Researcher blogged about workaround for Apple OS update's USB Restricted Mode

11 July 2018, by Nancy Owano

Credit: elcomsoft

The iOS 11.4.1 update carries the USB Restricted Mode. But could law enforcement work around it? That dominated news about the feature on Tuesday. Let's see what the feature is all about and how it has been, of sorts, outsmarted.

Fundamentally, the explanation from *iTnews* was succinct. Juha Saarinen said this is "a security feature designed by Apple to prevent iPhone and iPad data ports being used by law enforcement to crack passcodes." What were other definitions of iOS 11.4.1's USB Restricted Mode?

Rob LeFebvre in *Engadget* and other tech watchers explained it as a defiance of passcode-cracking solutions, a defense against security hacking. LeFebvre said, "Restricted mode was created to protect iPhones against USB devices used by law enforcement to crack your passcode and get around encryption."

Restricted Mode is activated if the iPhone or iPad is left locked for more than an hour.

Benjamin Mayo, who creates apps for iOS as a professional indie developer and contractor, wrote in *9to5Mac* that this Restricted Mode feature was "quite a significant roadblock."

Then how was a workaround even possible?

Forensics expert Oleg Afonin had the message: A $39 Device Can Defeat iOS USB Restricted Mode. He blogged this on Monday in the ElcomSoft site.

First, this is what is supposed to be the case.

"If anything, an iPhone in USB Restricted Mode acts as a dumb battery pack: in can be charged, but cannot be identified as a smart device. This effectively blocks forensic tools from being able to crack passcodes if the iPhone spent more than one hour locked. Since law enforcement needs time (more than one hour) to transport the seized device to a lab, and then more time to obtain an extraction warrant, USB Restricted Mode seems well designed to block this scenario."

OK, then here is what Alfonin found. In tests the USB Restricted Mode was fooled, in that an accessory device connected would reset the one-hour timer. The USB Restrictive Mode would be stopped from turning on. Mayo walked *9to5Mac* readers through ElcomSoft discovery, that "any USB accessory can be plugged into the iOS device within the hour safe window, and this prevents the timeout from ever being reset."

Mayo said, "law enforcement agencies simply need to connect the phone to an accessory as soon as the suspect is apprehended, and leave it connected as they transport the device to a facility for data extraction." Meantime, Mayo also made a useful

point. "What ElcomSoft describes isn't a vulnerability per se, it's just a relatively straightforward workaround for how the feature works," Mayo said.

In Alfonin's own words: "We performed several tests, and can now confirm that USB Restricted Mode is maintained through reboots, and persists software restores via Recovery mode. In other words, we have found no obvious way to break USB Restricted Mode once it is already engaged. However, we discovered a workaround."

In the blog, Alfonin commented that "The ability to postpone USB Restricted Mode by connecting the iPhone to an untrusted USB accessory is probably nothing more than an oversight. We don't know if this behavior is here to stay, or if Apple will change it in near future."

More information:
blog.elcomsoft.com/2018/07/thi … usb-restricted-mode/

APA citation: Researcher blogged about workaround for Apple OS update's USB Restricted Mode (2018, July 11) retrieved 18 July 2018 from https://techxplore.com/news/2018-07-blogged-workaround-apple-os-usb.html