ALLURE

ACTIVE BREACH DEFENSE

PATENTED DECOY DOCUMENTS IN THE OPERATIONAL ENVIRONMENT THAT PROVIDE ACTIONABLE, REVEALING INTELLIGENCE

DETECT, RESPOND, IDENTIFY

The inability to detect and understand modern attacker-type breaches has created new interest in deception technology. To date, deception products have mostly focused on the build out of complex 'honey' environments designed to lure attackers into fake environments to distract and track their behaviors. However, the value compared to the effort required to create and maintain these honey environments on an ongoing basis has hindered adoption. For those who have invested, success comes at a high cost. First, you need to establish an environment that mimics the operational environment in order to have any chance that attackers will believe it is real. Then, that environment must be populated and maintained on an ongoing basis to keep it realistic. Additionally, hackers have become increasingly sophisticated in identifying even the slightest 'tells' in these honey environments, so they can more quickly go back to the operational environment to continue their pursuits of finding and exfiltrating confidential data, undetected. To combat this, complex deceptive assets must constantly be deployed to keep attackers engaged. This poisons asset management, which creates headaches for IT operations teams, and provides very little actionable intelligence to security teams.

At Allure, we recognize the need for deceptive techniques, but understand the challenges with deploying honey environments at scale. Our approach is to deploy deception in the real operational environment, eliminating the need for a honey environment and its large burden on IT operations and security teams. We do this by dropping patented Allure Decoy Documents, deceptive documents embedded with beacons, in operational folders, directories and cloud shares, creating an alarm system with GPS for confidential data. When Allure Decoy Documents are opened, real-time alerts are generated with proprietary geofence and telemetry insights to detect early breach activity, respond with countermeasures, and identify leakers and hackers. This approach is entirely agnostic to whatever the attack vector may be: nation state, insider threat, programmatic APT, drop in malware. It doesn't matter - the data becomes the instrumentation.

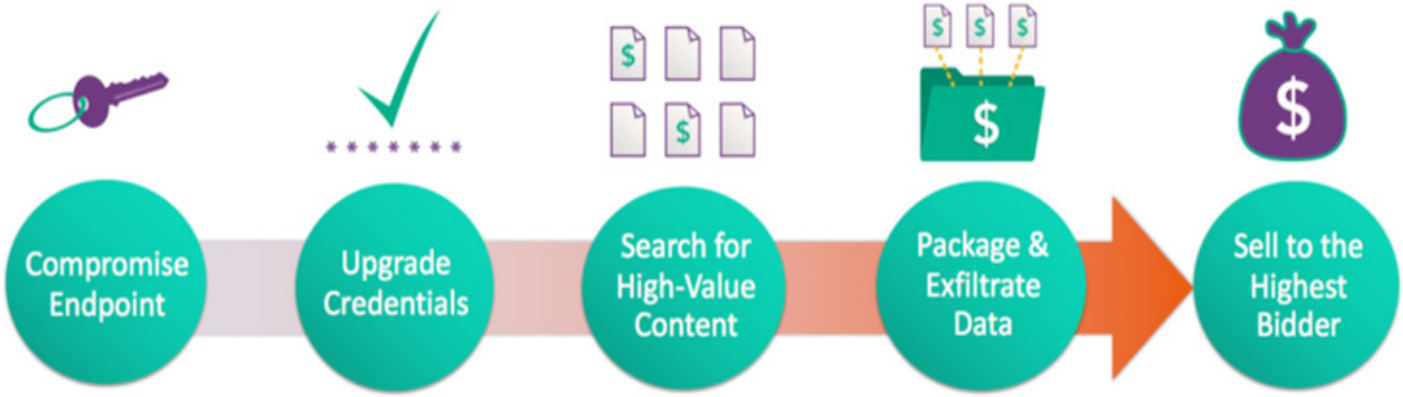
Detect

The longer a breach goes undetected, the longer attackers have to hone in on intended targets and take their time exfiltrating large stores of data, resulting in costly losses. According to the Ponemon Institute 2018 Cost of Data Breach Study, sponsored by IBM, there is a 28% (1 in 3) chance a business will suffer a breach within the next two years, resulting in a $3.6 million loss based on the average cost of a data breach. Furthermore, according to the study, detection of a breach within 30 days or less (rather than the average 197 days) saves the company $1 million in costs.

The team of security professionals guarding an enterprise needs to be right all the time in order to prevent a breach. But a bad actor has to be right only once. For every 50-foot virtual wall that a defender may build, all it takes is one hacker's 51-foot virtual ladder to get what they came for in the first place: confidential data. Once they've gained access to thier targets, via stolen credentials, a compromised third party or other means, attackers will execute a series of actions designed to remain undetected.

*Ponemon Institute, https://www.ibm.com/security/data-breach

*DARPA: http://ids.cs.columbia.edu/sites/default/files/CSET_2011_0.pdf



Patented Allure Decoy Documents are 98% effective in detecting early-stage breach activity, according to DARPA research.

