Illusive Networks

RED TEAM CASE STUDY

How Illusive Networks' Forensic Analysis Uncovered Aggressive Attempts To Insert Malicious Tools And Breach Servers In A Bank's Network

Executive Summary

Illusive Networks conducted a capture the flag exercise on the network infrastructure of a large Middle Eastern bank as part of the bank's regular penetration testing procedures.

The exercise was conducted over 22 days. The bank had engaged a highly credible third party testing company to attack its network. Unbeknownst to the testing company's team, the bank also installed Illusive Networks' deception technology in its infrastructure.

On Day 1, Illusive began a process of forensic analysis in response to an alert. Illusive deception technology generated the alert when it detected malicious activity on one of the company's Citrix servers, SERVERA, by user USERA. Responding to the alert, the Illusive forensic team found the methods used by the attacker to insert malicious tools inside the customer's network and attempt to exfiltrate data.

On Day 22, Illusive conducted a second forensic analysis in response to new alerts in the bank's network. Again, Illusive detected malicious activity by USERA, this time on another server, SERVERB. The team also discovered aggressive attempts to log into critical accounts using two different sets of deceptive user credentials.

This case study serves as a summary of Illusive Networks' Red Team exercise with the bank, highlighting the incidents that Illusive detected and the forensic information that they yielded. The fact that a system employing Illusive's deception technology can stand up to an expert, third-party testing company, with all attack tools and methods at its disposal, demonstrates how financial services organizations can use Illusive Networks to protect their systems against increasingly sophisticated cyber attackers.

In this study, you will learn why a threat deception-based approach to cybersecurity, focusing on the human element behind advanced attacks, is the most effective way to deal with modern cyber threats.

- Capture the Flag exercise
- 22 days
- Highly credible 3rd party testing company
- Illusive Networks' deception technology detected malicious activity and aggressive attempts to log into critical accounts
- Demonstrates how organizations can use Illusive to protect their systems against increasingly sophisticated cyber attackers

How Exactly Does Cyber Capture the Flag Work?

The idea of cyber capture the flag is fairly simple. One team takes an offensive role trying to capture and retrieve a target that is being protected by the defensive team. In this case, Illusive Networks functioned as a silent defensive team to analyze malicious activity targeted at the bank's Citrix servers.

The attackers had multiple success paths available to them and no knowledge of Illusive's presence in the network. If the attackers made a series of correct choices, they would pass through the network undetected, triggering no alerts on their way to their target. Attackers had access to all attack tools and methods, but Illusive had the advantage of deception.

ILLUSIVE'S DECEPTION TECHNOLOGY COMBATS ATTACKERS BY INTRODUCING AN ENDLESS STREAM OF FALSE DATA TO THE ENVIRONMENT THAT ONLY ADVERSARIES WILL SEE.

Inescapable Deceptions: A Technical Overview

Cyber attackers are slow and methodical, using various tools and techniques to collect and analyze data and move laterally throughout a network. Through trial and error, with enough time they will find what they are looking for. Advanced attackers rely on the fact that what they see is real and that the data they collect is reliable.

Illusive's deception technology combats attackers by introducing an endless stream of false data into the environment. Attackers unknowingly encounter carefully crafted deceptions deployed across the entire network---on endpoints, servers and attack surfaces---that appear identical to what the attacker needs in order to move laterally in the bank's network. False data forces attackers to spend more time sifting through what's real and what's illusive, giving the Information Security (InfoSec) team data and time to make strategic decisions as early as possible in an attack.

In this exercise, Illusive deployed deceptions that appear real to an attacker across the network. When an attacker accesses a deception on an endpoint, the interaction automatically begins running real-time forensics on the source of the attack.

Illusive's deceptions are not generic---they are intelligently crafted specifically for the organization deploying them and defined using information specific to the company's network. Because the Illusive technology is agentless, attackers do not interact with running executables. Deceptions are deployed in such a way that attackers find the deceptions, but employees do not. By segregating deceptions to the attacker's side, Illusive virtually eliminates all false positives. High-fidelity alerts enable the InfoSec team to immediately address an incident, knowing that the attack is real.

In the end, Illusive Networks' deception technology is built to take the power out of the attacker's hands and return it to the organization's IT and security departments. Illusive deceptions are **inescapable**.

Deception Strategy: How Illusive Approached the Red Team Exercise

Illusive deployed deceptions to every endpoint within the customer's 5,000-node network and customized the deceptions based on specific data and topology for a banking environment.

- **Share deceptions dupe attackers into accessing fake shared folders and files**
- **Windows credentials deceptions ensnare attackers with nonexistent domain credentials**
- **File deceptions induce attackers to access and use credentials stored in fake files**

Different sets of deceptions are deployed across the assigned computers throughout the network, ensuring that attackers can't grow complacent and rely on any consistent data. With a web of deceptions in place, Illusive was prepared to face the penetration testers.

ILLUSIVE TAILORS DECEPTIONS TO SPECIFICALLY SUIT THE NETWORK BEING PROTECTED.

The Battle Begins

Incidents Detected by Illusive Networks

Illusive Networks' deception technology delivers real-time forensic data from the source of the attacks. As the attacker engages with deceptions placed in the network, Illusive detects, alerts and analyzes the attacker's movements. Between day 1 and day 22 of the exercise, Illusive's technology alerted the bank's security operations center (SOC) team to multiple incidents triggered by lateral movements involving attempts to engage with deceptive servers.

