TrapX Security, Inc., 3031 Tisch Way, 110 Plaza West
San Jose, CA 95128

+1–855–249–4453
www.trapx.com

# DECEPTION AS A SECURITY STRATEGY

*By: Boyd Brown*

***On August 2, 1991, Iraq invaded Kuwait in a two-day operation to seize Kuwait's oil fields and establish Kuwait as Iraq's 19th province. As the Coalition forces deployed, military press conferences focused on US Marine and Coalition naval actions in the Persian Gulf, as well as other indicators that the Coalition would attack directly into Kuwait, caused the Iraqis to concentrate their defenses on the Kuwaiti beaches and border with Saudi Arabia. Iraq wrongly believed their western flank was secure, as they discovered when three Coalition armored corps appeared out of the supposedly impassable western desert. The Iraqis' misunderstanding of the direction and timing of the Coalition ground attack, combined with Coalition use of emergent technology such as the Global Positioning System, stealth aircraft, and ship-launched cruise missiles allowed the Coalition to defeat the entrenched Iraqi Army in fewer than four days.***

Throughout the history of warfare, armies have employed surprise and misdirection to confuse and outmaneuver their opponents, transforming defeat into victory. Deception is not a tool of last resort, employed from a position of weakness, but instead provides deceivers with the ability to conserve their resources by causing adversaries to expend time and energy against false targets. Deception quite literally alters the enemy's understanding of reality, allowing the deceiver to seize the initiative even if they are in the defense. For those readers who may not be familiar with deception in warfare, deception also plays a prominent role in sports. The bunt, the onside kick, the old Statue of Liberty play, the fake handoff, and the bicycle kick are all examples of misdirection that give the deceiver an advantage because his opponent's understanding of reality has been compromised.

# CHALLENGES IN THE NETWORK SECURITY ENVIRONMENT

IT networks pose the single greatest security vulnerability to most businesses because of the ease with which they can be penetrated, the sensitivity of the data they store, and their criticality to day-to-day operations. Cyber attackers use anonymity and a wide variety of software tools to gain access to your most valuable data, constantly working to penetrate networks to implant ransomware, steal money and intellectual property, corrupt data, and use your networks as a launching point to access other businesses. Network security breaches occur thousands of times every day, costing hundreds of millions of dollars in lost revenue and intellectual property, damaging brand reputations, and reducing customer and business partners' faith in your ability to keep their data secure. Cybercrime damages are predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. While cybercrime insurance may offset some of the immediate costs of a network security breach, the less tangible and longer-term financial impacts of a security breach may never be recovered. Well-trained, diligent CISOs and SysAds set out to defeat these attacks every day, yet networks are still penetrated and data breaches still occur. In most cases, it's not a question of whether a penetration will occur, but when and how severe the impact will be.

[1] Cybercrime Magazine, "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021," https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

# DECEPTION AS A NETWORK DEFENSE STRATEGY

There are many obvious parallels between competition in the physical world and in cyberspace, and cyber attackers seem to hold many advantages, hiding behind false identities and choosing the time and method of their attacks. Just as military units use deception to conceal their true location, obfuscate their adversary's view of the battlefield, and cause them to expend valuable time, energy, and resources against targets that don't really exist, the same can be accomplished in cyberspace. Deception provides cyber defenders with a powerful tool to counter many of the attacker's advantages by detecting, deceiving, and ultimately defeating their attack.

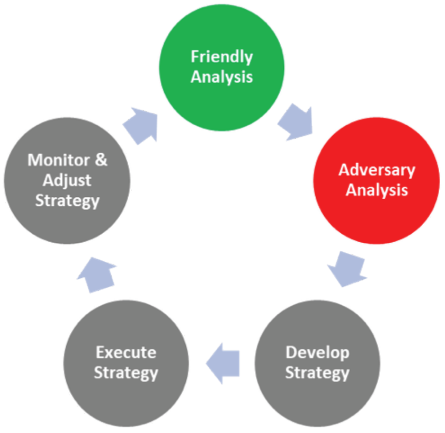
Deception as a cyber-defensive tactic is not a new concept. As with physical deceptions, deception in cyberspace must withstand the scrutiny of cautious attackers, but many early attempts were manpower and time-intensive, and difficult to scale at the enterprise level. However, with recent advances in emulation technology, cyber deception assets can be rapidly deployed and scaled, providing cost-effective options for network defenders.

Modern deception technology can deploy a variety of lures and traps that emulate native software and hardware that are indistinguishable from their real counterparts on the network. Once an attacker penetrates the network perimeter, he conducts reconnaissance to map the network and begins to move laterally to explore potential targets. A network containing deception lures or artificially generated traffic provides the attacker with tempting targets in the form of credentials or software tokens needed to access other portions of the network. These lures lead attackers to traps that mimic physical devices such as servers or individual workstations or virtual / cloud-based assets. As the attacker proceeds further along the path formed by these lures and traps, the deception continues, allowing the attacker to install malware within traps, creating the illusion of a successful attack while isolating the malware from the actual network. More advanced deception technologies allow enterprise-scale deployments which ensure that attackers will be intercepted by the deceptive grid. Traps that have a higher level of interaction continue to reinforce the attacker's belief that his attack is being successful to perpetuate the deception and elicit further attacker engagement.

