
***Issued 7/12/18***

## Apple's iOS Passcode Cracking Defense can be Bypassed using a USB Accessory

Apple released iOS 11.4.1 this morning, and with it came a new software mechanism that blocks passcode cracking tools favored by law enforcement. Called USB Restricted Mode, the tool renders the iPhone inaccessible to third-party software of any kind after its screen has been locked for one hour. That way, malicious third parties or law enforcement agencies can't break into the phone using passcode cracking tools like GrayKey. However, researchers at cybersecurity firm ElcomSoft have found a loophole that resets the one-hour counter so long as you plug a USB accessory into the iPhone's Lightning port, regardless of whether the phone has ever connected to that accessory in the past. Here's ElcomSoft's Oleg Afonin explaining the situation: "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. What we discovered is that iOS will reset the USB Restrictive Mode countdown timer even if one connects the iPhone to an untrusted USB accessory, one that has never been paired to the iPhone before (well, in fact the accessories do not require pairing at all). In other words, once the police officer seizes an iPhone, he or she would need to immediately connect that iPhone to a compatible USB accessory to prevent USB Restricted Mode lock after one hour. Importantly, this only helps if the iPhone has still not entered USB Restricted Mode." Afonin says you can even use Apple's own Lightning to USB 3 Camera adapter, which goes for $39 on the company's online store. (Afonin notes that the $9 Lightning to 3.5mm

adapter does not work, however.) ElcomSoft is apparently in the process of testing other adapters, including cheap third party ones, to see which reset the counter.