All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Deception Rising Again

In 2002, as part of the "Managing Network Security" sequence of analyst reports, I wrote "Deception Rising".[1] I summarized (a paragraph) by stating: "In short, it looks like deception is a technology on the rise." It's 16 years later now, and finally, I am right!

In more ways than I wish were true

At its basis, deception is cognitive[2] in nature. Done well, it attacks the cognitive system of the intended target(s) by inducing and/or suppressing signals so as to alter the behavior of the target to favor the deceiver. Of course we see this in politics and it appears to be rising despite the incredible technology that allows us to record and almost instantly play back almost anything these folks say and do. It seems like objective truth is being challenged even as we have more and more objective sensors and capacity to clearly demonstrate the lies.

For technical cyber defense

That example is about the offensive side of deception, in which deception is used to influence people against their own well being (in many cases). The deception rising for defense is a very different story. While it is still based on cognitive exploitation, the exploitation is against those who would seek to break into systems. This includes both people and the mechanisms people device and deploy to attack. A simple attack example is a network scanner used in the intelligence gathering (exploration) portion of an attack (explore, penetrate, expand, exploit). By giving different responses to authorized and unauthorized parties, unauthorized party cognitive mechanisms produce faults (wrong answers) that result in failures (undesired outcomes for the attackers). This particular process is usually indirect in nature, so that the attacker consumes resources aiming and firing at the wrong target.

How is deception rising exactly?

In looking at the emerging global cyber security market, per the claims of some vendors, the demand for buying technical deception for defense has tripled in the last year. Depending on the specific technology involved and the volume of sale, the market is settling into the same sort of mode as computer virus defenses did as it became popular and widespread, but not ubiquitous. The price seems to be something like $10/system/mo for each solution PLUS from $10,000 to $50,000 for the central control to manage it on an enterprise level. The emergence of cloud-based controls will likely translate into a cost of $10/system/mo for central control for small end user groups willing to share the central control with all of the other customers using the cloud-based solution and have controls run over the Internet. This represents a leveling off of price as volume reaches the millions of endpoints per company similar to the same leveling off in the computer virus defense space at a similar level in the early 1990s. If you sold 2 million units last year and are selling 6 million this year (tripling) that translates to $72M in revenues for one substantial company. Note then that the valuation for such a company is likely in the $100M-$150M range today, also tripling what it was a year ago.

1 http://all.net/Analyst/netsec/2002-09.html
2 i.e., concerned with the act or process of knowing, perceiving, etc. - per dictionary.com

How many are there?

There are many different approaches to deception for defense and in each niche, there are multiple players. To date, I have found no example of a defender buying more than one deception technology of the same sort for the same endpoint. They may buy a network facing stealth defense (e.g., you cannot see the endpoint unless you have the right “code”) or a network facing noise defense (e.g., a mechanism that creates false returns from intelligence processes and perhaps even responds at volume by adding stealth to targets from the source of the threat), but they don’t yet buy more than one for the same endpoint. I have also seen no example of a company buying internal deception defenses along with the external defenses except in cases where the same vendor offers both functions from the same platform. Unified control is also an issue, and in deception-based defense it is particularly important because of the potential for defenses fooling each other.

There are at least a dozen network deception defense companies in the marketplace today, with sizes running from the millions of units deployed to early stage companies with no or almost no substantial customers and less than $1M revenue. On the other hand, major players like Cisco, Microsoft, and HP are all using and in some cases licensing the technology from the smaller providers. As more niches come to be and are filled, this looks like a market that will continue to grow at increasing space for at least 3-5 years before the next generation of embedded implementations shows up and the technology becomes ubiquitous.

Then what?

The current round of evolution appears to be in the network-level defense on endpoints, but you can reasonably anticipate router and switch technology adding this capability for the network and embedded deceptions at the operating system and hardware level following in their expansion over time. Embedded systems are also starting to see security technology and it seems likely that IoT technology will also start to see deceptions as part of the embedding of security in these devices over time.

How big and when?

We’ve seen this movie before. Technical deception for defense is starting to accelerate. Like the early days of virus scanning, the early days of firewalls, and the early days of identity management, the niches are starting to appear, the price has dropped to the level associated with millions to tens of millions but not hundreds of millions or billions of deployed instances. Initial opposition is withering in the face of demonstrated protective value and improved enterprise efficiency, and we are now beyond the point of “beading edge” and well into the “early adopter” stage. Within a 5 years this should enter the phase where it is standard fare with economy of scale pricing (perhaps $1/mo/endpoint for 100,000 endpoint license) and general acceptance with hundreds of millions of protected endpoints (~$10B TAM).

Conclusion

Deception for defense is rising, and rising quickly. Like most such things, it is an overnight success after 20 years. But also like so many other similar things, the market is becoming predictable and mature as the knee point for deception technology is now reached for the largest providers. In the US, the EU, and emerging elsewhere, the technology is being accepted, being used, and proving effective for changing the equation between attack and defense.