DAY 1

Using Domainname\USERA, the attacker logged into the bank's network. With Internet Explorer, the attacker downloaded malicious text files to the bank's domain, opened them with Notepad and saved them in a shared folder on the bank's network.

DAY 1 cont'd

Attackers then executed a powershell.bat command and opened a PowerShell script named powerUp.ps1.

They converted additional text files into executable binaries and attempted to access SERVERC/deceptivename. This triggered an Illusive alert.

In this attack, it appears that the attacker was able to download an arsenal of malicious tools into the bank's network and prepare for the next phase of moving laterally in the network. When the SOC team used Illusive's forensic analysis to examine a folder created by the attacker, it found the PsExec tool, which allows users to execute processes on remote systems. Additionally, the sysret.exe and MinHookx64.dll attack tools that were found allow for privilege escalation.

DAY 22

The attacker logged into SERVERB using the same account as before. This time, he created a new file in the shared folder. Three minutes later, he attempted to log into one of the bank's Citrix servers using a deceptive file name, which triggered an Illusive alert.

Later that morning, the attacker used a system tool named msinfo32 under C:\Windows\System32, and discovered deceptive server, SERVERC, which he tried to access. This also triggered an Illusive alert and was forwarded to the SOC's Security Information and Event Management (SIEM) tool.

Within 10 minutes, the attacker saved more tools and data gained by netstat.exe and systeminfo.exe to the shared public folder. Several hours later, he created new text files (Test_File_Upload.docx and Test_File_to_Download.xlsx) in the shared public folder. He then began an aggressive attempt to log into another server with a different deceptive user credential, which again triggered Illusive alerts. The attacker managed to save files named Credit_Card_Numbers.docx and Credit_Card_Numbers.xlsx to the shared public folder.

In the second incident, the attacker downloaded his desired weapons to the bank's network and appeared to have several objectives. One goal was to move laterally. Another was to conduct a lockout of privileged accounts. The attacker tried to lock out a critical account---a member of the Domain Admin group---by attempting multiple automated log-ins. Finally, the attacker tried to exfiltrate confidential information. Files in the shared public folder indicate that the attacker probably scraped credit-card numbers from a compromised machine and was preparing to exfiltrate them.

Recommendations

Early detection of suspicious behavior enables the SOC and InfoSec teams to block attacks in several ways. Illusive forensic analysis assists with mitigation processes.

Correlating a general brute-force event with Illusive's alerts on attempts to use deceptive accounts ensures a reliable alert---a 100% true positive of malicious activity in the network.

illusive®

What Can Illusive's Deceptions Do For You?

Consider the two main sections of cybersecurity spending: detection and protection. Many financial services companies are content to spend the majority of their efforts on compliance and their budget on protection---new firewalls, intrusion prevention systems (IPS) and security applications that claim to prevent attacks. However, cyber attackers are relentless and continue to customize their attacks until they find a way to penetrate the network.

Post-penetration detection and response must be higher on the security priority list. When---not if---the network is infiltrated, InfoSec and SOC teams must detect the attack and respond immediately. Illusive's deception technology provides critical benefits for any mid-sized or large enterprise organization looking to finally get ahead of cyber attackers.

> The penetration testers learned first-hand the power of Illusive Networks' innovation. This exercise simulated real-world environments. If one of the best testing companies couldn't capture a flag protected by Illusive Networks, your network will be protected too.

Illusive is Agentless, Cost-Effective and Ever-Changing:

- Illusive improves the organization's security posture without introducing costly, complicated management applications on endpoints. Legitimate network users don't interact with deceptions, so employees are free to work uninterrupted. Attackers cannot distinguish threat deceptions 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.

Illusive Provides Unprecedented High Detection and Low Maintenance:

- Current security solutions have low detection rates and high maintenance costs. This is why honeynets and software-defined network (SDN) diversions haven't been effective in the real world. Illusive's inescapable deception technology provides a multi-dimensional approach, customized for each environment. The ability to detect attackers early---within three lateral moves---with 99% reliability puts Illusive Networks far ahead of competitive solutions that lack context.

Illusive Provides Actionable Detection for Greater Security:

- Many security solutions fail to identify an attacker until data is already lost. Real-time, source-based forensic data provided by Illusive's deception technology empowers IT to stop cyber attackers in their tracks or follow their every move to learn their methods.

TO BEAT AN ATTACKER, YOU NEED TO THINK LIKE AN ATTACKER.

For more information

Visit us at www.illusivenetworks.com

Email us at info@illusivenetworks.com

Call us at +1 844.455.8748 (North America)
or +972 73.272.4006 (EMEA and AsiaPac)

Illusive Networks stops cyberattacks by destroying attackers' ability to make safe decisions as they attempt to move toward their targets. Using Illusive, organizations eliminate high-risk pathways to critical systems, detect attackers early in the attack process, and capture real-time forensics that focus and accelerate incident response and improve resilience. Through simple, agentless technology, Illusive provides nimble, easy-to-use solutions that enable organizations to continuously improve their cyber risk posture and function with greater confidence and agility.