Security Manual Reveals the OPSEC Advice ISIS Gives Recruits

0 0 0 2
December 8, 2015

This article comes from wired.com

by Kim Zetter

In the wake of the Paris attacks, US government officials have been vocal in their condemnation of encryption, suggesting that US companies like Apple and Google have blood on their hands for refusing to give intelligence and law enforcement agencies backdoors to unlock customer phones and decrypt protected communications. But news reports of the Paris attacks have revealed that at least some of the time, the terrorists behind the attacks didn't bother to use encryption while communicating, allowing authorities to intercept and read their messages.

Reports in France say that investigators were able to locate some of the suspects' hideout this week using data from a cellphone apparently abandoned by one of the attackers in a trashcan outside the Bataclan concert hall where Friday's attack occurred, according to Le Monde. Authorities tracked the phone's movements prior to the attack, which led them to a safehouse in a Paris suburb where they engaged in an hours-long shootout with the other suspects early Wednesday. These would-be attackers, most of whom were killed in the apartment, had been planning to pull off a second round of attacks this week in Paris's La Defense business district, according to authorities.

Other reports indicate that a previous ISIS terrorist plot targeting police in Belgium was disrupted in that country last January because Abdelhamid Abaaoud—suspected mastermind of both that plot and the Paris attacks—had failed to use encryption. He also carelessly left behind a cellphone in Syria, which contained unencrypted pictures and videos, including one now-infamous video showing him smiling from a truck as he dragged bodies of victims through a street.

All of this suggests that the attackers were guilty of major OPSEC failures—that is, if it weren't for the fact that some of them still managed to pull off the Paris attacks without prior detection. This suggests they either did use encryption during earlier planning stages of their attacks, or that authorities were so overwhelmed tracking other suspects—French investigators claim they recently thwarted six other attacks

—that they overlooked the suspects who pulled off the Paris attacks. This indeed might be the case since Turkish authorities have said they tried to warn French authorities twice about one of the suspects but never got a response.

Despite this, US authorities have flooded the media this week with stories about how ISIS' use of encryption and other anti-surveillance technologies has thwarted their ability to track the terrorists. But authorities have also slyly hinted that some of the encryption technologies the terrorists use are not as secure as they think they are, or are not being configured and used in a truly secure manner. So what exactly are ISIS attackers doing for OPSEC?

It turns out that a 34-page guide to operational security (.pdf) that ISIS members advise recruits to follow, offers some clues. Aaron Brantly and other researchers with the Combating Terrorism Center at West Point's military academy uncovered the manual and other related documents from ISIS forums, social accounts and chat rooms. The originals are in Arabic, but the center provided WIRED with translated versions of a number of documents that had been passed through Google Translate.1

The guide was originally written about a year ago by a Kuwaiti security firm known as Cyberkov to advise journalists and political activists in Gaza on how to protect their identities, the identity of their sources and the integrity of information they report. But members of ISIS have since co-opted it for their own use as well.

Read more here.

Categories: All, Featured