CASE STUDY

Financial Company Upgrades Data Security with Fidelis Deception*

The Company

Headquartered in Chicago, Illinois, the company is a global provider of research data on investment offerings including stocks mutual funds, and similar vehicles. The company operates in more than 20 countries and has over $180 billion in assets under advisement or management.

Threats and Challenges

As a leading financial services firm, the company, is well aware of the high risk posed by cyberattacks. As such, the company is committed to building a secure work environment where information can be stored, shared, and communicated safely without risk of financial loss, violation of customer records or integrity, or damage to reputation.

With the number of cyber-threats constantly on the rise, it has become apparent that the largest losses come from attacks that were not quickly detected. Fully aware of the constant risk, the company's security team sought a solution that would provide real-time detection of attacks on their valuable data assets. In addition, the team required fully correlated information of their network traffic along with operational alerts based on relevant threat intelligence.

Seeking a Solution

Today's cyber attackers use sophisticated tools and are better organized and more persistent than ever before. Therefore, the company understood that it must change its security mindset from 'keep them out' to 'they're already inside-and we need to find them before they cause any harm'. After evaluating a number of solutions, the company's security team selected Fidelis Deception for its deception-based technology and in- depth network visibility capabilities.

Unlike other security solutions that rely on signature updates, Fidelis Deception is completely malware-agnostic, making it ideal for rapid detection of APTs and zero-day attacks.

Benefits

- Detect advanced persistent attacks in progress
- Detect zero-day attacks
- Gain critical insight about potential threats
- Enhance existing security tools
- Comply with regulations concerning data security

The solution focuses on setting up decoys, traps, and breadcrumbs that mirror real corporate assets, deployed automatically to create an active deception that engages with, lures, and traps attackers.

Fidelis Deception also provides comprehensive visibility of all inbound and egress traffic including DNS, TCP/IP, HTTP, SSL, home-grown apps, and more. The combination of the deception and visibility engines makes Fidelis Deception the most powerful tool for exposing advanced attacks in their initial phases.

The data that Fidelis Deception collects and records can be analyzed easily using the solution's intuitive dashboard and reports, or it can be fed into 3rd party SIEM/SOC solutions. The granularity and breadth of the data, as well as the speed at which it can be retrieved, empowers administrators with easily understood, actionable network and threat intelligence.

*formerly Topspin DECOYnet

Setting Decoys

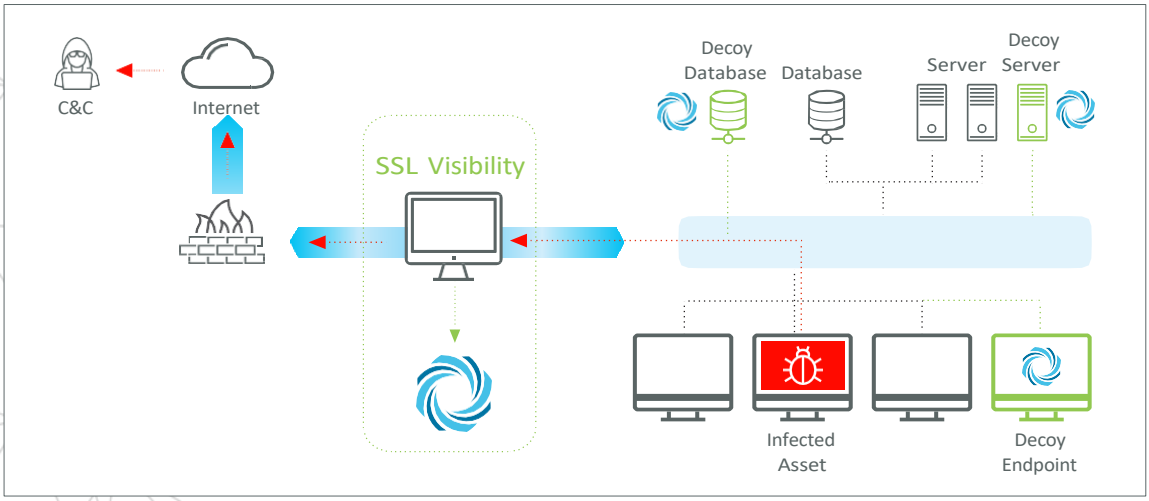
Fidelis Deception creates decoys that behave like real network assets. Once in place, the decoys 'advertise' themselves in order to attract intruder attention, for example, by using NetBIOS queries or having the decoys answer pings, queries, or scans. To increase friction with the attacker and to draw their attention away from real network assets, Fidelis Deception deploys breadcrumbs. These are fake credentials and bogus data that are distributed onto organizational assets (endpoints, servers, etc.). The breadcrumbs actively lure attackers into the decoys ultimately exposing them and allowing security teams to take quick action to resolve the problems they might cause.

An Active Defense Layer

Fidelis Deception's active deception layer goes beyond breach detection. Using the platform, the company's IT staff can continuously monitor breached data, engaging with attackers instead of just blocking them, to gain valuable intelligence about their intentions and origin. "Fidelis Deception gives us actionable threat intelligence so that we can focus our efforts on solving problems quickly," said the company's CISO. "It really makes our job much easier and allows us to keep our customers' data safe and secure."

"Fidelis Deception* gives us actionable threat intelligence so that we can focus our efforts on solving the problem quickly."

~ The Company's CISO



*formerly Topspin DECOYnet

Contact Us Today to Learn More About Fidelis

Fidelis Security | 800.652.4020 | info@fidelissecurity.com

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.