BIZCOMMUNITY

What advanced threat technology actually look like

By Sam Curry

29 Sep 2015

Two facts: an infrastructure breach is inevitable due to a fundamentally intelligent, human opponent; and the real mission for security personnel, until such time as we create true artificial intelligence, is to prevent information breaches.

The goal, therefore, is not to create another generation of technology that got trapped in the inevitable content race of any purely technology play, but rather to enable defenders to stand up and win the race against attacks over and over again. This begs the question of what's needed to support this team of people, and ultimately what does an 'advanced threat' technology actually look like.

Sam Curry

Let's start with support for the humans who fight to protect information. To do that, I will draw on a simple analogy: a child learning to write.

When a child learns to write, there is a tremendous amount of frustration. The mechanical skills of writing get pulled to the front before anything else. The knuckles go white. The sweat breaks out, and torturous letters slowly appear on a page. At this rate, it's impossible, even when assuming excellent language skills, for a child to write a long, insightful dissertation. The same is true of an adult learning to type later in life.

Impossible task

The reason for this is that all the energy of the potential writer is going into how to write rather than into what is being written. The mistake here is to think of this as merely subtractive from the time available to write. It doesn't just make the task longer; it makes the task utterly impossible. It doesn't matter how much time you give our hypothetical child or adult; until they master the tools, they won't advance the object to which it is applied.

For too long, this has been the single biggest obstacle to security departments. Right off the bat, we have to have the means for security practitioners to apply their knowledge to their craft without focusing on how they do this. The tools for working events and incidents, for collaboration, for learning over time and for thinking, leaping from high-level idea to high-level idea with crashing down to the mundane questions of how to get data or how to collaborate, are critical.

So let's say that data mining tools, traffic analysis tools, work-flow management tools, and then the pairing of this to risk insight, business data and having contingencies ready for making decisions and carrying out plans, all have to exist. Then we can talk about advanced threat tools.

The existing perimeter and endpoint technologies have failed. The reason for that failure is inevitable: intelligent opponents by default create their attacks and tools to bypass the basic security kit in organisations.

Important tools

Now, this does not mean that anyone should throw out firewalls and anti-virus, or at least not for the foreseeable future, they remain important tools for stopping basic threats and for filtering some of the noise. They provide layers that slow down (but don't stop) attackers and buy time in the race to protect information, but they are not where the focus of any security department should be in actually stopping attacks.

There's a new generation of technologies emerging claiming to be 'advanced threat' products from white-listing and micro-virtualisation to network behavioural analysis and payload sand-boxing. Which of these is just young technology and which is truly advanced? To tell that, we have to first define what is an advanced threat product (as opposed to what is a new, young but fundamentally basic threat product).

An advanced threat is one that is designed to, by default, evade and not be caught by existing machine-based security technology and controls for a sufficient window of time, enough so that it can only really be stopped by human beings.

Significant edge

By definition, this means that advanced threat solutions have to give a significant edge in reducing the window of opportunity available to attackers by in some way shortening the defenders timelines or making them meaningfully more efficient at processing events.

This means that an advanced threat solution should survive the following inevitable challenges:

- **Legitimate software evolution**: Advanced threat solutions must weather changes in how legitimate software evolves over time to take advantage of new features and new techniques, even when some of those come from the bad guys.
For example, back in the day, key loggers were defined as 'anything that shims the keyboard' because nothing legitimate did this. In the 2003 time-frame, the technique crossed the line as a development tool, and all the world's IM vendors started shimming keyboards and setting off false alarms.

- **Malware evolution**: This might seem obvious, but I have seen countless products claim to have 'foolproof' behavioural analysis for spotting bad behaviour. What they actually have is something with a shelf life because bad guys adapt. This means that advanced threat solutions must weather changes in how illegitimate software evolves to look normal over time.

If a technology becomes successful, and winds up in the same situation with ineffective content races as the traditional kit,

then I have news for the vendor: you're just 'new', not advanced. Content updates aren't a bad thing in and of themselves, but they have to be a meaningless sop to deal with the malware evolution bullet above.

They have to really help make people more effective at stopping attacks: pull the needle from the haystack, find new needles, process needles faster, enumerate the damage done by needles more quickly, and equip teams to deal with the aftermath of the needle quicker and better.

ABOUT THE AUTHOR

Sam Curry is Chief Technology and Security Officer at Arbor Networks