Deception - Attackers’ Achilles Heel

ilusive Layers of Deception
Become Offensive to Attackers

You’ve invested thousands or millions of dollars in security appliances and applications to defend every possible avenue that a cyber attacker could take to launch an attack. Your defenses are entrenched. The only problem? You don’t know what the offense—the attacker—is doing. However, you can take action and turn the tables on attackers by using their own weapon of choice against them—deception.

Lateral Movement Precedes Every Breach

A state-sponsored or advanced attacker is human, like everyone else. He—or she—has emotions, motivations, priorities, and a level of patience that allows him to pursue their goal of stealing data, causing damage, or ruining reputations. Attackers who patiently gather intelligence and make lateral moves in your environment for weeks and months carry out Advanced Persistent Threats (APTs) to get what they’re after. Once they gain access to your environment, they make decisions that further their moves and own interests.

Advanced attackers don’t care how many security layers you have in place or how your network, endpoints, or applications are configured. They know that the weakest link in any security chain is always a person. Attackers bypass security investments by going directly to a human, usually through believable fake emails. Email is the most heavily used application for most organizations and connects everyone internally. An attacker sends hundreds or thousands of invalid email messages, knowing that at least one person will be fooled into thinking the message is legitimate. When the person clicks on a link or opens a malicious attachment, the attacker can plant malware and establish a communication channel back to his command and control.

From this beachhead, he conducts reconnaissance, gathers intelligence, and plans his next move. The next move will be lateral—performing an activity that gets him from the initial entry point to his next target. Every breach is fueled by lateral movement. Without lateral movement, there is no breach.

The Name of the Game is Deception

Attackers use fake credentials and other means to gain entry to your environment. Turning the tables on attackers means beating them at their own game, without catching valid users in the deceptions.

When an attacker lands in an environment, he first has to orient himself. What machine is he on? Who is the user, and what systems and applications does this user connect to? What data is readily available on the system? When the attacker lands on an endpoint, he now has access to a wealth of data, such as bookmarks, registry data, credentials in memory, and connections to real servers and network assets. Based on this data, he will use various tools to scrap credentials for future use, scan the network to see what assets are nearby, execute scripts, or interact with the data to validate that it is real.

The next move is lateral. Depending on the data he collects and his ultimate goal, he might move to another endpoint or to a network asset such as a web server, remote database, or FTP location. Each time the attacker lands on his next hop, he continues this pattern of reconnaissance and data collection using the same, or different, tools to continue progressing through the network to the server, application, or data that he is after.

Unless they are caught.
Using Deception Against Deceivers

Attackers rely on the fact that what they see is real and the data they uncover is reliable. But what if it isn’t? And what if the attacker has to sort between many potential paths instead of just two or three? Using multiple network, endpoint, application, and data deceptions across the infrastructure greatly shifts the odds in your favor.

Network Deceptions
Attackers often scan the network during their initial reconnaissance to identify options for the next lateral move. Network deceptions emulate network protocols, real Windows, Linux, or other machines on the network and are named with the same conventions as the organization’s real machines so that they are indistinguishable. Then, they are multiplied. For example, the attacker might see 10 potential targets—8 of which are deceptive—when he ordinarily would have seen two. To make things even more difficult for the attacker, network traffic deceptions also send fake traffic over the network. Tools that are designed to intercept traffic and eavesdrop on communications now are faced with deception when they try to intercept communications for their own benefit. The attacker’s decision-making becomes much more complicated, and the odds of him choosing a deceptive target—and giving away his presence—are much more in your favor.

Endpoint Deceptions
Endpoint deceptions fool an attacker into believing that he has pieces of information from the endpoint that will get him to his next target. Attackers understand human nature and look for commonly used shortcuts that save time for a user. For example, an IT employee saved his server password so that he didn’t have to reenter it each time he logged in. Endpoint deceptions can be based on passwords, files, registry data, and many other artifacts on the endpoints. When the attacker encounters an endpoint deception, like a password, it appears exactly like a real password. The only difference is that when the attacker tries to log into a target system, the attempt gets him nowhere close to his target, triggers an alert, and he is caught.

Application Deceptions
As you move up the deception stack, deceptions become more difficult to create. Application deceptions blend in with existing applications and enable the attacker to interact with them believably. For example, suppose an attacker is targeting a bank’s wire transfer server. If the bank has deployed application deceptions to protect wire transfers from attack, the attacker might successfully land on a wire transfer server login page with the correct (stolen) credentials—but the page is a deception. When he tries to log in, an alert is triggered. The real login page is never touched.

Data Deceptions
The most difficult deceptions to pull off are data deceptions. The challenge is to create effective and authentic-looking deceptive data and place it inside real applications. Email is a highly effective application for data deceptions. For example, users might email a password to themselves so that they don’t forget it. They send internal emails to other employees that often contain sensitive information. Attackers easily harvest data from emails. Email data deceptions place deceptive data inside real email clients. When attackers try to use the data that they harvested, an alert is triggered.

Dynamic Deception Patterns
As we mentioned earlier, attackers are persistent. Even if they are caught once, they will try again. That’s why deceptions must change dynamically over time as an organization’s network changes. If an attacker successfully gathered intelligence in a previous attempt, he is likely to return and use that data to further the attack. However, deceptions can be automatically moved around, added, or otherwise changed to reflect the current state of the network, so that when he returns, the environment looks different. The attacker has to completely start over, facing new deceptions.
illusive networks
Deceptions Everywhere

Understanding how an attacker thinks enables you to take a truly proactive approach to detection and response. Multiple layers of preventive measures still cannot assure 100% protection against threats. Depending on the organization and its geographic location, the median time that an attacker spends in a network ranges from 99 days (in the Americas) and 106 days (Europe and the Middle East) to 172 days in the Asia Pacific region (M-Trends 2017, A View From the Front Lines, Mandiant). Detecting an attacker’s lateral move early with very high fidelity—is the earliest and single most effective way to stop cyber attackers before they can compromise valuable organizational assets.

Deceptions Everywhere® technology from illusive networks® places a deceptive layer across the infrastructure—endpoints, network, applications, and data—creating a rich maze of false data and what seem to be potential routes to crown jewels. Even an advanced, knowledgeable attacker can't distinguish between real and fake information, and progressing towards your critical assets becomes virtually impossible without being detected. At the same time, illusive deceptions are invisible to valid users, so they do not accidentally encounter them and set off false positive alerts. illusive creates artificial intelligence-based deceptions automatically, instantly diversifies them, and deploys them based on your corporate environment conventions. Agentless technology ensures zero impact to business operations and working environments.

Because valid users can't wander into the layer of deceptions, anyone that does is immediately identified and reported as a threat. Highly reliable alerts without false positives allow you to focus valuable security resources on real threats. illusive detects attackers with 99% accuracy within three lateral moves. It also provides supportive real-time forensics that unveil attack location, path, techniques, and context to accelerate incident response.

Use Deception to Your Advantage

Advanced and state-sponsored attackers are well-funded, aggressive, and here to stay. Take action and turn deception to your advantage. With multiple, highly believable deceptions around them, attackers make incorrect decisions, engage with deceptions, and become disoriented, although they don't realize it. They also are discovered but don't know it. Let illusive show you how to turn the tables using attackers' weapons against them.

For more information, contact illusive today
illusivenetworks.com/contact