

Computer Crime

Professor Ohm

In-Class Exercise 9/9/9: 18 U.S.C. § 1030(a)(5)

One night, David Getches—cosmopolitan law school Dean 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: U.S. News Business School Server

First, Dean Getches targets the computer network of the magazine, U.S. News & World Reports, hoping to gain access to the ultra-secret “law school rankings” server housing the statistics used in their annual survey.

Inadvertently, he first accesses the “business school rankings” server, and by guessing passwords gains administrator access.

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

Perhaps, if “integrity” might be defined to mean “loss of trust”. See Note 11 at top of p.97.

After logging in, the server displays the message, “Welcome to our sirver.” A stickler for spelling, Dean Getches modifies the file containing the greeting to fix the misspelled word.

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

Probably. Damage is so 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)(5) at this point? Has he violated any other 1030 provision?

No. But he has probably violated 1030(a)(2)(C).

Instead of typing the correct command, “end,” he accidentally 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 the misdemeanor in (c)(4)(G) under (C). Damage and loss are probably satisfied. The damage isn’t intended, so probably no (A). Is it reckless? If so, (B), if not, then no. Maybe talk about “transmission” for (A) Talk also about footnote d on p.103 about what intent do damage means.

As it happens, the Business School rankings server was also being under a special contract with the U.S. Government to help rank colleges in Iraq, as part of the rebuilding effort. A secret part of the hard drive contained military assessments of each college, including categories like “potential to breed extremism.” Dean Getches’ “rend” command deletes that data too.

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

Target Two: U.S. News Law School Server

Second, Dean Getches correctly identifies the U.S. News server containing the law school rankings. He tries to guess passwords, but he cannot.

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

Probably not. No access. Transmission of code?

Not being able to gain access, Dean Getches commands his botnet army to launch a distributed denial of service attack at the law school rankings server. The attack succeeds, and the law school rankings 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 broad definition of damage. Whether it is a felony turns on loss definition and \$5,000.

After learning about the attack, U.S. News executives take the seven steps in response listed on page 92, Note 2 (A-G) of your casebook.

[D-1 to D-4] Has Dean Getches committed a felony under 1030(a)(5) if U.S. News takes response A? B? C? D? (assume for each that this is the only response they undertake)

[E-1 to E-3] Has Dean Getches committed a felony under 1030(a)(5) if U.S. News takes response E? F? G? (assume for each that this is the only response they undertake)

For both, should be looking at case in Note 4 about damage “related to computers.”

[E-4] If U.S. News’s Chief Security Officer, who makes an annual salary of \$100,000, spends 100 hours investigating and fixing the nonresponsive server, has Dean Getches committed a felony under 1030(a)(5)?

Close call, but see Sablan. Good if they cite language from Note 3, p.93 “could have been spent on other duties under the contract.”

Target Three: Assembling the botnet

After the successful denial of service, FBI agents begin to investigate the Dean’s botnet. Over the span of a few years, the Dean has spent his evenings infecting as many computers on the internet as he can with a virus. The viruses listen for commands from the Dean 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 Dean violated 1030(a)(5)? Has he committed a felony or just a misdemeanor?

Misdemeanor (A), (B), and (C) are all easy. Must go through (c)(4)(A)(i)(I) carefully. Aggregating \$5000? Probably not. (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?

Helps get to \$5000 (notwithstanding VI makes it less important to do so). But upgrades to Windows 7 or Linux 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."

Target Four: The Registrar's Computer

Basking in the glow of his attack on U.S. News, Dean Getches turns his attention to his problem Professor, Professor Ohm. Professor Ohm is up for tenure next year, and Dean Getches is bent on preventing him from getting it. To help sink Ohm's chances, Dean Getches decides to modify Ohm's past student evaluation grades which are stored on the Registrar's computer, because teaching quality is the only factor important in the tenuring process.

Dean Getches logs into the Registrar's computer using his "master password," the password he was given as Dean that allows him onto any law school computer. He finds Ohm's student evaluations and begins changing all 5's into 1's.

[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 registrar's computer to access the personal files of the registrar—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.