The Ultimate Guide to Deception-Based Security

Anti-Malware Deception Solutions

Written by

Bavelle Technologies

Bavelle Technologies
100 Eagle Rock Ave, #301, East Hanover, NJ 07936
www.bavelle.com

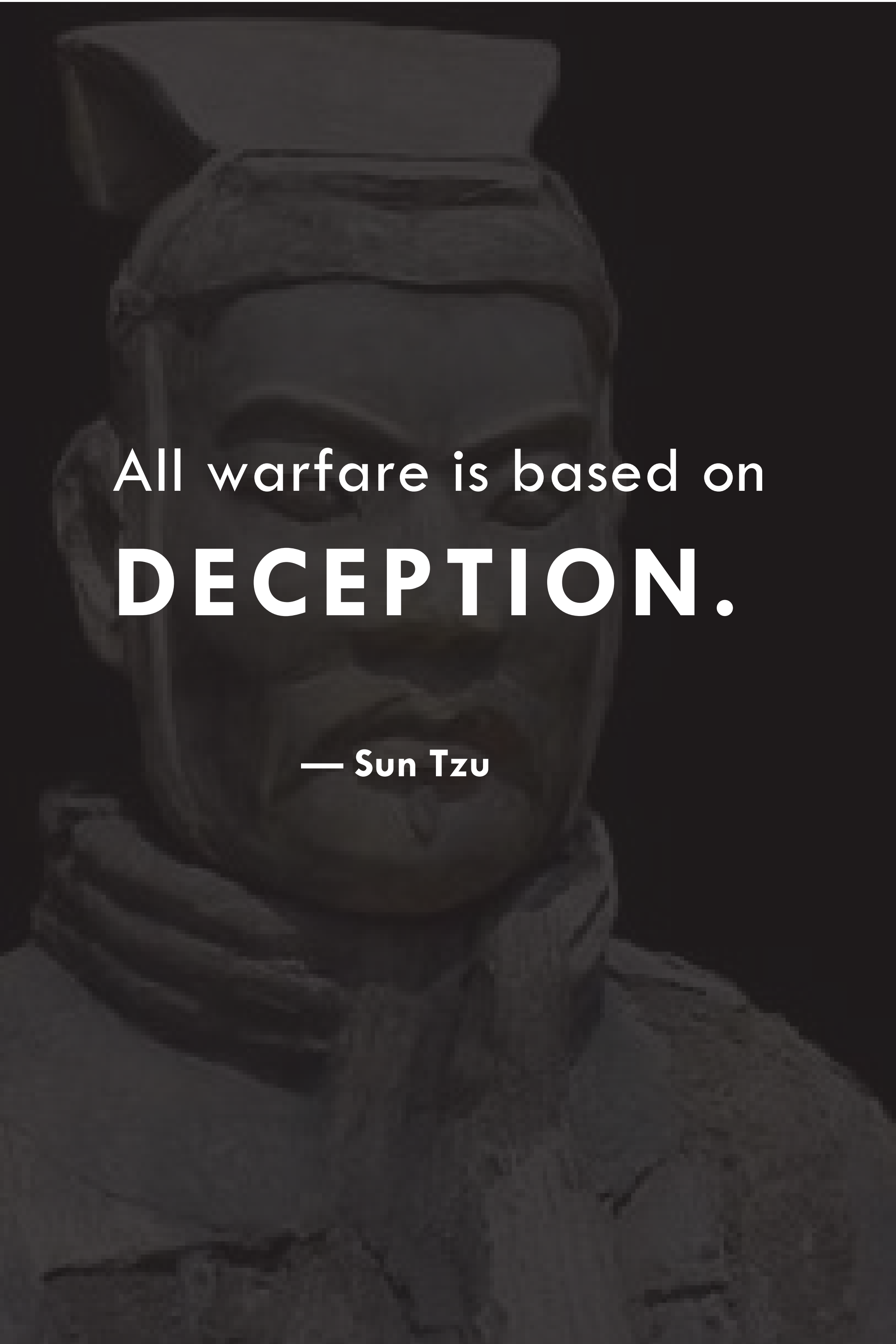
The Ultimate Guide to Deception-Based Security

Anti-Malware Deception Solutions

CHAPTER 1

CHAPTER 2

CHAPTER 3



All warfare is based on

DECEPTION.

