All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Is your threat intelligence intelligent?

Threat Intelligence is a rising buzzword in cybersecurity. Vendor-supported intelligence feeds have been around for at least 15 years, but today, flows are bigger and faster, and the challenges more daunting. There is a yet unmet expectation that intelligence feeds will turn into automated interdiction, and that's where the heat is being turned up.

Remember self-defending networks?

There are many names for the claims. Automated immune system, self-defending networks, intelligent defenses, etc. While nobody disputes the desire to turn intelligence into action, but the reality is that we're not there yet. What we increasingly see is automation for information sharing between people. Someone identifies an activity that is malicious, feeds the details into a computer, the data gets shared through an information sharing organization, results are available as feeds to members, and decision-makers act on the feed it if it's right for them.

The pipes are too big for the valves

Information overload is already here. Daily there are tens of thousands of new pieces of malware in some feeds, thousands of “indicators of compromise” (IOCs) in others, and a lack of the piece parts to turn this into actionable intelligence. Effective insight into the campaigns (who is doing what) and tactics, techniques and procedures of higher value than IOCs, but it's far harder to develop. Policies defining who shares what with whom are too complex to be useful and too immature for standardization. And the pipes don't yet fit together, so trying to connect them is still an interface nightmare.

But even if we had all the right pipes and pipe-fitting, we face the far bigger challenge of what to do with all the data. If you are seeing attacks from an identifiable source against an identifiable target type using an identifiable method, in theory I should be able to interdict it as soon as I know about it by cutting off the path from the source to my relevant targets. But in reality today, the process is largely manual, we don't have inventory systems to identify what's important, and if we did we don't have the means to act without manual efforts. And of course there is reflexive control and issues of trust that have to be dealt with.

The year of the brain

It seems simple enough to make a database that identifies the things I have, looks for those things in your feeds, and stops the things you identify before they harm me. It should take a few seconds. With automated detection and response, the time from initial attack to final defense should be just that quick. 2016 looks like it's the year we start to deploy this concept. Interoperability demonstrations are planned with limited automated intelligence starting to operate. It won't be all that intelligent, but it's a start.

Summary:

Artificial intelligence it is not. But it's not natural stupidity either. Automated fusion and analysis of commensurable data is what we need, and 2016 is the year we will start to see it. It won't stop the APT attacker or the authorized insider. But at least it can stop the mass attacks.

