Emerging Technology Analysis: Deception Techniques and Technologies Create Security Technology Business Opportunities

16 July 2015 | ID:G00278434

**Analyst(s):** Lawrence Pingree

**Summary**

Deception techniques such as honeypots are not a new concept in security; however, new techniques and capabilities promise to deliver game-changing impact on how threats are faced. This research articulates how product managers can successfully use threat deception as a threat response tactic.

**Overview**

**Key Findings**

Although still nascent, deception as a defense strategy against attackers has merit, and can be an attractive new capability for larger organizations desiring advanced threat detection and defense solutions.

Many organizations don't understand what threat deception is; educating security buyers on its usefulness will be crucial to furthering adoption of deception technologies and concepts.

Deception as an automated responsive mechanism represents a sea change in the capabilities of the future of IT security that product managers or security programs should not take lightly.

Deception decoy sensor providers emerge to offer enhanced detection of east-west attacks by distributing sensors across an enterprise's internal environment, and mimicking enterprise endpoint services, applications and systems.

**Recommendations**

Product managers:

- Examine how threat deception techniques can be leveraged to enhance your existing threat defense capabilities against advanced adversaries.
- Consider whether integrating with existing threat deception providers can bring additional value to your current offerings.
Evaluate existing deception capabilities across the security market, and articulate them correctly to your product marketing managers to demonstrate the value of deceiving the attacker.

Strategic Planning Assumption

By 2018, 10% of enterprises will use deception tools and tactics, and actively participate in deception operations against attackers.

Analysis

This document was revised on 31 July 2015. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com (http://www.gartner.com/technology/about/policies/current_corrections.jsp).

Technology Description

Deception technologies are defined by the use of deceit and/or feints designed to thwart or throw off an attacker's cognitive processes, disrupt an attacker's automation tools, delay an attacker's activities or disrupt breach progression. Deceptions are achieved through use of deceitful responses, purposeful obfuscations, feints, misdirections and other falsehoods. These techniques leverage the trust that attackers and the attackers' tools must have in the network protocols, infrastructure, applications, systems and data elements they interact with or access during the execution of their attacks or throughout their intelligence gathering activities. Deception in this context is used as a technique for defensive or disruptive purposes, and is not offensive in nature.

Overview

Throughout the years, use of deception techniques (also called feints, misdirections or lies) have been used widely and effectively to enhance threat detection and as a threat response strategy. Use of deception techniques has spanned a variety of enterprise security technologies and security programs — most notably, government entities such as the Department of Defense have leveraged deception techniques against adversaries for many years. Most security practitioners know of honeypots or honeypot sensors; these solutions, in fact, use deception as a key strategy to gather threat actor intelligence. For many years, technology providers have used a substantial number of honeypot sensors and techniques to improve the detection of attackers, and to provide enhanced telemetry in the form of machine-readable threat intelligence and strategic human intelligence on threat actors. They have largely used this intelligence-gathering capability to enrich their products or service offerings, and to enhance their products' threat prevention capabilities. However, providers across the security markets can improve their use of deception, and move beyond detection to prevention and threat actor diversion. This research will analyze how market participants can leverage threat deception in their solutions, as well as examine emerging providers currently using deception techniques as a core threat detection and prevention approach.
Deception solutions are emerging to play a greater role in the future of enterprise threat defense. Detection is often a prerequisite to higher-quality deceptions. However, use of deceit in the enterprise is beginning to be used to actively thwart or "black-hole" malware botnets, threat actors and suspicious connections. In some cases, federal investigators have used deception techniques to intercept and disrupt command-and-control communications during botnet takedowns, but many of these uses have been manually executed network protocol or command-and-control server deceptions. The goal of deception technology continues to be detection; however, use of deception has been widening across many different types of products throughout the years, including the age-old honeypot sensor. Deception technology implementations now span multiple layers within the stack, including endpoint, network, application and data. However, many technology providers have been reluctant to mention these (often cool) techniques to trick the attacker or their intrusions because threat deception is widely misunderstood, or is unknown as a concept to buyers.