— **Sun Tzu**

1 THE HISTORY OF DECEPTION

1 **Use of deception as a part of natural selection in evolution**

2 **How deception has been adopted by human-kind**

3 **Failure of traditional security mechanisms in safeguarding network perimeters**

4 **Role of deception in cyber-security**

Species have often relied on deception as a survival technique. We start with deception in nature to provide an understanding of the origins of deception. For creatures higher on the evolutionary ladder, the ability to deceive is linked to creativity. The same cognitive skills that enable imagination go into telling a successful lie. The inventiveness of humans has further improved upon nature and made deception into an artform. We use warfare as an example to study this art of deception. Warfare in the 21st century has moved to information technology. The last section in this chapter looks at the history of war and the role of deception as a battle tactic.

DECEPTIONS IN NATURE

In the animal and plant kingdoms, deception is among the most effective and widespread tools for survival, and has been an evolutionary adaptation in various forms as a successful strategy. As psychologist Harriet Lerner observed, "Deception and 'con games' are a way of life in all species and throughout nature. Organisms that do not improve their ability to deceive – and to detect deception – are less apt to survive."

A FEW EXAMPLES ILLUSTRATE THE VARIETY OF DECEPTIONS:

PLANT DECEPTION: Western Skunk Cabbage emits a scent quite similar to that of skunk spray to draw in its pollinators – scavenging flies and beetles.

PLANT DECEPTION: Rye used to be a weed in wheat fields, until it began mimicking the qualities of wheat and even surpassing it in some areas through a phenomenon called Vavilovian mimicry.

PREDATOR DECEPTION: Angler fish have a long filament on top of their head that it can wiggle to resemble a prey animal to lure other predators close.

PREY DECEPTION: Sepiola squid inserts a cloud of ink, which is colored and shaped just like the squid, between itself and the predator. The squid then changes color and darts away, leaving a confused predator in its wake.

IMPORTANT POINTS TO NOTE FROM NATURE:

DECEPTIONS ARE VARIED. There are literally thousands of examples of deception.

DECEPTIONS ARE SPECIALIZED. Each type of deception works only for a specific species, in a specific environment for a particular threat or opportunity.

DECEPTIONS ARE NOT STATIC. The arms race between the predator and prey keeps throwing up newer deceptions as the opponent evolves to circumvent the previous deception.

The many disguises of the mimic octopus

MILITARY DECEPTION

Active deception requires a higher level of cognitive ability. In humans, deception has been related to cognitive development and has been observed even in children of 2-3 years old 1]. Deception requires the ability to mentally balance reality and fiction, in addition to the capacity to recognize the difference.

Deception has always been a strategic component of warfare. Numerous historical references exist where ploys were designed to defeat an enemy by drawing them into weak position.

VARIOUS TYPES OF DECEPTIVE ACTIVITIES HAVE BEEN EMPLOYED THROUGHOUT THE HISTORY OF WARFARE, SUCH AS:

FEIGNED RETREAT: Leading the enemy, through a false sense of security, into a pre-positioned ambush.

FICTIONAL UNITS: Creating entirely fictional forces or exaggerating the size of an army.

SMOKE SCREEN: A tactical deception involving smoke, fog, or other forms of cover to hide battlefield movements.

TROJAN HORSE: Gaining admittance to a fortified area under false pretenses, to later admit a larger attacking force. The most famous example being the subterfuge used by the Greeks to enter the city of Troy.

STRATEGIC ENVELOPMENT: A small force distracts the enemy while a much larger force moves to attack from the rear. A favored tactic of Napoleon.

These general tactics can be combined or customized to suit the need[2] . For instance, use of camp fires by George Washington to fool the British scouts, or the use of 15,000 dummy horses in the battle of Megiddo during World War I, or even the inflatable arsenal deployed by Russia in 2016[3] can all be seen as different forms of Deception.

In all the examples, successful use of deception in warfare depends on secrecy, concealment, originality and speed. The same deception is not appropriate in all circumstances. The deception must blend into the environment. When the dummy horses were used in the example above, they had real horses walk up and down to the nearest water source multiple times to create the illusion. A successful deception is always the result of an extremely well-orchestrated plan.

