How illusive networks Beat the Most Advanced Attackers When the Odds Were Stacked Against Them

Red Team Case Study

illusive

Executive Summary

Not all Red Team exercises are created equal. This was confirmed by illusive networks in a recent Red Team showdown with a Fortune 50 global technology leader (GTL).

The Capture the Flag exercise was conducted on a subset of the GTL's own network and their Red Team took advantage of every opportunity it found to stack the odds against illusive networks'® Deceptions Everywhere® technology.

The Red Team exercise was conducted between January 25, 2016 and February 29, 2016. This gave the Red Team plenty of time to work through the five predesigned subnets to discover one of the success paths to the final objective.

The illusive defense team monitoring the game observed various instances in which the Red Team, comprised of 6 experienced attackers, used tools and techniques that were outside the scope of the game. Just as in the real world, attackers will do anything to win.

The Red Team's willingness to bend the rules of the game was a challenge for the illusive networks® Deceptions Everywhere® cyber-defense solution.

The Red Team had prior knowledge of illusive technology and architecture, and obtained a foothold into the system by accessing the illusive server prior to starting the game and planted a few surprises to help them in their attack.

Although the Red Team was able to make some lateral movements, they were never able to reach the linux server that housed the flag within a MySQL database.

This case study serves as a summary of illusive networks' Red Team exercise with the GTL, highlighting the incidents that illusive networks detected and the forensics information that they yielded.

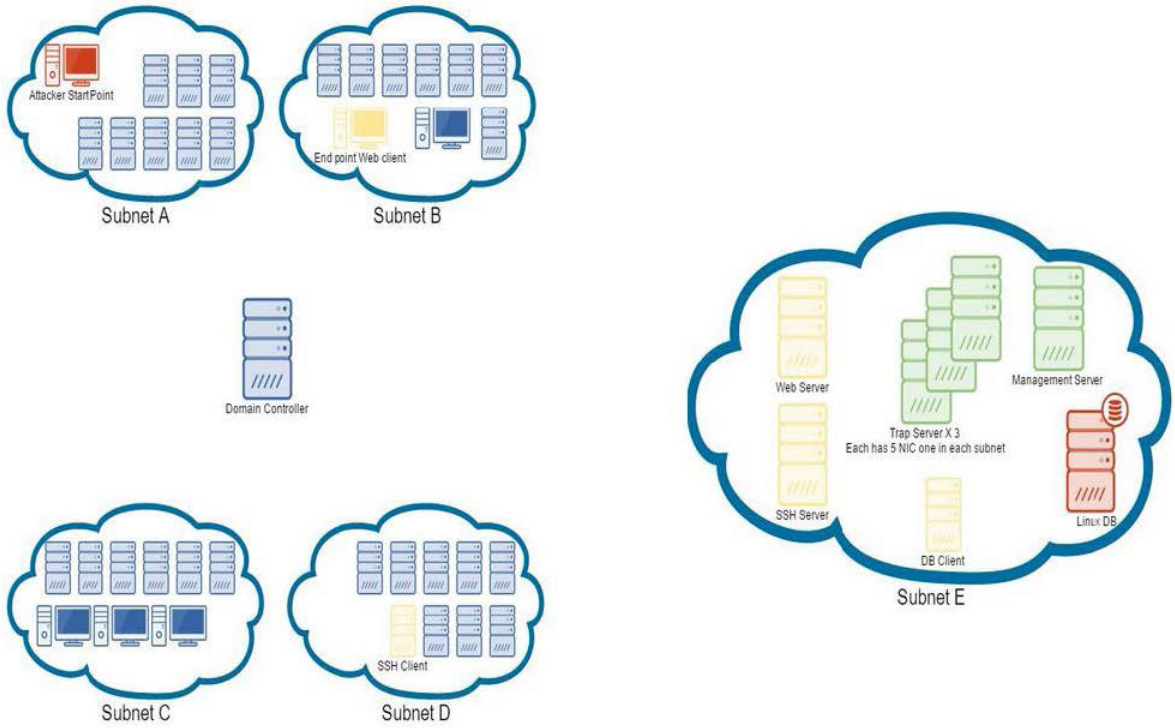
The fact that a system employing illusive networks® Deceptions Everywhere® technology can stand up to a highly-trained Red Team with the odds stacked against it demonstrates how you can protect your systems against increasingly sophisticated cyber-attackers with illusive.

In this report, you'll learn why a threat deception approach to cybersecurity that focuses on the humans behind advanced attacks is the most effective way to deal with modern cyberthreats.

How Exactly Does a Cyber Capture the Flag Work?

The idea of cyber Capture the Flag is fairly simple—one team assumes the offensive role, trying to capture and retrieve a target that is being protected by the defensive team. In this case, illusive networks defined the target: a network diagram, placed on one of the computers within the network.

