

Push to Stalk : The Latest in Mobile Technologies

Around 5 minutes into every conversation I have involving my profession, I am asked the question *"Is mobile malware really an issue?"* in some form or the other.

The goal of my presentation is to address that very question with some facts and real world examples.

With smartphones getting smarter by the day, a modern day cellphone presents an attacker with the perfect attack scenario - a device that the victim carries around at almost all times that stays connected to the internet.

And if that wasn't enough, throw in a GPS, a camera and a microphone and you have the perfect spying device. Move over James Bond, there's a new sheriff in town.

Moreover, you don't need to be a diabolical criminal mastermind either to sniff out the opportunity to exploit that.

Attack vectors: Most of the malware we see disguise themselves as a plethora of useful applications ranging from wallpapers and games to battery/power enhancement applications to even the classic 'Fake AV' trick.

Motivations/Rewards: Apart from spying, as I explained above, many malware are designed with the motive of making money. In the simplest example, this can happen by sending out SMS messages to premium numbers from the infected phone. On the other end of the spectrum, the most potentially 'harmful' examples we've seen so far have been Trojans that steal/forward Banking Tokens received on the victim's phone. These tokens were introduced by banks as a second factor of authentication to verify the legitimacy of transactions. As a result, pro-active attackers are now using mobile Trojans in conjunction with traditional PC malware to carry out fraudulent banking transactions from infected victims' accounts.

By means of this presentation, I plan to provide you with uncensored information on this new frontier of mobile malware that attackers are exploring.

Most of all, I would like to take this opportunity to demonstrate in real-time their working, and how well-hidden and effective some of these attacks are.