Imagine the Future — A Deception Wave Is Eminent

Imagine for a moment, that once malware is detected in an end user's environment, the user's systems had the ability to begin to lie to the attacker at the other end of the command-and-control console, or to the malware itself on the infected endpoint, or both. These capabilities are now becoming a reality. Use of deception through use of honeypot sensors as a detection measure has often been a security practitioner's dream, yet has been unattainable because the honeypot sensors of the past required too much administration, handholding and maintenance, and were mostly based on open-source code. Honeypots have been perceived by some to potentially add additional risks by enraged the threat actor, creating new security holes or increasing liability for an organization if the attacker were to compromise a system, and then begin to attack outwardly onto the Internet from the honeypot itself. Today's honeypot has evolved toward greater automation, and offers enterprise-class features and operations capabilities. Product managers need to encourage product marketing managers to examine and enhance their messaging based on the types of deception techniques they can use, threat deception effectiveness and what deceptions they already use in their products, to enhance and communicate their threat defense capabilities against advanced advisories.

For the past 20 years, most active security control responses built into network security products have remained fairly constant, offering only a limited number of response actions, such as log, reject, drop and quarantine, with very little innovation or evolution beyond these more-simple automated response concepts. Although these responses are effective at both detecting and blocking individual attacker attempts, responses such as reject and drop are widely visible to a skilled adversary, especially advanced persistent threat actors. These types of responses allow an attacker to rapidly (or even immediately) identify when they are detected, and serve to inform the attacker that it must quickly adapt its attack strategy to continue to move forward. These basic defensive actions must evolve so that a strong hold against the attacker can be maintained and to increase the
attacker’s economic burden to attack; product managers need to support product marketing to articulate the types of economic burdens the product achieves using deception.

Why Leverage Deception?

Attackers and their automation tools must rely on the responses of the network protocols, endpoint services, operating system behaviors and data they encounter throughout the process of their attack to successfully move their attack goals forward. For example, an attacker may scan the network using TCP to elicit open ports on endpoints throughout the network to find hosts to interact with and services or applications to compromise. During this intelligence-gathering activity, they often gather banners that are used by network protocols to announce protocol specifications, and negotiate and agree on communication constructs. A great example of a protocol negotiation is Secure Sockets Layer, whereby a negotiation of the cryptographic algorithm and keys is initiated prior to the conversation taking place.

Although many security practitioners have touted the phrase “security through obscurity is not the answer,” this statement, however, is not entirely true. Gartner believes that security technology providers must consider use of deception techniques during the course of their threat responses to enhance the value of attack disruption they desire within their products. Use of deception as a technique to thwart attackers has been used for many years in military scenarios (see Note 1).

The Honeypot Lives On With the Emergence of Distributed Decoy Systems

Today, deception technologies are being employed within security products and include use of both emulated/virtualized and real endpoint decoy systems, as well as network services, protocols, applications or fake data elements. A new class of products with distributed endpoint decoys is emerging with threat deception capabilities that can enhance our defenses. In this new class of security products, distributed decoy systems are used to portray deception across multiple layers of interaction by attackers. Each of these layers and data elements serves as deceptive lures, and aids in the successful deception, disruption and/or misdirection desired against an attacker and its attack automation software. Traditional honeypot sensors of the past generally provided a networked endpoint system (often a server) or emulation of a service on a live system, with a variety of adjacent emulated services and network protocols, such as HTTP, SMTP, Network Basic Input/Output System, Telnet and FTP (see Note 2).

Gartner believes that more lean-forward organizations should also leverage deception in-depth as a new strategy for comprehensive threat defense against the onslaught of advanced attackers and attack techniques. Product managers who help product marketing managers articulate the value of deception in their own products or integrations with other deception products can enhance their attractiveness, especially for larger organizations under constant threat, for example, the financial services, healthcare, government and software verticals.