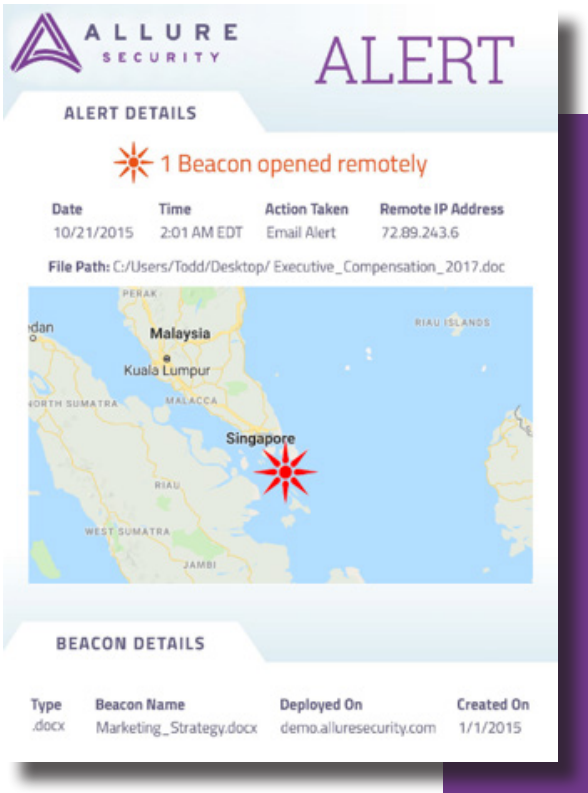
This is because our approach combines the power of deceptive documents and beacons, with decades of studying attacker behavior and how to leverage it to defeat attackers. Allure Decoy Documents are strategically placed to align with the attacker behavior depicted above, and security teams don't just know if planted documents are opened, but receive alerts with proprietary geofence and telemetry insights. This actionable information initiates and informs real-time response to defend the organization and catch attackers.

Respond

Allure Decoy Documents track and report on breaches in progress using a deceptive technique at the data level that is undetectable by attackers. This creates a unique advantage for incident response teams. Rather than luring attackers into a honey environment and relying on distraction that only slows an attack, the beacons in Allure Decoy Documents alert incident response teams to malicious activity in real time, without the attacker knowing he or she has been detected. The proprietary geofence and telemetry insights gathered from every opening is logged, and alerts are generated based on desired criteria. Attackers continue to hunt thinking they are succeeding, but instead have revealed themselves and are now sitting ducks. Incident response teams can take immediate steps to thwart the attack and use the alert insights to take corrective actions to prevent future incidents.

*DARPA: http://ids.cs.columbia.edu/sites/default/files/CSET_2011_0.pdf

Allure alerts provide high-value information to aid incident response and architecture review. Once an Allure Decoy Document is opened and the beacon is triggered, the following actions can be taken during and after an attack to reduce overall risk:



Active Breach Defense:

1. Revoke access using available permission controls
2. Update employee training procedures to prevent future attacks
3. Invoke internal endpoint controls to isolate the breach source
4. Move critical files that are at risk of being stolen
5. Address endpoint vulnerabilities that contributed to the breach
6. Plant more Allure Decoy Documents based on attack insights to narrow down suspects; identify leakers and attackers
7. Invoke penalty clauses if the breach is caused by a third-party
8. Gather forensics to determine the extent of a threat by correlating with other threat intel
9. Detect if lost documents are posted on public websites
10. Update data security and compliance policies based on findings

Identify

Revealing attackers and uncovering identities remains a vexing problem for security teams, and deception techniques are uniquely poised to meet this need. Since the beacons embedded in Allure Decoy Documents are undetectable by attackers, they can be used very effectively in active investigations, both inside and outside the operational network, to identify leakers and hackers. Allure has helped numerous companies identify external adversaries and insider threats. For example:

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.

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.

Deception Made Easy, Deployed As A Service

Delivered entirely as a service, Allure Decoy Documents require no software to download, no agents to install and no hardware to configure. Mean time to value is measured in minutes, with virtually no daily overhead from a personnel resource constraint.

Allure is the only company to hold patents for decoy documents with beacons, making it completely unique in the market. See all patents here: http://www.alluresecurity.com/patents.

HONEY ENVIRONMENTS

- Don't protect growing volumes of documents moving to cloud shares
- Reveal perpetrator tools & methods, but do not pierce them (i.e. Tor & VPNs)
- Require high management and resource overhead
- Interfere with regular IT activities (asset discovery, monitoring, etc.)
- Require a high level of systems and network expertise for implementation and support
- Don't detect if an attacker leaves the fake environment and enters the real one

ALLURE DECOY DOCUMENTS

- Leverage patented technology, unique to the industry
- Deploy as a service, requiring limited resources and overhead
- Detect breach activity at the data source, in operational or cloud environments, without interference
- Generate high efficacy alerts with proprietary, actionable geofence and telemetry insights
- Pierce TOR and VPNs to reveal hacker and leaker identities
- Provide the opportunity to deploy countermeasures before attacks are completed

ALLURE SECURITY

Are you ready to adopt deception as a service?

http://info.alluresecurity.com/demo