The Sound of „Cyber“ of Zero Days in the Wild – don’t forget the Facts

Posted on **January 26,2017** by **lynx**

The information security world is full of buzzwords. This fact is partly due to the relationship with information technology. No trend goes without the right amount of acronyms and ~~l~~eetspeaktechnobabble. For many decades this was not a problem. A while ago the Internet entered mainstream. Everyone is online. The digital world is highly connected. Terms such as *cyber*, *exploit*, *(D)DoS*, or *encryption* are used freely in news items. Unfortunately they get mixed up with words from earlier decades leading to *cyber war(fare)*, *crypto ransom(ware)*, *dual use*, or *digital assets*. Some phrases are here to stay. So let's talk about the infamous *cyber* again.

In case you have not seen *Zero Days* by Alex Gibney, then go and watch it. It is a comprehensive documentary about the Stuxnet malware and elements of modern warfare (i.e. remote sabotage of infrastructure). Given the secrecy of the incident / operation it is the best compilation of facts and their non-existence up to date. No matter what you think of people using the word *cyber* for a variety of meanings digital warfare is here to stay. In essence it is an attack on communication and control infrastructure. Manipulating systems connected to physical devices has always been used for disrupting the Things without Internet. Cut a pipe(line), block a spinning wheel, loosen some screws, and there you go. Instant analogue sabotage. Using the benefits of modern connected industrial controllers turns this into digital sabotage – *cyberwar*. Like it or not, talking about semantics won't help. The fact is that modern communication networks and the networked infrastructure is now being used for political, military, academic, entertainment, education, (organised) crime, business, cultural and multimedia purposes. This list isn't even complete (and don't worry, terrorism is already included in the list).

Reality has shifted the border between now and (science) fiction. If you want to deal with modern threats to your data and flow of information, then you need to catch up. Urgently, that is. To set the tone for 2017, here is a quote by Richard A. Clarke from the interview he gave for *Zero Days*.

> *„I'm old enough to have worked on nuclear arms control and biological weapons arms control and chemical weapons arms control. And I was told in each of those types of arms control, when we were beginning, "it's too hard. There are all these problems. It's technical. There's engineering. There's science involved. There are real verification difficulties. You'll never get there." Well, it took 20, 30 years in some cases, but we have a biological weapons treaty that's pretty damn good. We have a chemical weapons treaty that's pretty damn good. We've got three or four nuclear weapons treaties. Yes, it may be hard, and it may take 20 or 30 years, but it'll never happen unless you get serious about it, and it'll never happen unless you start it.…“*

That's one way of putting it. There are different perspectives. However no matter how you look at it, systems get attacked and compromised. That's what you can see when you work with and in IT departments. Once you use networks, the threats will become part of your job description. Call it *cyber* if you like, but always include context and additional information. We need the facts. For 2017 we like to revisit the threat landscape and address the security implications with scientific accuracy. DeepINTEL will be the first event, DeepSec will follow. And we would like you to join us.

Posted in:Discussion,High Entropy | Tagged:Attack,Defence,Internet | With 0 comments