Throughout the incident, attacker interaction with lures and traps results in high-fidelity alerts to network defenders, helping defenders respond more quickly and precisely to mitigate damage and reduce threat dwell time on the network. These interactions also provide critical real-time data on the attacker's objectives and activities, which helps defenders gain an understanding of the threat. This information also provides a better understanding of vulnerable attack surfaces, which is particularly helpful for defenders who are in the early stages of assessing their network vulnerabilities and developing a network defense strategy.

# DECEPTION STRATEGY DEVELOPMENT AND EXECUTION

Good deception strategies do not happen by accident. With advance preparation and a solid planning process, network defenders can develop a comprehensive cyber deception strategy that will detect, deceive, and defeat attackers and greatly reduce the impact of network penetration incidents. To develop an effective cyber deception plan, defenders need to analyze both themselves and their adversaries (or potential adversaries), develop a deception strategy based on their analysis, then execute, monitor, and adjust their strategy. This cycle is essentially endless, because network attackers can be extremely persistent and constantly adapting their tactics to find new ways around network defenses.



**Friendly analysis:**

• What information and / or assets are most important to your business and what is the potential impact if they are compromised? Developing an effective deception plan requires that you know what your most critical information is, where it is stored, how it is protected, and what sort of adversary would be most likely to seek it out.

• What is your endgame for the deception and how does it support your corporate strategic objectives? To be effective, deceptions must be "nested" within a larger strategy … deception without linkage to a comprehensive security strategy accomplishes little. Particularly if faced with a sophisticated attacker, deception requires integration with your larger corporate security program and must also be supportive of your overall business strategy.

**Adversary analysis:**

• Who is your adversary? Are they amateurs, criminals, activists, trusted insiders, industry competitors, or nation-state sponsored hackers? Will they only use the cyber environment to collect information, or will they use social engineering or physical surveillance methods? How can you tell? Understanding who your adversary is (or at least which category they fit into) is critical to designing a deception strategy that will defeat their attacks. A highly sophisticated attacker will very likely use a combination of cyber, physical, and social engineering methods to acquire the privileges needed to gain access to your networks, and deception planners need to assess the impact of these issues on your deception strategy.

• What is your adversary trying to accomplish? Are they intruding on your network for direct financial gain, to steal intellectual property, or to collect sensitive personal data? Or are they there for a different reason, like using your network as a "bridge" to one of your business partners? Even a limited installation of deception technology can provide critical basic information to help defenders gain an understanding of the threat and develop a more comprehensive deployment plan for their deception technology.

**Strategy development:**

• What must your adversary see, think, and (most importantly) do for your deception to be successful? If your deception creates a highly improbable view of reality, your adversary will realize that something is amiss, and your deception efforts will likely fail.

• Are you trying to increase or decrease ambiguity? If your adversary already believes "X," do you want to reinforce that belief, or do you want to change the situation so he believes "Y?" One of the key deception maxims, known as Magruder's Principle, holds that it's easier to reinforce a preconceived notion (supporting cognitive bias) than it is to change a target's opinion, but under certain circumstances a contrarian approach may be necessary.

**Strategy execution:**

• What type of deception technologies do you need to install to achieve your intended objectives? How many of each type? Where do they need to be installed? Is there a logical sequence and explanation for the changes? Any modifications to your network should be consistent with your normal system update or you need "backstopping" to explain the changes to support your deception story.

• Where do you want to direct attackers, and do you need to change the configuration on other portions of your network to support your deception? The overall picture that your network presents after installing deception technologies should be realistic and reasonable for an organization of your size and industry.

**Strategy monitoring and adjustment:**

- What feedback mechanisms do you have in place to monitor your adversary's activity, increase your understanding of his goals, and tell if your strategy is working? High fidelity alerts provide insight into the deception's success and may also cause changes in your organization's broader security posture, depending on your attacker's sophistication.

- Is your strategy flexible and scalable enough to adapt when your adversary changes his approach? As your understanding of your attacker's objectives increases, your approach may need to be adjusted. Deception resources must be available for rapid deployment to present attackers with traps and lures to divert them from actual network assets.

Despite the many and persistent threats posed by network attackers such as amateurs, criminals, anarchists and others, network defenders should not remain in a passive posture awaiting the next incident. Just as military units use deception to misdirect and defeat an adversary's attack in the physical environment, the same applies in cyberspace. Network defenders can leverage modern deception technologies to steal the initiative from attackers, developing comprehensive strategies that allow them to detect, deceive, and defeat attackers. These technologies are scalable, flexible, and can precisely mimic software and hardware assets, allowing defenders to reduce attacker dwell time on the network, buy time to mitigate damage, and ultimately reduce the bottom-line impact of network penetrations.

**ABOUT TRAPX SECURITY**
TrapX Security is the pioneer and global leader in cyber deception technology. Their DeceptionGrid solution rapidly detects, deceives, and defeats advanced cyber attacks and human attackers in real-time. DeceptionGrid also provides automated, highly accurate insight into malicious activity unseen by other types of cyber defenses. By deploying DeceptionGrid, you can create a proactive security posture, fundamentally halting the progression of an attack while changing the economics of cyber attacks by shifting the cost to the attacker. The TrapX Security customer-base includes Forbes Fortune 500 commercial and government customers worldwide in sectors that include defense, healthcare, finance, energy, consumer products, and other key industries.
Learn more at www.trapx.com.

TrapX Security, Inc.,
3031 Tisch Way,
110 Plaza West
San Jose, CA 95128

+1–855–249–4453
**www.trapx.com**
sales@trapx.com
partners@trapx.com
support@trapx.com