Advanced and In-Depth Persistent Defence

Posted on **March 26,2018** by **lynx**

Image not found
http://blog.lynxbee.com/wp-content/uploads/2018/03/Two-dimensional-space-depicted-in-three-dimensional-spacetime.-300x300.png

Two-dimensional space depicted in three-dimensional spacetime.

The attribution problem in digital attacks is one of these problems that get solved over and over again. Of course, there are forensics methods, analysis of code samples, false flags, mistakes, and plenty of information to get things wrong. This is nothing new. Covering tracks is being done for thousands of years. Why should the digital world be any different? Attribution policy tactics, APT, is part of the arsenal and thus part of the threats you are facing. It has less impact though, because it is only of interest when your defence is breached – and this means you have something else to worry about.

Attribution is not useful for defending against threats. While you can use to to „hack back“, this will most probably not help you at all. The main problem with attribution is, that it is not your first priority. The Internet is not the ocean, and your servers aren't line ships that exchange broadsides. So you should be a lot more worried about intrusion detection and prevention. IDS/IPS have been around for some time. It's the best place to start for improving your defence. Switch the radar on, tune in to reduce the noise, observe, and learn. Attacks won't come through walls. Adversaries usually use open doors. Just as in physics, interactions are the key. That's what you should focus on.

Speaking on interactions: DeepINTEL 2018 will focus on sophisticated threats, how they work, what traces these incidents leave, how defence can match well-prepared attacks, and what you can do in order to not get distracted. The call for papers is still open. Let us hear your thoughts.
Posted in:Discussion,Security Intelligence | Tagged:DeepINTEL,Mindset,SecInt,Security | With 0 comments