Intelligence-Led Deceptions Are Crucial to Disrupting the Attacker
Threat intelligence sharing continues to provide significant improvement in security for many organizations (see "How to Collect, Refine, Utilize and Create Threat Intelligence" and "Intelligence Awareness and Adaptive Security Response Will Transform Network Firewall Markets""). This threat intelligence data could lead us toward intelligence-led deceptions — where a threat actor that is known to originate from a certain location or uses a certain pattern of engagement can be led astray, versus given access to sensitive systems, applications and data types. Deception as an automated responsive mechanism represents a sea change in the capabilities of the future of IT security, and should not be taken lightly by product managers or security programs. Gartner believes that enterprises (especially those with lean-forward programs) will continue to expand their use of deception as a threat response tactic, whereby threat management teams utilize intelligence and orchestrated deceptions to divert attackers away from their sensitive assets. This tactic can enable threat management teams to assert more active control of an attacker and its activities throughout the enterprise environment, and allow organizations to track and share even greater intelligence on threat actors. Ideally, upon detection, threat actors and their compromised systems or applications will be automatically isolated into a network deception zone, where they are provided with what is equivalent to a hall of mirrors, in which everything looks real, and everything looks fake. The most critical reason to use deception is to delay an attacker and force it to spend more time, causing it economic harm while it tries to figure out what is real and what is not, and whether to proceed.

Four Styles of Deception — The Deception Stack

We examine four styles of deception, which we call the Gartner deception domains.

Deception technologies can use a wide variety of capabilities to create their deceptions. Deception techniques are typically deployed across the deception stack (see Figure 1) to make a deception effective and believable. The deception stack consists of sets of tools and responses that operate at different layers the attacker may interact with — the network, endpoint, application and data layers. It is important to note that the further up the stack deceptions move, the more difficult the deception is to maintain against a formidable and well-educated adversary. Deception technologies such as distributed decoy solution providers should be orchestrated across the four styles of deception.

Figure 1. Four Styles of Deception — The Deception Stack
Believable deceptions must use a variety of deception techniques deployed across the entire deception domain stack, leveraging disruption of the kill chain model (see "Addressing the Cyber Kill Chain") for the deception to be useful, believable and comprehensive. Product managers should consider how they effectively address the different deception styles to make their deceptions believable and effective.

As illustrated in the deception stack in Figure 1, deception can utilize a variety of technologies across an entire array of capabilities. Much of today’s deception technologies employ one or many aspects of this deception stack, including a distributed grid of emulated and/or real decoy endpoints, network infrastructure, network protocols, services, applications or data elements, to participate in deceiving the attacker across these domains. Since we now understand the domains of deception, we can utilize. Now, let’s examine how this is oriented to the attack kill chain concept.

Figure 2 is an example of the Gartner deceptive response kill chain, where deceptions are injected as an overlay to the Gartner cyber attack kill chain concept. The deceptive response kill chain represents several distinct uses of deception across the entire life cycle of an attack. Deceptions deployed using the four styles of deception as a deception deployment framework can be used to create a more complete and comprehensive maneuver against an attacker, and trick an attacker into either triggering a detection event, or specifically disrupting segments of the attack kill chain. The most advanced deception solutions currently leverage all the four styles of deception (the deception stack) in conjunction with the deceptive response kill chain, to provide organizations the most believable deceptions that are most likely to be triggered by an attacker.

**Figure 2. Deceptive-Response Kill Chain**
Examination of Deceptions Possible at Each Kill Chain Phase

**RECONNAISSANCE**

The first stage of most attacks is the reconnaissance or recon phase. At this stage, a good strategy for deflecting the attacker is to lie to the attacker. This confuses the attacker and makes it difficult to identify potential services, applications, data or infrastructure components for the attacker to exploit.

**WEAPONIZATION**

At the weaponization stage, misdirecting the attacker through deceitful application responses or emulated services can delay the attacker further. It also delays the attacker's tool selection or misdirect the attacks toward services that are not actually being used. A common tool to detect maliciousness during the weaponization phase is a network sandbox. These tools are designed to lie to malware, providing a deceptive environment to execute in and behaviorally assesses the malware for maliciousness. These tools could be extended as a blocking mechanism or to run malware for longer periods of time and invoke other deceptions, such as lie about the operating system that's running or other system or application details. Additionally, weaponization has a lot to do with the attacker's or its malicious code's exploit selection. Just one example is tricking drive-by download scripts into believing you have Windows XP, when you are running Windows 7, which effectively thwarts exploit selection.

**DELIVER**

At the deliver phase, a simple example is using other subterfuge, such as a diversion technique, to send unknown, suspicious or known malicious binaries that enter an organization's environment into a deception zone (like a network sandbox), where it executes in a virtual environment on a real system that looks like it's being used by a real user.