Illustration: Megiddo dummy horses in 1918; Russia's inflatable arsenal imitation T-80 tank

It is a double pleasure to DECEIVE the DECEIVER.

— Jean De La Fontaine

2 ADVANCED THREATS

IN THIS SECTION:

1 Advanced threats – kill chain model

2 Detect, Engage & Respond – the three stages of deception

3 Traditional deception vs. Endpoint deception as a strategy to detect and mitigate attacks

In spite of heightened attention to perimeter security, advanced cyber-attacks have been increasingly successful year over year.

In this section, we outline the nature of advanced threats and the different ways that deception can be used to detect and respond to these threats. Thereby, we outline the approaches required for next generation deception technologies.

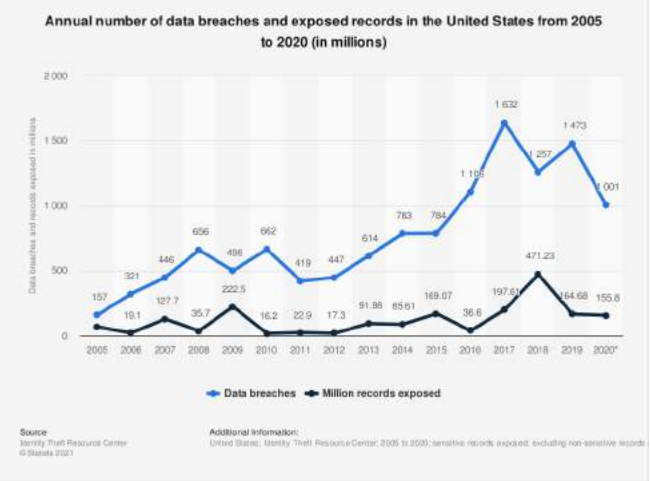
We will use the kill-chain model to understand how advanced threats operate. The next section discusses how deception can be employed against advanced threats using three progressive levels of interaction. The last section explains the difference between "endpoint deception" and "network deception," and how the former can reduce overhead, and can be widely deployed with minimal resource usage. We also illustrate how endpoint deception is used in the different stages of a "kill chain".

CYBER THREATS ARE INCREASINGLY SUCCESSFUL

The network perimeter has become "porous" by design. Cloud computing, BYOD (Bring Your Own Device), IoT (Internet of Things) devices and applications have made the traditional cyber security perimeter defenses largely ineffective. In 2014, speaking to CBS' "60 Minutes", FBI Director James Comey said, *"There are two kinds of big companies in the United States. There are those who've been hacked...and those who don't know they've been hacked".*

The chart shows the rise in the number of data breaches from 2005 to 2020. The average total cost of a data breach has also increased to reach $8 million in 2019

In 2014, speaking to CBS' "60 Minutes", FBI Director James Comey said, "There are two kinds of big companies in the United States. There are those who've been hacked... and those who don't know they've been hacked".



Annual number of data breaches and exposed records in the United States from 2005 to 2020 (in millions)

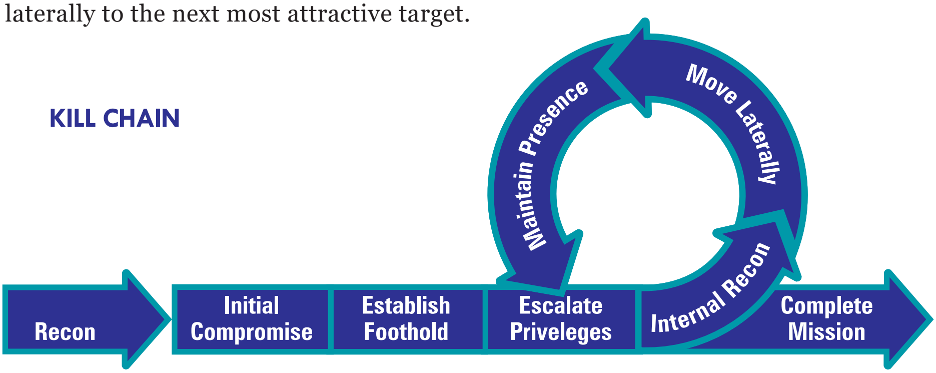
Source
Identity Theft Resource Center
© Statista 2021

Additional Information:
United States; Identity Theft Resource Center; 2005 to 2020; sensitive records exposed, excluding non-sensitive records

THE KILL-CHAIN MODEL

The *"kill-chain"* model captures the various stages of an advanced threat attack scenario. Perimeter security systems try to prevent the initial compromise, but a persistent attack ultimately succeeds, through social engineering, phishing, or other means of compromise, and establishes a foothold. Once the threat is inside the perimeter, it spreads by escalating privileges, doing a reconnaissance of the network neighborhood and moving laterally to the next most attractive target.

