

University student pleads guilty to making Android spy app

August 25 2015, by Joe Mandak



A Carnegie Mellon University student who hoped to sell enough malicious software to infect 450,000 Google Android smartphones pleaded guilty Tuesday to a federal law meant to prevent hacking of phones and computers.

But how many phones were actually infected by Morgan Culbertson's malicious creation remained a mystery after his court appearance before a federal judge in Pittsburgh. Infected phones could be remotely controlled by others and used to spy and secretly take pictures without the phone owner's knowledge, as well as to record calls, intercept text messages and otherwise steal information the owners downloaded on the devices.

Culbertson, 20, of Churchill, faces up to 10 years in prison and \$250,000 in fines when he's sentenced Dec. 2. But he'll likely face probation or a short prison term under sentencing guidelines that will take into account his lack of a criminal record.

Culbertson is one of 12 people charged by U.S. authorities, and the fourth to plead guilty so far, in the worldwide takedown of the Darkode.com cybercriminal marketplace.

A total of 70 people have been targeted for allegedly using the cybercriminal marketplace where hackers bought and sold malicious software, and otherwise advertised schemes to infect computers and cellphones with software that could cripple or illegally control the devices.

"I committed the crime, so I am responsible," Culbertson told Senior U.S. District Judge Maurice Cohill Jr. on Tuesday and apologized to those whose phones were affected by the malware.

"I understand what I did was wrong and I take full responsibility," Culbertson said. "I would like in the future to use my skills to help protect people."

Culbertson said he has taken a leave of absence from Carnegie Mellon, where he's completed his sophomore year. He previously interned for a

cybersecurity firm in California's Silicon Valley.

Assistant U.S. Attorney Jimmy Kitchen said Culbertson worked online with a man identified only as "Mike from the Netherlands" to create Dendroid, the malware that was secretly linked to Android phone apps available for purchase through Google Play.

Culbertson developed the "binder"—or computer code used to hide Dendroid on the apps—with another unidentified man, then "bought out" Mike's share of the operation and planned to sell 200 to 300 copies of the malware on Darkode.com for \$400 a copy, Kitchen said.

Culbertson expected each person who bought Dendroid would be able to infect about 1,500 phones with it, or 300,000 and 450,000 phones total.

Culbertson also tried to sell the "source code" that would enable others to make their own copies of Dendroid for \$65,000 and at an online auction for \$10,000, but defense attorney Emily McNally said that never happened.

Kitchen wouldn't say how many Dendroid copies Culbertson actually sold.

McNally said Culbertson personally used a copy to infect and control about two dozen phones, though some of those were Culbertson's and were controlled for testing how Dendroid worked.

She and Culbertson declined comment after the hearing.

© 2015 The Associated Press. All rights reserved.

Citation: University student pleads guilty to making Android spy app (2015, August 25) retrieved 3 May 2024 from <https://phys.org/news/2015-08-university-student-guilty-android-spy.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.