**EXPLOIT**
During the exploit phase, deceptions can exist at any point in the deception stack to trick or disrupt exploitation from actually occurring, depending on the target of the exploit attack itself. For example, if we have declared that a particular traffic pattern looks malicious, we could automatically use network address translation or other transport layer protocols, and redirect suspicious traffic to a deception decoy environment, rather than the protected system or application. There are a variety of deception techniques that can be used during this phase to disrupt exploitation, but responses must be crafted according to the types of malware and attacker behavior. At the network layer, technology providers selling intrusion prevention systems have an opportunity to disrupt exploitation by providing deceptive responses and faking the outcome of a successful exploit, or shunting traffic into the deception decoy environment.

**INSTALL**

At the installation phase, often on the endpoint itself, it is possible to disrupt malware itself by deceiving the malware into believing it is running in a virtual environment, or making the malware believe it has written files that it hasn't. We know that many malware forms will stop functioning because they detect virtualization, or when they believe their execution has been successful. We can take advantage of this trust, and thus, interrupt the installation phase.

**COMMAND**

During the command phase, most common malware uses command-and-control to receive commands to execute and provide the remote agent malware instructions to download other payloads or for other remote control purposes. At this stage, attackers commonly manually interact with a specific agent to gather intelligence, exfiltrate data or move laterally within the network. The most common approach of using deception at this stage is to redirect command-and-control traffic to socket servers (hosts with open TCP sockets) to understand the communication protocol used by the botnet. It is also possible to take down botnets by issuing commands back to the agent technology, and deceiving the agent itself. This approach is commonly used by federal investigators to take down botnets, but can also provide critical telemetry to enterprises, as well as disrupt attacks in a similar manner using automation and deceit, thus, disrupting the attack.

**ACT**

During the act phase, an attacker is exploring the environment in which the malware is contained. This is the most common phase in which lateral movement, network scanning, host probing, credential gathering and other activities occur. Endpoint agent technology, or even network-based solutions, can intercept and deceive at this stage. For example, deception techniques can be used to make attackers believe they have received valid credentials or that they've explored real endpoint systems and are seeing real sensitive data, leading us to enhance the detection of their actions. Using the attackers' trust against them, we can increase detection and delay their efforts, causing them more financial harm. For example, if we provide an attacker with faked credentials, it may take a week for the attacker to crack a credential that is actually useless within the enterprise.
environment (that is, the credential has no real privileges). Additionally, the attacker may attempt to use that cracked credential within the environment, increasing the likelihood of detection.

Table 1 provides an overview of deception providers and their primary domains of deception.

<table>
<thead>
<tr>
<th>Deception Provider</th>
<th>Network</th>
<th>Endpoint</th>
<th>Application</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allure Security Technology</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Attivo Networks</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
</tr>
<tr>
<td>CyberTrap</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
</tr>
<tr>
<td>Cymmetria</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
</tr>
<tr>
<td>ForeScout</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>GuardiCore</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
</tr>
<tr>
<td>Hexis Cyber Solutions</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>illusive networks</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>Partial</td>
</tr>
<tr>
<td>LogRhythm</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Percipient Networks</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Rapid7</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Shape Security</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Specter</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
</tr>
<tr>
<td>TrapX Security</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
</tr>
<tr>
<td>TopSpin Security</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Note: The categories above are defined as the primary method for injecting a deception versus what type of deception is taking place. For example, some providers have support for endpoint deceptions such as network shares, basic network protocols like address resolution protocol (ARP) and other network broadcast capabilities that can be deployed with their endpoint decoys. However, since they are not injecting deceptions using an in-line or out-of-band network appliance, they are not categorized primarily as a network deception capability since their deceptions are generated by the endpoint, or using back-end engagement services to invoke the deceptions. The purpose for this is to call out the market opportunity for network devices to perform deceptions and not to penalize distributed decoy providers that do have deceptions that are related to network functions, or the mimic network infrastructure.

