illusive®

Deceptions Everywhere

Solution Brief

illusive

Advanced Persistent Threats: Sophisticated attacks

Advanced attacks target organizations with a clearly defined target. Inside a compromised network, attackers use trial and error to slowly and quietly expand their access until their mission is complete. Throughout an attack, attackers constantly seek answers to the following questions: Where am I? Where is my target? How can I get from here to there?

Iteratively, they collect data, analyze it, and use it to move laterally. These attackers are persistent. They do not stop until they find what they are looking for – whether it is a credit card database, file-server with client-information, or any other sensitive asset. These attacks are called Advanced Persistent Threats (APT).

Due to the growth of the Crime-as-a-Service model, Europol's 2016 Internet Organized Crime Threat Assessment report stated that APT attacks are expected to continue increasing, targeting a growing number of industries. These attacks pose not only a financial threat to targeted companies, but also a fundamental threat to their brands. For example, excluding legal costs, Target's 2013 APT cost the retail giant $162 million while Forbes business magazine reported that, for that year's final quarter, sales declined by almost 50% and up to 10% of customers indicated that they would never shop there again.

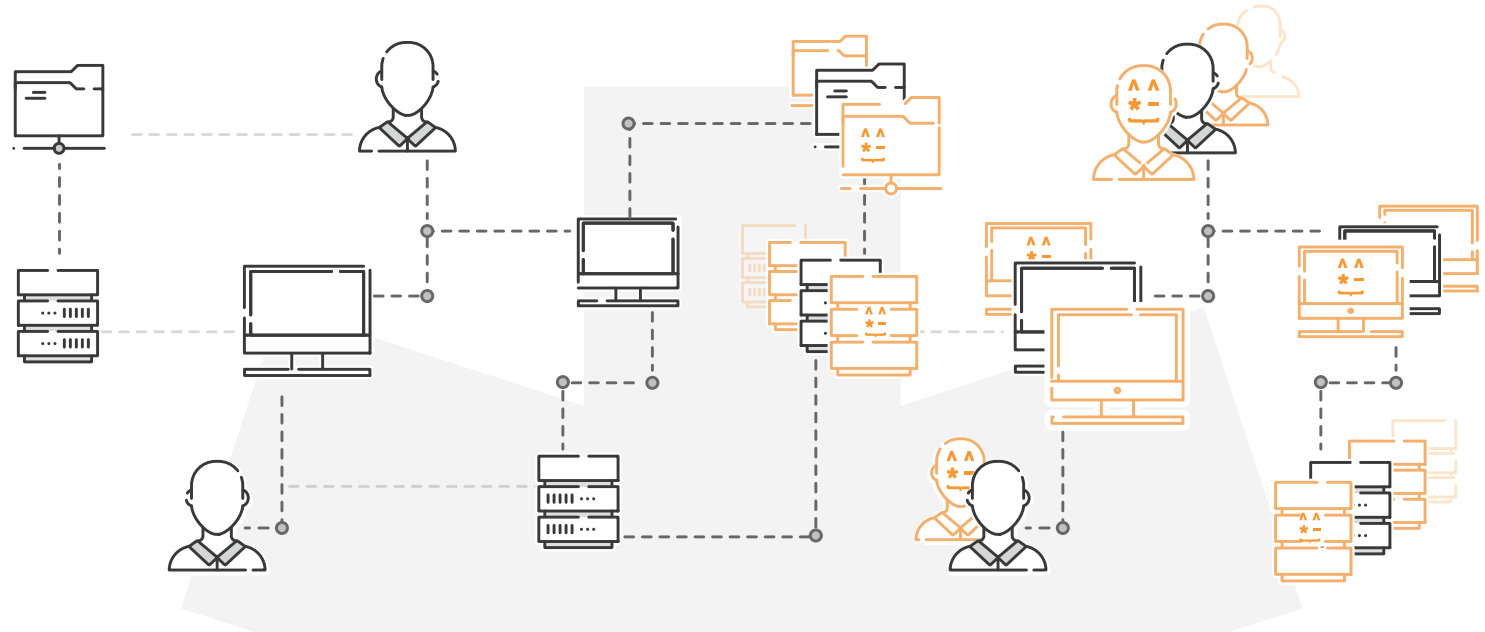
Deceptions Everywhere: The illusive difference

illusive exposes attackers by turning their strengths into weaknesses. Advanced attackers rely on one simple fact: that what they see is real and that the data they collect is reliable. The revolutionary illusive networks Deceptions Everywhere® solution weaves a deceptive layer over your entire network, creating an environment where attackers cannot rely on the information they collect. If attackers can't collect reliable data, they can't make decisions. And if they can't make decisions, the attack is paralyzed. With every endpoint, server, and component coated with illusive deceptions, attackers cannot avoid detection.

As illusive deceptions are invisible to authorized users and systems, no false-positive alerts are triggered; every notification of deception-use is a high-fidelity indication of an attack.

illusive's actionable alerts provide the real-time forensic information needed to investigate and contain attacks. Information is collected from compromised hosts at the exact moment that attackers use false data, before they have time to clean their tracks.

Using the illusive Deception Management System™ (DMS), deceptions are automatically optimized, instantly diversified, and constantly monitored. The intuitive DMS interface makes deploying and scaling a solution quick and easy, while the agentless technology ensures zero-impact to business operations and working environments.



Real Network

Network with Deceptions

illusive

About illusive networks

illusive networks is a global pioneer of deception technology – the most effective protection against advanced attacks. To lead the Distributed Deception Platform, top cyber-attack specialists from Israel's elite cybersecurity Intelligence Corps (unit 8200) were brought together with pioneering experts and entrepreneurs with over 50 years of combined experience in cyber-warfare and cyber-security.

With offices in Tel Aviv and New York, illusive networks changes the asymmetry of cyber-warfare by focusing on the weakest link in a targeted attack – the human team behind it.

For more details, visit www.illusivenetworks.com or contact info@illusivenetworks.com.

"By 2019, continued weaknesses in prevention will drive at least 10% of large enterprises to adopt deception-enabled tools and tactics (up from just 5% in 2016), improving detection and response, and shifting some of the economic burden to attackers."

Gartner Competitive Landscape: Distributed Deception, August 2016

A Unique Approach

- *illusive's Deception Management System (DMS) automatically manages, distributes, and monitors dynamic deceptions*
- *Attackers reveal themselves long before reaching sensitive data*
- *The earliest attack-alerts in the industry*
- *Highest-fidelity alerts available*
- *The most detailed, real-time source-based forensics attainable*

"illusive networks is a perfect example of the kind of 'out of the box' thinking necessary to challenge the growing threat of targeted attacks."

Eric Schmidt, Google Chairman and Founding Partner at Innovation Endeavors