Disinformation Warfare – Attribution makes you Wannacry

Posted on **May 16,2017** by **lynx**

After the Wannacry malware wreaked havoc in networks, ticket vending machines, companies, and hospitals the clean-up has begun. This also means that the blame game has started. The first round of blame was distributed between Microsoft and the alleged inspiration for the code. The stance on vulnerabilities of security researchers is quite clear. Weaknesses in software, hardware, protocols, or design needs to be documented and published. This is the only way to address the problem and to give the defenders a chance to react. The discussion about how to deal with the process is ongoing and will most likely never come to a conclusion. What about the source of the attack?

Attribution is hard. Knowing who attacked has become increasingly difficult in the analogue world. Take any of the conflicts around the world and have a look. There is no clear picture of who did what exactly for which reason. When it comes to *cyber* warfare you basically have to deal with lots of disinformation. We have had many talks about the use of the Internet and other networks in digital skirmishes. Routing data via a different set of connections is the core property of the Internet. You cannot trace the trajectory of a projectile. You can only rely on the forensic analysis of the attack (and even this is disputed since forensic software can be manipulated) and on data you see in network interactions. Deception is the basic ingredient of any attack. The glorified open field battles where people run at each other screaming is not what you can expect from real situations.

There are speculations that Wannacry was launched by North Korea. Russia, China, and North Korea are the default origins any analysis starts with (the only exception being Stuxnet for obvious reasons). Most people forget that false flags operations are a common military tactic. There is an easy recipe to fake an attack. Want to look like APT28? No problem. Need a specific origin for your reconnaissance? That's what the *cloud* is for! You can also use the vast archive of malicious software as a starting point. The code, contrary to the truth, is out there.

Getting intelligence right is as hard as getting the attribution right. It's not impossible, but you have to keep this in mind when reading the news about incidents such as Wannacry or others. The last attack didn't even take advantage of the Internet of Things. Imagine that! We have just seen a glimpse of the future. If you want to prepare yourself for what's next, you need to get your intelligence right in addition to your security. Why not join us in September for DeepINTEL and think about strategies for the future?

Posted in:Discussion,High Entropy,Security Intelligence | Tagged:Attack,Cyberwar,DeepINTEL,Mindset | With 0 comments