Technology Adoption

Deception techniques and technologies have so far had only nascent adoption in the market. Most recent adoption has been focused on distributed decoy sensor providers, deployed inside the network to enhance malware and threat detection. This has largely been because deceiving a threat actor can be difficult, and must be orchestrated in the proper way for it to be believable. However, some providers are now successfully deceiving in a believable manner. Distributed decoy systems and endpoint deception agent solutions are gaining traction within financial services and healthcare verticals because they are entities that are very commonly attacked for their sensitive information. Additionally, other large type-A buyers with lean-forward security programs are adopting distributed decoy systems to enhance their deception operations capabilities. The relatively low level of adoption outside of these verticals and lean-forward programs has been predominantly because most organizations have traditionally focused on preventive security controls, and less on detection and response capabilities, and the maturity of deception solutions has been relatively low. The latest Gartner Security Summit in Washington, D.C. directly called out Gartner clients to enhance their detection and response capabilities in lieu of a dynamic perimeter and a greater reliance on cloud and software-as-a-service delivery infrastructures. With continuous attacks against critical organizations with sensitive data types, organizations are focused on raising detection, which will likely lead to increased demand for detection-focused products such as distributed decoy provider offerings. Existing deception technology providers can certainly do more to articulate their threat deception capabilities and enhance their existing technology products to better leverage deception techniques to thwart attackers and enhance detection.

Factors That Will Drive Adoption

LEVERAGING "DECEIVE" AS AN ACTION

Gartner believes that leveraging deceive as an action can now be a reality for many existing security technologies, enhancing existing security threat management programs and solutions. So far, the security market and programs have focused most often on blocking attacks, rejecting sessions and serving only as a small impediment to the attacker onslaught. Deception provides greater delay, confusion and disruption of the
attacker than traditional approaches, and this fact will drive preventive controls that can leverage deception further into client environments. Lean-forward product managers must consider use of deception techniques and adjacent deception technology integrations to evolve their solutions to address today's attackers.

Note: Below are current examples of security technologies, and emerging deception providers and the deceptive responses they can leverage to enhance detection and further disrupt attackers.

FIREWALLS AS A DISRUPTIVE-DECEPTION CAPABILITY

Provider Examples: Check Point Software Technologies, Cisco, Dell, Fortinet, Intel Security, Palo Alto Networks, WatchGuard, Sophos

Firewalls with intrusion prevention, blacklists, reputation feeds and URL filtering have an opportunity to enhance the protection of hosts within their protected network zones by leveraging threat deception as an active response to thwart confirmed attackers. For example, if a host known for being malicious tries to connect to a demilitarized zone (DMZ) system on a specific port, such as SMTP, FTP, Telnet, secure shell, HTTP or HTTP over a secure sockets layer, the action in a policy could be to set "deceive." The deception responses could be either generated by the firewall itself, or by leveraging integration with deception providers that specialize in emulating services or providing deception hosts designed specifically to be attacked. One method for implementing deception actions is to leverage on-demand network address translation or by building on-demand generic routing encapsulation tunnels to transport connections back to deception decoy services, hosts or other infrastructure within a deception zone. The key to successful deceptions is believability; therefore, firewall policies would need to be constructed in a way to align the real services with deceptive services within the deception provider emulated services (for example, deception mappings). Since firewall providers often sit within the internal DMZ network path, they can easily take advantage of deception techniques to disrupt attackers.

STAND-ALONE INTRUSION PREVENTION APPLIANCES THAT DECEIVE WHEN ATTACKED

Provider Examples: Cisco, HP, IBM, Intel Security

Stand-alone intrusion prevention appliances can perform deception as a response to attack detection. Because of their greater dedicated compute resources, attack telemetry and deep inspection at the application layer, deceptions within stand-alone intrusion prevention can be invoked and provide higher fidelity response than other product families. These products can invoke deception at the network protocol layer, for example, within the TCP, whereby simple responses such as a synchronized acknowledgment packets used in the proper way can help thwart attacks. For example, in the past, TCP tarpits ⁴ (a basic deception example) were a popular response to mass TCP port sweeps by attackers that were scanning and profiling systems on the Internet to attack. The concept was simple, when a TCP handshake was requested, the device would respond appropriately, but the destination host would never open a connection, thereby, creating backlogged connections within the attacking hosts stack. However, similar to firewalls, stand-alone intrusion
prevention appliances can also integrate with even more elaborate deceptions, including deception decoy providers and their emulated services to enhance deceptive responses or to redirect the attacker into a deception zone.