Refer to the following graphic to see how the environment for this Red Team exercise was designed:



Multiple success paths were available to the Red Team. If any of these were taken, the Red Team attackers would pass through the network undetected, triggering no alerts on their way to the prized target.

In an effort to simulate a real-world attack scenario, illusive networks did not impose any restrictions on the Red Team. All tools and attack methods were available to the offensive team as they pursued the network-design file. illusive networks was ready for the task.

Deceptions Everywhere®: A Technical Overview

Cyber-attackers are slow and methodical, using various tools and techniques to collect data, analyze it and move laterally throughout your network. In a process of trial and error, if given enough time, they will find what they are looking for.

The Deceptions Everywhere® technology, deployed by illusive networks®, combats these attackers by introducing an endless stream of false data to the environment.

Attackers are forced to spend more time sifting through what's real and what's illusive, enabling the detection system to alert you of the attack. Product configuration installs two new servers on two machines on the network—the illusive Management Server™ and illusive Trap Server™.

The Management Server deploys deceptions across the network and defines them using company-specific information, making them appear real. Deceptions are not universal—they are crafted specifically for the organization deploying them.

Because the technology is agentless, there are no running executables with which attackers interact. The deceptions are deployed in a way such that attackers find the deceptions, but the employees do not.

By segregating the deceptions to the attacker's side, illusive networks virtually eliminates all false positives. When an alert is triggered, IT can address it because an illusive alert equals an attack. In the end, Deceptions Everywhere® technology is built to take the power out of the attacker's hands and return it to the IT department.

The Deceptions Everywhere® technology, deployed by illusive networks®, combats these attackers by introducing an endless stream of false data to the environment.

Deception Strategy: How illusive Approached the Red Team Exercise

When the network environment was ready, illusive deployed deceptions throughout the network. Multiple deception types were placed on each VLAN, but what does this really mean? To maintain customer security, illusive deception types are proprietary and confidential, but example deception families include:

- **SSH Deceptions**
  The information provided in this family helps lure an attacker to reach for a non-existant SSH server.

- **Share Deceptions**
  These deceptions dupe attackers to access non-existent shared folders.

- **Windows Deceptions**
  This information ensnares attackers with non-existent domain credentials.

The Deceptions Everywhere® solution tailors all of these deceptions to specifically suit the network being protected.

The solution tailors all of these deceptions to specifically suit the network being protected. The names of shared folders and servers are created to match the rest of the environment, making attackers second-guess their every move.

The illusive networks® Deceptions Everywhere® solution deploys different sets of deceptions across the assigned computers throughout the network, ensuring attackers can't grow complacent and rely on any consistent data. With a network of deceptions in place, illusive networks was prepared to face the Red Team's comprehensive 30-day attack.

Incidents Detected by illusive networks

Throughout the 30-day exercise, the illusive networks® Management Console™ alerted the defensive team to multiple incidents triggered by the Red Team. For the sake of the exercise, illusive networks allowed the Red Team to continue even though each individual alert gives defenders the opportunity to address threats and trace attackers.

With illusive networks'® Deceptions Everywhere® technology in place, these are some of the incident alerts that the Management Console identified in this GTL Red Team exercise:

- **ICMP Scanning (Jan. 28 to Feb 29)**
  The Red Team tripped over deceptions when conducting a ping sweep, gathering TTL and payload length data for live hosts in the environment. 19 of these incidents were detected in just 3 days.

- **Share Access (Jan. 31)**
  The Red Team tried to compromise a deceptive user, **diskdrv**, to access the C: drive and the IPC$ share. Their intent was to compromise inter-process communications and take control of remote command protocols. **diskdrv** was lowhanging fruit with the common password, “Pass123.” The Red Team fell for the deception.

- **SSH Port Scanning (Feb. 9)**
  illusive detected 13 incidents in the course of a few hours. The Red Team scanned the entire environment for open SSH over port 22. By using **powershell.exe**, the Red Team took advantage of a misconfiguration and disabled programs to launch remote commands.

  The Red Team modified registry keys, made a remote desktop connection and executed a file called **b-B.exe**. This executable copied to the machine prior to the beginning of the exercise allowed meterpreter to run on the machine for credentials theft and privilege escalation.

- **Windows Domain Credentials (Feb. 12)**
  The Red Team set off alerts when it failed to authenticate a domain admin: **forescout_admin**.

- **Browsers (Feb. 18)**
  From the attackers' starting point, the Red Team triggered alerts by using a web-access technique on one of the illusive networks® Trap Servers. The Internet Explorer process that initiated the incident was non-malicious. However, **diskdrv** was involved in an open connection that could have been used to transfer tools and files.

- **Database (Feb. 26)**
  The Red Team injected a conhost.exe executable via remote connection to try and log into an **MSSQL** database—which was deceptive and triggered alerts.