KILL CHAIN



DETECT, ENGAGE & RESPOND

Advanced threats establish multiple footholds using several exploits. Effective mitigation requires a detailed understanding of the Tactics, Techniques and Procedures (TTP) of the threat.

Deception solutions should interact with a threat at three levels to provide detection and mitigation.

DETECT

Any access to a deception reveals a threat with a high degree of confidence. The deception could be a fake privilege inserted in an endpoint, a fake network share, a honeypot server or any mimicked resource.

Detection requires only a low-interaction deception and cannot identify all the TTPs used. Hence detection is necessary but not sufficient to completely eliminating threats.

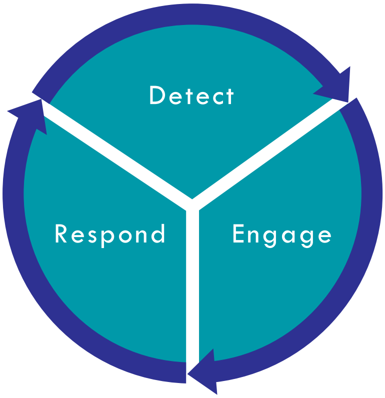
ENGAGE

Once a threat is detected, deception enters the engage phase and starts interacting with the threat to gather information. Typically this requires a high-interaction deception, maybe a server, a router, a software service etc., which is essentially a copy of the production resource.

The engage phase collects detailed threat TTPs, specifically the payload, lateral movement exploits, command and control centers, accounts compromised and the goal of the attack.

RESPOND

Understanding the attacker's techniques and goals helps in both slowing down the attack and remediating all vulnerabilities. This needs automated intelligence to correlate the threat TTPs collected in the engage phase and devise a proper response strategy. A typical response can be shutting down access to the external exfiltration sites.



TRADITIONAL NETWORK DECEPTION

Traditional network deception requires many forms to detect and engage the threat at every step of the kill chain. Network deceptions can be broadly divided into four types:

DECOYS

A decoy is a fabricated system or a software service that presents an attractive target to the attacker. A honeypot is a type of decoy. Other decoys can be routers, printers, a database service etc. A decoy usually is more tempting than the real production network neighbors, with interesting data and known vulnerabilities.

BREADCRUMBS

Breadcrumbs are used to lead an attack to a decoy. These are important since the initial compromise is usually an enterprise endpoint. When an attacker does a reconnaissance, breadcrumbs on the endpoints and in the network point to decoys as interesting targets.

BAITS

Baits are honey tokens, for example counterfeit data or fake credentials to a service, which the attacker finds worthwhile to steal. Baits are laid carefully so that ordinary IT procedures or normal user behavior do not touch them. An attack can be detected by monitoring the access or usage of the bait.

LURES

A lure makes a decoy, a breadcrumb, or a bait more attractive than the actual enterprise network assets. For example, to make a software service decoy attractive, it can be set with factory default credentials. A file used as bait may contain fabricated enterprise financial information.

ENDPOINT DECEPTION

In order to be pervasive, traditional network deceptions must be diverse, sometimes using a combination of thousands of decoys, lures and other types of deceptions, installed on planned machines- and that can take up just as many resources as the business is already using. Endpoint deceptions like Deceptive Bytes are more lightweight and scalable and can be installed on every endpoint with no significant impact on productivity and efficiency.

Pervasive deception is required at every stage of the kill chain in order to disrupt the attacker.

The list below provides a few examples of network deceptions to disrupt the kill-chain.

