ALLURE

ALLURE SECURITY FOR ACTIVE INVESTIGATIONS

REDUCE TIME & COST OF INVESTIGATIONS BY PIERCING TOOLS HACKERS AND LEAKERS USE TO REMAIN ANONYMOUS AND AVOID ACCOUNTABILITY

Cyber attackers and leakers thrive on anonymity. They feel comfortable making bold attacks and demands because they are confident in their abilities to hide their malicious activities and identities. Leakers rely on their knowledge of systems and process to hide activity, and then use secure email and messaging tools to leak confidential data. Hackers rely on masquerading as legitimate employees via phishing attacks and stolen credentials, and negotiate ransoms and demands via secure chat tools.

These stealthy techniques often leave security teams in the dark, even after they become suspicious or aware that malicious activity has occurred. When an incident investigation is triggered, the investigators often rely on word of mouth, hunches based on various log data, and suspicions from historical actions of employees or adversaries, to come up with a short list of potential suspects. But then what? How do you narrow the lists of suspects or confirm that the perpetrator is on the initial list? How do you reveal the actual bad actor and hold that person accountable?

Allure Security uses attacker behaviors and confidence to the advantage of investigators. Using Allure Beacons embedded in real or decoy documents, incident investigators can:

1. Narrow and eliminate suspects by planting or sharing alluring documents with beacons to see who takes the bait. Once documents are opened, investigators will receive proprietary geofence and telemetry insights.

2. Reveal attackers and leakers by correlating Allure's proprietary geofence and telemetry insights with other available data.

3. Hold attackers accountable by sharing identifiable findings with law enforcement.

4. Reduce investigation cost and effort using Allure's affordable, easy to deploy method, and provide the opportunity to follow more hunches that previously were pushed off due to cost and time restrictions.

A Ransomware Attacker Revealed

A large telecom company experienced a ransomware attack that seemingly utilized portions of the NSA leaked malware. Post-attack forensics determined that the adversary had penetrated the organization through a vulnerable set-top box, which then allowed the attacker to riffle through the organization's folders and directories, and exfiltrate data.

Identifying this attacker, thwarting the attack in its final stages and not paying the ransom became a top priority. Allure stepped in to help. In order to receive the ransom, in bitcoin of course, communication between attacker and target was conducted via the typical Tor chat protocol. The attacker was clearly feeling quite protected and proceeded to conduct his business without fear of being caught.

However, while the telecom company claimed that it had paid the bitcoin ransom, in actuality it had not. Instead, the company's CISO used an Allure Decoy Document, disguised as a bitcoin payment page. The attacker received the confirmation page over Tor and proceeded to open and review the document on his phone. The beacon triggered an alert upon opening, and conveyed geofencing and telemetry insights that allowed the security team to reveal the attacker via his phone service provider. This person is now well known to Interpol.

A Greedy Insider's Plans Are Foiled

A large enterprise experienced a stock tampering case that demonstrated a financial fraud attack. In this scenario, the indicator was sensed from public sources arousing suspicions that lead this enterprise to investigate whether it had a rogue insider illegally benefiting from inside knowledge of an impending acquisition. It was clear that the insider was leaking and manipulating news about the target company to affect its market valuation. Allure Decoy Documents with compelling information about the target company were strategically placed in file shares. One of the documents was later opened externally at the home of the alleged inside attacker, triggering an alert, surfacing his identity and providing proof for law enforcement. The FBI then did its duty.

Deployed As A Service

Delivered entirely as a service, Allure Security requires no software to download, no agents to install and no hardware to configure. Allure is the only company to hold patents for document beacons, making it completely unique in the market. See all patents here: http://www.alluresecurity.com/patents.

Request a trial: http://info.alluresecurity.com/free-trial