# Video – Breaking Down Stuxnet (3 min)

You know when it comes to security news, It's always puzzling what gets reported. As viewers of this show, you know there's a very regular rhythm of security issues that are always bubbling just below the surface and it takes something truly profound to grab the public's attention. Well one new threat making the rounds did have the right mix of ingredients last summer. Stuxnet. I mean it makes sense, right? Computer attacks, nuclear power. Foreign governments, sabotage. Spy versus spy, but how much of it is real? Enough to say it's a sign of the times.

Now as all good threats, the details will continue to evolve, but I do think that there are five items worth paying attention to here. the first one, non-trivial distribution. Primarily spread via USB sticks. Think non-internet connected systems that then propagate by escalating privilege levels through zero day exploits, notable for the fact that true zeros are special and they're only valuable for a short period of time. Very expensive, very hard to come by. The next one, sophistication. This is an intelligent worm. Initially targeting Windows computers, where it even installs its own drivers using a stolen but legitimate certificate. The offending certificate gets revoked of course, but then another one gets added within 24 hours. Our third point, modular coding. This thing can get new tires while still on the road. Multiple control servers. First in Malaysia, then Denmark, now more, including peer-to-peer. In fact, when two run into each other, they compare versions and make sure that they're both updated. Fourth point, unique targeting. Windows is just the intermediary, the friend of the friend. Stuxnet is looking for a particular model of PLC. That's programmable logic controller, which is technically not SCADA as it's often reported. These are small imbedded condustrial control systems that run all sorts of automated processes, from factories to oil refineries to nuclear power plants. Stuxnet will leverage the vulnerability in the controller software to reach in and change very specific bits of data. Shut things off. Don't grease a bearing for 10 minutes. Don't sound an alarm. This is really unique knowledge. Respectable coding skills that imply a higher level of patience of good funding resources. Our final point, motive. Stuxnet does not perform... Excuse me. It does not threaten. It performs sabotage. Really has no criminal focus. Does not spread indiscriminately or steal credit card information or login credentials. It does not recruit systems into a botnet. It targets infrastructure, our most essential necessities like power, water, safety and much, much more. You know these are older systems. Very established. Generally run with the mentality of hey, if it ain't broke, don't fix it. These things don't get watched over and patched by technical handlers who understand these kind of things. Not yet anyway. So stay tuned. This one is not done. We all have a lot to learn and somebody is working hard to teach us.