computer" both defined broadly.

Target Four: The FTC HR Computer

Basking in the glow of his attack on FedWatch, Chairman Leibowitz turns his attention to his problem Employee, Paul Ohm. Ohm is up for a promotion next year, and Chairman Leibowitz is bent on preventing him from getting it. To help sink Ohm's chances, Chairman Leibowitz decides to modify Ohm's past work evaluations, which are stored on the FTC HR Department's computer.

Chairman Leibowitz logs into the HR computer using his "master password," the password he was given as Chairman that allows him onto any FTC computer. He finds Ohm's evaluations and begins changing all favorable comments and numerical grades to their opposites.

[G-1] Has he violated 1030(a)(5) at this point?

Probably not. He is exceeding authorized access, but not acting without authorization as required. But, maybe his act is without authorization because maybe he's not supposed to be on this particular computer (need facts). Even better, maybe this is a (a)(5)(A) which puts the mens rea on the damage without authorization, not on the access.

For fun, he exploits a program on the HR server to access the personal files of the director of HR—files he can't access even with his master password. Once logged in, he modifies her computer's login scripts to blare the "Chicken Dance Song" every morning when she logs in.

[G-2] Has he violated 1030(a)(5) at this point?

Yes, probably the misdemeanor provisions.