**ENDPOINT PROTECTION PLATFORM PROVIDERS AND ENDPOINT DETECTION AND RESPONSE PROVIDERS COULD DECEIVE THE MALWARE AND THE ATTACKER**

**EDR Provider Examples:** Bit9 + Carbon Black; CrowdStrike; CounterTack; Cybereason; Cisco; Cylance; Digital Guardian; RSA, The Security Division of EMC; FireEye; Guidance Software; Promisec; Triumfant; Tanium, Ziften

**EPP Provider Examples:** Intel Security, Symantec, Kaspersky Lab, Sophos

Because endpoint protection platform (EPP) provider endpoint agents sit on the host that malware is often targeting, they are advantaged to leverage deceptive techniques to thwart the malware itself. Based on further examination of the deceptive response kill chain concept shown in Figure 2, it is clear that endpoints are often the target of the exploit, install, command and act phases of the cyber kill chain. Today's malware often profiles a system before delivering secondary payloads that contain malicious actions and perpetual-install binaries. The profiling typically done by today's malware includes checking to see whether an endpoint is virtualized. This is performed by the attacker's malware because the attacker is wise to network, cloud-based and endpoint sandbox solutions, and they often delay or terminate execution of the malware after recognizing they are running in a virtual environment. Leveraging deception in this case could thwart malware installation by deceiving the malware into believing it is within a virtual environment. Although, ideally, only unknown binaries would be deceived in this way, this is only one example of leveraging deception to thwart malware. Other malware commonly circulating looks for the processes of antivirus products; by emulating running processes that look like several versions of antivirus, a malware can be guided toward dormancy through spawning look-alike antivirus processes. Product managers should examine common malware infection and system evaluation methods to augment their existing products to leverage deceptive responses for unknown binaries to enhance the effectiveness of their endpoint malware prevention capabilities.

**WEB APPLICATION FIREWALLS AND APPLICATION DECEPTION SOLUTIONS**

**Web Application Firewall Provider Examples:** Akamai, Citrix, Barracuda Networks, Imperva, F5

**Web Application Deception Provider Examples:** Shape Security

Deception baked into the Web application firewall can provide better disruption of an attacker than just blocking. Threat actors continue to breach Web applications, and this will continue to drive adoption of new approaches for Web defense and new strategies to thwart attackers at the application layer.

Juniper Network's acquisition of Mykonos Software leveraged Web deception, and is moving this technology into the Juniper infrastructure itself to help deceive attackers where it matters most — within the environment that is breached. Juniper has since placed the stand-alone Mykonos technology as end of life while it integrates the technology into
its other network offerings. When conceived, the Mykonos Web deception product used
deceptive Web content and "tar trap" responses to intelligently detect, deflect and slow
attacker's activities. Juniper's Mykonos deceived by injecting things like Java-based
browser fingerprinting scripts, CAPTCHAS (refers to completely automated public Turing
test to tell computers and humans apart), persistent tokens, slowed connections, session
logouts and other elements in the HTML code itself to detect, disrupt and track the
attacker.

Shape Security currently offers a compelling automation technology that disrupts an
attacker's automation through use of Web application deceptions, and Web browser and
HTTP countermeasures. Its primary capability is what it calls polymorphism. This concept
is the use of deceptive obfuscation of common HTML content and application inputs to
remove attack vectors, such as tamper-proofing URL parameters, input fields and
obfuscating sessions, to deflect session takeover attacks. Effectively, what Shape Security
does is rewrite content and these parameters on the fly, obfuscating them and lying to the
attacker's automation. Shape Security has a relatively unique offering that is gaining
traction as a Web deception capability. Although Shape Security continues to focus on the
upper enterprise and early adopters, the company and Web application firewall providers
will need to respond to this new competitive threat. In the Web application firewall market,
buyers continue to buy not only for threat detection capabilities, but also compliance
reasons. For Shape Security, there are currently no underlying regulations compelling the
purchase since it does not currently offer Web application firewall capabilities.

DISTRIBUTED DECOY PROVIDERS PEPPER THE INTERNAL NETWORK WITH DECEPTION SALT

Provider Examples: Attivo Networks, Cymmetria, TrapX, GuardiCore, TOPSpin Security

Distributed decoy providers specifically leverage the use of deception and fake decoy
either systems distributed across the enterprise for detection as a core value
proposition. These providers exploit market inflection points in virtualization, software-
developed networking, emulated services and real operating systems or applications to
improve detection and reduce false positives against advanced attacks. Distributed decoy
solutions offer enhanced detection and stronger fidelity than other traditional security
solutions because when an attacker touches a decoy, it is immediately recognized as an
unwanted interaction, and likely an attacker or insider threat. A great analogy for
distributed decoy solutions is to imagine you are a rabbit hunter setting traps all across
your internal environment. This is the primary concept used to increase detection through
use of traps. In fact, some of the providers call them traps to try to articulate this concept
to their customers.