ESCALATE PRIVILEGES – counterfeit user credentials in OS caches (bait)

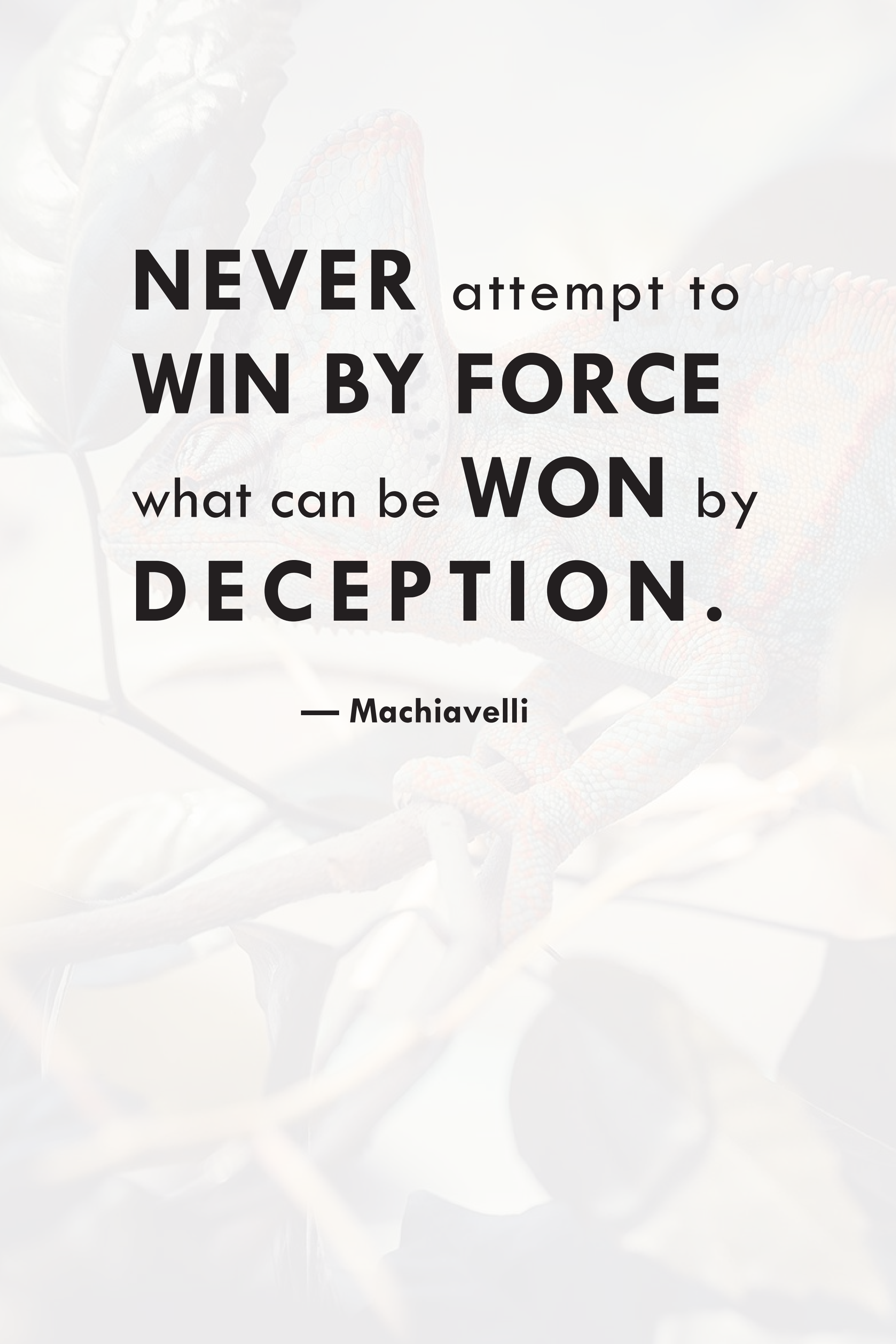
INTERNAL RECON – FTP/RDP/SSH links & credentials that direct to honeypots (breadcrumb)

MOVE LATERALLY – Honeypots, fake network shares (decoy)

COMPLETE MISSION (Data Exfiltration) – honey data files in honeypots (bait)

DECEPTIVE BYTES - SOLUTION

The benefit of Deceptive Bytes is that it does not rely on thousands of decoys to prevent attacks on their networks, but instead, this lightweight endpoint solution is able to detect and respond to active threats before they move laterally across the network, and tricks the malware into thinking it succeeded, or camouflages the host to appear as though it is not a worthwhile target, thus, terminating the infection process.