The Red Team found some ways to move laterally through the environment but ultimately, the majority of its moves interacted with a deception server or machine and triggered alerts. The exercise continued, but in a real-world environment, IT departments can act upon these alerts as they see fit.

Real-World Surprises in the Red Team Environment

Just like in the real-world, this Red Team exercise was not entirely predictable. Throughout the month of targeted attacks, a number of issues emerged. These are some of the surprises that allowed the Red Team to gain more traction in the network:

- **Disabled Firewalls**
  illusive found that it misconfigured the environment and unintentionally disabled its Traps' firewalls. This led to one of the most effective Red Team movements—the use of **b-B.exe**.

- **External IPs Introduced**
  Midway through the exercise, illusive identified an IP address that belonged to the GTL but was not in the scope of the game. A Share incident was initiated by this source and was dealt with.

While these surprises weren't expected in the Red Team exercise, they serve to prove that Deceptions Everywhere® technology is effective even in a more unpredictable real world setting.

The key to illusive's approach is a focus on the human behind attacks—not just specific attack vectors. This approach offers a number of important benefits to your organization.

What Can illusive networks'® Deceptions Everywhere® Technology Do for You?

Consider the two main sections of your cybersecurity spending—detection and protection. Many companies are content to spend the majority of their budget on protection—new firewalls, IPS, and security applications that claim to prevent all attacks. However, cyber-attackers are relentless and can customize their attacks and find a way to penetrate your network.

Post-breach detection and response must be higher on the security priority-list because if your network is infiltrated, you'll need to detect the attack and respond immediately.

Deceptions Everywhere® technology provides key benefits for any mid-size, enterprise, or large enterprise company looking to finally get ahead of cyber-attackers:

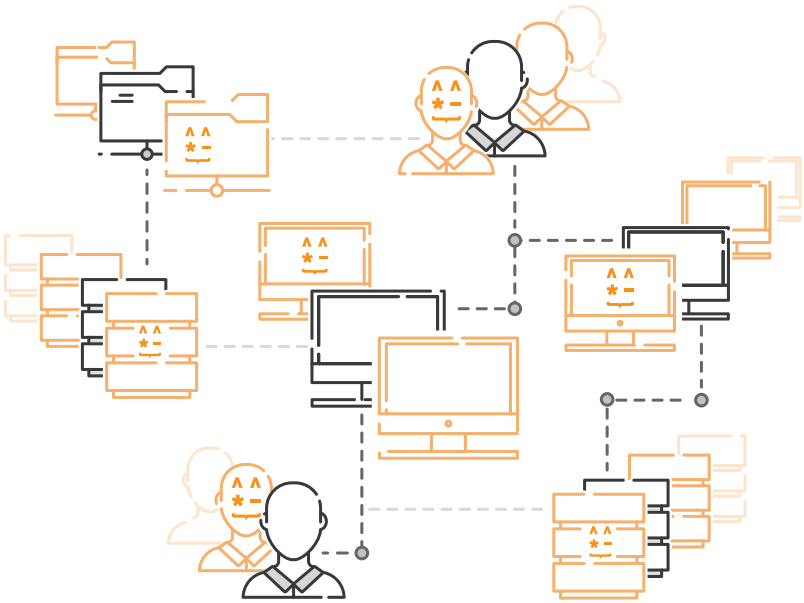
- **Agentless, Cost-Effective, and Ever Changing**
  Improve your security posture without introducing complicated and expensive management applications on endpoints. Network users don't interact with deceptions, so employees are free to work uninterrupted. Threat deceptions are indistinguishable by attackers from real network information. illusive provides a scalable solution with seamless, rapid updates of new, ever changing threat deceptions to stay ahead of innovative cyber-attackers.

- **High Detection, Low Maintenance is Unique**
  Current security solutions have low detection rates and high maintenance costs. This is why honeynets and SDN diversions haven't been effective in the business world. Deceptions Everywhere® is a multidimensional solution that is customized for each environment, distancing it from context-less competitors.

- **Actionable Detection for Greater Security**
  The real-time source-based forensic data provided by the Deceptions Everywhere® architecture detects attacks very early to empower IT to either stop cyber-attackers in their tracks or follow their every move to learn their methods.

  Many security solutions fail to identify an attacker until data is already lost. Deceptions Everywhere® detects attackers during their first lateral movements and provides the attack path with contextual information giving you ample time to respond.

The GTL Red Team learned first-hand how Deceptions Everywhere® architecture innovates beyond the cybersecurity norm. The Red Team exercise simulated real-world environments.



If one of the best global Red Teams couldn't capture a flag protected by illusive networks' Deceptions Everywhere® architecture, your network will be protected too.

Are you ready to learn how illusive networks will keep your network safe?

Visit illusive networks or call 1-844-ILLUSIVE. Stop falling behind attackers by focusing on their attack vectors—cut off the head of the threat by fighting back against the humans behind targeted attacks.