Deception Technology

What is it?

Deception technology is the cyber-defense strategy that detects, analyzes and prevents unknown and advanced attacks by means of deception. It is based on baits that mimic legitimate assets, and are designed to make the attacker believe he has found vulnerable paths in the target infrastructure. Baits are designed so that they misdirect the attacker, drive him away from real valuable assets, alert the defender of the attack, and give the defender the opportunity to analyze the attack and design better defensive measures.

Who is it directed at?

Deception technology is addressed to environments that are threatened by highly skilled attackers, stealth or passive threats, insiders and other hard-to-detect threats. Critical infrastructures and user networks where users can be easily fooled by an attacker (eg by means of social engineering) use deception solutions to identify attacks that bypass other security measures. Deceptive baits look like all those things that an attacker is really after, and therefore detect the attack based not on the process followed to gain access or exploit a system, but on the asset the attacker wants to compromise.

Why is it important?

Deception is not just a products category, it's a strategy. Traditional security defense approaches can defend only against what they know, either based on signatures, training sets of attack data (AI) or deviations from the norm (Behavioral Analysis). Deception allows the identification of unknown attacks by creating a fake reality for the attacker to exploit, but without adding any risk to the real infrastructure. With deception defenders can detect with zero-rate of false positives, not only the attackers that try to get into the network, but also those who have managed to bypass traditional security mechanisms and are already in the defender's premises. It's the only way to detect what can not be seen.

Where is it taking place?

By using modern deception platforms such as Neurosoft's Illicium, companies are able to deploy their deception strategy throughout their infrastructure with ease. Those platforms allow the defenders deploy a large number of sophisticated baits, increasing the chances of detecting high-risk threats. Through a unified interface, the defender has full management over the deception deployment. Cyber Deception can be deployed in any deception layer – network, endpoint, application or data – detect and interrupt the attacker at any stage of his attack – recon, gain access, escalate privileges, persistence, lateral movement, even in the exfiltration stage.

When is it going to make an impact?

The need to incorporate deception in a corporate security strategy is real. There is a large number of threats that other approaches will never be able to detect. Many enterprises have already identified the value of deception and incorporated a deception solution in their infrastructure, bringing a total revenue of more than $100 million in 2018 to the companies that develop deception solutions. Gartner noted deception technology as a "far underutilized technology that can provide serious advantages over attackers". Analysts estimate a market size exceeding $1 billion by 2020, and cumulative deception technology market value at $12 billion (2017–2022), growing at about 19% CAGR.

How will it affect your business?

Whether through a simple scan or an attempt to download malware, once an attacker goes after a bait, it is safe to observe what they do in a contained environment. In most cases, when an attack is detected, the right thing to do is shut the attack down immediately. But with deception you have the option to first watch what is happening, learn more about the nature of the attack, and better understand the way that the attackers intend to spread through your business. Through deception, security analysts can observe attackers in a safe manner because the assets under attack are designed to trick an attacker into thinking they are escalating their attack. You can therefore engage an attacker and then use this threat intelligence to activate countermeasures.