NEVER attempt to **WIN BY FORCE** what can be **WON** by **DECEPTION.**

— **Machiavelli**

3 RECOGNIZING A GOOD DECEPTION SOLUTION

IN THIS SECTION:

A persistent cyber-attack usually has very good odds of success – it only has to succeed once in penetrating the perimeter defenses. Deception is unique in that the threat actor needs to be wrong only once before he gets detected.

An effective enterprise-scale cyber-deception solution lays carefully crafted decoys to detect and study an attack at every step of the internal recon and lateral movement.

THE FOLLOWING ARE THE TEN ESSENTIAL REQUIREMENTS OF A POTENT CYBER-DECEPTION SOLUTION.

1 Deceptions must provide both SCALE AND DEPTH

Enterprise deception solutions should be lightweight to scale up cost-effectively while also providing the ability to engage and respond to the attack.

Solutions that provide thousands of decoys are not necessary - you can use a lightweight process that can be installed on all machines.

2 Deceptions must be DYNAMIC

Staleness is the enemy of deception. As the network and threat environments evolve, deception must adapt.

Solutions with static, in-network deceptions are easy to fingerprint and are of little value. With endpoint deception, you can prevent the attack before it moves laterally.

3 Deceptions must be PERVASIVE

Effective deception can use various kinds of decoys, baits and breadcrumbs.

Solutions that are decoy-only (or even worse, honey-pot-only) or breadcrumbs-only are partial, incomplete and marginally effective solutions. Endpoint deception is more light-weight and can prevent the attack before it spreads.

4 Deceptions must be AUTOMATIC

An enterprise-scale deception solution needs to lay out a multitude of deceptions and manage them dynamically. Automation of every step is a requirement for practical deception at scale.

Solutions that require manually deploying or managing deceptions do not scale. Solutions that don't require decoys require little handling after deployment.

5 Deceptions must NOT INTRODUCE NEW RISK

Deception technologies, by design, introduce vulnerable systems in the enterprise network to lure and engage attacks. A vulnerable system increases the risk of compromise as the threat actor can use this as a pivot point to launch attacks against other systems in the network.

Solutions that physically locate high-interaction decoys in the enterprise network (connected directly to an access port or a trunk port) run the risk of compromise pivoting to the enterprise servers.

6 Deceptions must BE INTELLIGENT

Data science is an integral part of an effective deception solution. Machine intelligence is imperative for automation.

Beware of solutions that do not leverage machine intelligence. The effort involved to design, deploy, manage, monitor deceptions and correlate threat data is near untenable without the uncanny leverage of Data Science.

7 Deceptions must BLEND into the ENTERPRISE

A deception should not look any different from the network neighborhood. This applies to all decoys, baits and breadcrumbs. Requires dynamic deception to keep up with the changes in the network.

Solutions that need manual setup for blending do not scale.

8 Deceptions must be DATA-DRIVEN

A deception solution must be driven by the vulnerabilities in the network and the current threat landscape. Integration with the SIEM and cyber threat feeds is essential for effective deception.

Solutions that do not integrate with the SIEM cannot be dynamic.

9 Deceptions must STUDY THE ATTACK

Threat engagement and analysis is an intrinsic part of a complete deception solution. A thorough understanding of the attack helps fix all vulnerabilities targeted by the attack and close all back doors to completely neutralize the attack.

Solutions that do not provide attack TTPs are equivalent to low-interaction solutions.

10 Deceptions must be part of the LAYERED DEFENSE

A deception solution cannot function in isolation. It needs to integrate with the security ecosystem to both provide effective deception and quick response.

Solutions that do not interact with the security ecosystem cannot respond to the attacks.

REFERENCES

1. “Emergence of Lying in Very Young Children” Angela D. Evans, Kang Lee Dev Psychol. 2013 Oct; 49(10): 1958–1963

2. “Military deception” https://en.wikipedia.org/wiki/Military_deception

3. “New Weapon in Russia’s Arsenal, and It’s Inflatable” http://www.nytimes.com/2016/10/13/world/europe/russia-decoy-weapon.html