Issued 2/15/17

Stolen Apple IDs can hold your iPhone Hostage

There is a huge, thriving underground economy involved in the theft, sale, manufacture and abuse of Apple IDs, Palo Alto Networks researcher Claud Xiao told the BSides SF hacker conference in San Francisco. "The problem is, Apple IDs are used with too many services," Xiao said as he showed a slide listing 20 different Apple services accessible with an Apple ID, including the App Store, Apple Music, the Apple Online Store, iCloud, Find My iPhone, iMessage and the Mac App Store. "Every feature can be abused to make a profit." He explained that Apple IDs can be exploited to squeeze money out of almost any aspect of the Apple ecosystem, from deceiving users with spam Apple Messages, to locking users out of their devices and demanding ransom, to artificially pumping up the user ratings of dodgy apps so that they rank in the Top 10 on the App Store.

Worst of all are the scams in which a stolen Apple ID is used to lock the legitimate user out of his or her own device, by resetting the password and activating the Find My iPhone lock until the user pays a fee, usually $100 or so. The process holds the iPhone for ransom without the iPhone ever leaving the victim's possession. There are many ways to steal Apple IDs, Xiao said. He displayed a well-done phishing email that looked as if it had come from Apple, asking the user to verify his account by clicking a link in the message. Other phishing scams involve text messages, again telling the recipient that he or she needs to "confirm your Apple ID" by clicking on

links to Apple-sounding websites, such as mysecureicloud.com or support-appleid.com.

Some phishing scams are used by iPhone thieves to defeat Activation Lock on stolen iPhones, deliberately targeting the legitimate users by telling them that their devices have been found and that they need to log in remotely using their Apple IDs. Most of these "spear phishing" attempts come via email or SMS, Xiao said. One owner of a stolen iPhone, Xiao said, ignored hundreds of such emails and text messages but finally fell for a phone call that displayed the number of a known Apple support line when it rang. The caller pretended to be from Apple, asked the user to answer the standard security questions, and then sent the user to a phishing site that tried to steal his password.

Malware also tries to steal Apple IDs, Xiao said, listing three different iOS malware families of the past two years that stole Apple IDs en masse. Because countless users reuse passwords and email addresses for many online accounts, any massive breach of account credentials from a large online service (such as the Yahoo and LinkedIn breaches disclosed in 2016) will result in thousands, if not millions, of stolen Apple IDs. And some scammers don't even steal Apple IDs — they make new ones in batches of hundreds or thousands, then sell those IDs on the black market. Those IDs are valuable because they can make scammers money. Spam advertising deep discounts on fashionable items appeared in iPhone users' Messages and iCalendar apps during last year's holiday shopping season.

More lucrative is using stolen Apple IDs to artificially boost the popularity of App Store apps by making nonexistent purchases and writing phony glowing reviews. Xiao showed a price chart that offered to boost an app into the top 10 in the U.S. App Store for $16,000. He pointed out that one fake antivirus app, named after a well-known Norse god, made it to No. 3

among paid apps in the App Store, even though the app is really "scareware" that fakes infection in order to prove its own worth. (That app is still in the App Store, even though Apple says it doesn't let antivirus apps in.)