Factors That Will Inhibit Adoption

FEAR OF A FALSE-POSITIVE DETECTION

False positive detections can significantly hinder adoption of deceptive responses within
many security products. It is, therefore, important to a deception program and its
deception elements to be used in conjunction with high-fidelity threat detections. False
positives have led to quite a few technologies to be pulled out of service or placed in
passive modes of operations. For distributed decoy providers, this is less of an issue
because their deployment mode is dormant unless an attacker sends packets or initiates connections to the decoys. Product managers will need to make certain that integrations with deception products are used only in conjunction with high-fidelity attack signatures, host blacklists and other forms of telemetry to garner a higher rate of adoption and avoid customer rejection or pullback.

DECEPTION BELIEVABILITY

The single-greatest difficulty in leveraging deception techniques within security products is the believability of the deception itself and any business disruption that injecting deceptions into the application or network data path may cause. Most current providers have dealt with these potential issues adequately. Providers must continue to refine their deception concepts and injection points, and consider all the attacker’s thought processes to properly construct believable deceptions. For example, a good deception is one in which the attacker believes and trusts what their eyes tell them. As soon as attackers determine how they had been deceived, they immediately react and no longer trust the elements involved in the deception. However, automated electronic deceptions are much easier to perform because it is difficult for someone to perform closer examination of the elements in the deception. However, we still must recognize and understand the attacker for deception to work effectively. The greatest inhibitor of adoption will be the believability of the deceptions and the ability for providers to cross-integrate with threat intelligence services and other adjacent security products to leverage the ecosystem within most existing security programs.

ENTERPRISE READINESS — DECEPTION PRODUCT MATURITY

The maturity of products is essential to service the enterprise use cases that will emerge. For example, solid integration into incident response systems, processes and procedures are crucial for the enterprise use case, and many of today’s providers lack quality integrations. Since the deception decoy providers are some of the first higher-quality deception providers to emerge in the security market, these solutions must mature rapidly, supporting strong integration with other enterprise security functions. For example, for detections to be properly triaged, solid reporting and alerting functionality must exist. Additionally, role-based access control must be readily available so that security teams can properly triage and manage threat deception environments and gather forensic details, but retain separation of duties. The quality of forensic gathering and robust automated analytic functions will be the most successful capabilities for enterprises. Security operations teams are already overwhelmed with alerts and data; however, a simple user interface and built-in analysis capabilities will propel greater adoption of threat deception capabilities and solutions.

PROOF OF BETTER DETECTION THAN THE NETWORK LAYER ALONE

Providers must overcome the connotation that this new class of products offers more functionality and better detection of east-west attacks than network providers’ solutions — as most do not. Providers like TrapX have addressed this through use of a deep packet inspection engine capable of profiling and performing detection at the networking layer. GuardiCore has addressed this by leveraging software-defined networking, virtual switch
integration and agent-based socket redirection. However, many providers focus only on decoy systems and lures deployed on real endpoints to direct attackers to their detection capabilities. This allows TrapX to leverage network-centric buying behavior, as well as extend the detection capabilities of its solution and compete more effectively against some rivals. Similarly, providers like Attivo Networks offer intrusion prevention signatures such as Snort to use in a Snort-capable intrusion prevention solution, syslog integration to monitor for use of a credential lure (fake credential) and correlate indication of deceptive lure use with its distributed decoy solution.

SKILLED STAFFING AND DECEPTION MANAGEMENT EDUCATION PROGRAMS

Currently, many information security professionals lack the skills and understanding of how to create a deceptive response strategy or program, or to build out a deception environment that leverages the four styles of deception. This means that only educated buyers will be interested in the solutions and using deception as a detective for preventive security control, which will significantly inhibit adoption. Building out a deception strategy will be a crucial step for buyers to understand how to leverage deception and perform deception operations on threat actors. However, a thorough understanding of threat actors and intelligence about them is crucial for building out a deception program.

