Issued 8/14/17

Facebook Password Stealing Software

Facebook malware is nothing new, but an emerging threat offers some unique karmic retribution. In an unpublished report, security researchers at Sydney-based LMNTRIX Labs have identified software advertising itself as a Facebook password stealer that injects malicious code in the background once downloaded, making the user vulnerable to having their own credentials stolen. "This appears very widespread and growing," the research team told TechCrunch. "We classified this as an ongoing malicious campaign with the threat actors actively marketing it as 'Facebook Password Stealer' or, more innocuously, 'Facebook Password Recovery.' "The attackers also seem to be sophisticated marketers who understand there is potentially big demand for the purported service and are distributing the sample via Spam, Ad campaigns, Pop-ups, Bundled Software, Porn sites and also some times as a standalone software."

Fittingly dubbed "Instant Karma" by the LMNTRIX researchers, the malware campaign lures victims who are seeking software that can crack into other people's Facebook accounts. Once downloaded and run, it drops a remote access trojan in the background after the victim clicks the "hack" button. The researchers cross- referenced the contents of "spoolsvfax.exe" with VirusTotal's database, where they identified it as containing a newly uploaded trojan. Before identified and neutralized, Facebook malware that offers useful (if sketchy) services often thrives thanks to Facebook's incomparably massive user base. It can take many

forms, from tempting downloads that offer to notify a user when they are unfriended to malware bots posing as a friend on Messenger.

A simple search of "hack Facebook account" yields pages of results and links to all manner of likely malware-tainted software solutions, many of which are targeted toward the average user, no technical skill required. This particular threat appears limited to Windows desktop users, though malware targeting Facebook's mobile experience isn't uncommon either. It's no surprise that the largest social network in the world is a hacker goldmine if tricks like these can be leveraged successfully. "The target market goes beyond a typical hacker subset (if there is such a thing) and targets the general user who may be tempted to get inside someone’s Facebook account (friends, enemies, significant others, et al.)," the researchers told TechCrunch. "While there have been methods and apps offering Facebook hacks, this specific malicious campaign which uses the promise of easy Facebook password theft as bait is completely new."