Technology Impact

The most important technology impacts of using threat deception as a response strategy will be its effect on the threat actors and the execution of their attacks whereby organizations can potentially more directly control the attackers against the backdrop of the cyber kill chain. To properly leverage deception products and responsive strategies, organizations must adopt threat management and deception management concepts. Solutions for threat deception must align with these organizational initiatives. Product marketing managers must articulate the evolution of security programs toward leveraging deception as a security program element.

Actions for the Next Six to 18 Months

COMMUNICATE DECEPTION CONCEPTS TO YOUR DEVELOPERS

Product managers also need to articulate to their developers the benefits of using of the Gartner deception response kill chain as a guide to augmenting their product wherever their products sit in the cyber kill chain process. Product managers and developers should then brainstorm ways in which their products or services can evolve to support enterprise deception program operations and concepts.

BUILD-OUT OF THREAT DECEPTION CAPABILITIES IN YOUR PRODUCTS

Since many end-user organizations lack the understanding of what threat deception is, educating people on its use will be critical to furthering adoption of deception technologies and concepts. Threat deception is not an easy concept to understand and requires a mindset shift from being overly preventive, to a mindset that thinks like the threat actor, and placing lies and misdirection throughout their interactions. In essence, you must encourage security product developers to think like a magician: Their product is the magician on the stage, and the threat actor is the audience.

https://www.gartner.com/doc/reprints?id=1-2LSQOX3&ct=150824&st=sb&aliId=1117060

15/18
EDUCATE PRODUCT MARKETING MANAGERS ON THE VALUE OF CUSTOMER DECEPTION MANAGEMENT PROGRAMS

Product managers must guide product marketing managers to focus on educating their customers about the benefits of developing a deception management program and internal threat deception processes. This will allow their end user clients to maximize the use of deception as a defensive strategy, and help them understand that deception isn't just a point-in-time event, but can be preplanned to divert attackers and thwart or monitor their activities for longer periods of time.

ORIENT YOUR PRODUCT TO MANAGED SECURITY SERVICE DELIVERY OPTIONS — DECEPTION AS A MANAGED SERVICE

Product managers should consider augmenting their deception solutions to cater to managed security services that focus on threat management and security operations. This can be a clearer route to market because of the more active role that deception can play in both threat prevention and detection, and within security operations or threat management programs. Managed security services can also be a more effective delivery mechanism and channel for the adoption of threat deception security technologies because of the high touch involved in accounts and the lower overall education required to provide programmatic deception management. This also allows MSSPs to offer more attached security consulting services along with their managed security offerings. Deception technology providers must focus their education initiatives on partners to entice them to learn about deception operations and program management, focusing on the potential additional high-touch services they could offer to their client base.

References

"Competitive Landscape: Network Forensics Tools"

"Forecast Analysis: Information Security, Worldwide, 1Q15 Update"

Additional research contribution: Anton Chuvakin, Sid Deshpande, Jacqueline Heng, Adam Hils and Deborah Kish.

Evidence


4 TCP tarpits (http://labrea.sourceforge.net/Intro-History.html), Tom Liston.

Note 1

Example of Deception

During World War II, Operation Bodyguard used deception to its advantage. The military used inflatable tanks, large audible speaker systems, fake radio communications and empty tents, as well as other counter-intelligence activities, to misdirect the German army.
into defensive positions near the deception. Meanwhile, the allied forces marched toward the weaker point in the German lines, playing a role in the success of the war efforts.

**Note 2**

**Honeypots**

Although honeypots were useful, the honeypot sensor was widely, effectively used as a detection-only technology, and not to delay or disrupt an attacker. Honeypot sensors of the past were not easily centrally managed and deployed without significant resources, such as physical servers and manual human configuration. Additionally, security practitioners focused on preventive controls at the perimeter. Unfortunately, many security practitioners held the misguided view that their perimeters would remain relatively fixed over time, and that prevention should focus on that boundary. We now know that was a mistake. Public cloud and software-as-a-service options have rendered that traditional "walled garden" view less effective, and forced security practitioners to focus their efforts toward information flow, as well as rapid detection and response, as the key ingredients for their defense in-depth strategies.
influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity. (/technology/about/ombudsman/omb_guide2.jsp)"