

MASQUERADERS: THE ENTERPRISE NEMESIS

DO YOU KNOW WHO'S SNOOPING AROUND YOUR CONFIDENTIAL DATA?


According to the [2017 Verizon Data Breach Investigations Report](#), 75% of reported breaches are perpetrated by outsiders and 81% of breaches leverage stolen credentials. This has driven the concern around insider risk, by which external bad actors gain access by masquerading themselves as legitimate employees or contractors.

Once a masquerader has gained access to legitimate user credentials, preventative tools are easily bypassed. These measures are designed to be used by employees and trusted third-parties, so it's understandable that they'd be blind to an adversary posing as a legitimate user. More layers of authentication will only slow productivity and give employees cause to prioritize business mission over security, leaving data even more susceptible.


It is this very challenge that inspired Columbia professor, and Allure Security founder and CTO, Salvatore (Sal) Stolfo to conduct DARPA-funded research to build a better approach to stopping data loss. As a result, he founded Allure Security and introduced Allure Decoy Documents, deceptive documents with beacons, which act as an alarm system with GPS for confidential data.

A new approach:

DARPA initiated the Active Authentication program several years ago, under which Sal developed the approach that would define Allure Security: active breach defense to detect, respond to and identify attackers. The key driver was to protect the last mile of an attack - the data itself within its native setting (namely, business documents). Sal was determined to provide an effective means of early detection of masqueraders. Like thieves breaking into a home, masqueraders must gather information about the environment they just entered and search for valuables to steal. This early stage activity is key to detecting nefarious activity. Allure Decoy Documents act as tripwires within the folders and directories most likely to be searched as part of an attack, and serve as an effective early detection mechanism. Allure Decoy Documents are strategically placed based on years of research understanding attacker behavior, and catch hackers in the act. The geofence and telemetry insights gained from the opening of the documents then informs response and identification efforts to stop and limit data loss.

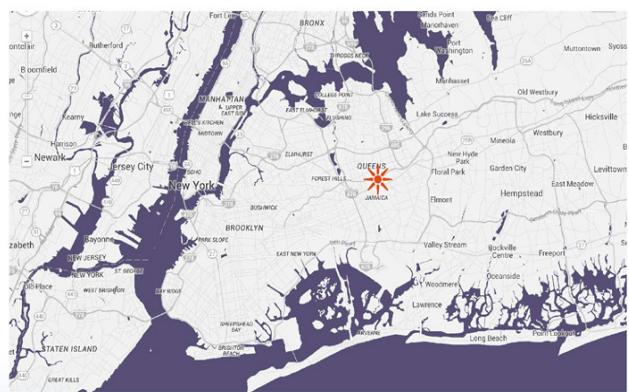

ALERT

ALERT DETAILS


1 Beacon opened remotely

Date	Time	Action Taken	Remote IP Address
10/21/2015	2:01 AM EDT	Email Alert	72.89.243.6

File Path: C:/Users/Todd/Desktop/ Executive_Compensation_2017.doc



BEACON DETAILS

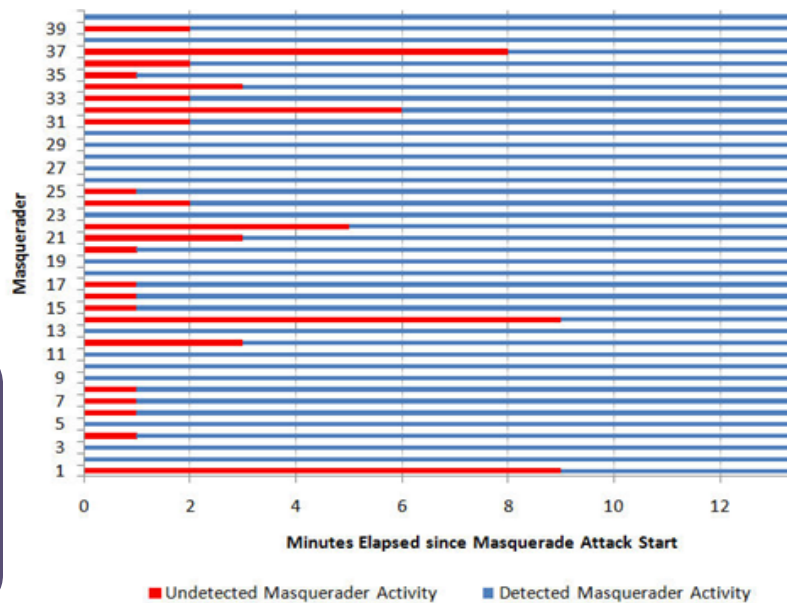
Type	Beacon Name	Deployed On	Created On
.docx	Marketing_Strategy.docx	demo.alluresecurity.com	1/1/2015

DARPA Research Study

The efficacy of Allure Decoy Documents was proven in a scientific study sponsored by DARPA. The study measured true positives, false positives, true negatives and ease of deployment. In the study, 39 individual masqueraders, all selected because of their sophisticated, deep knowledge of computer science and systems in general, were granted access to a system as if they had already succeeded in stealing the necessary credentials.

The masqueraders were then told that their job was to steal sensitive information in the system leveraging the credentials they were provided. The study followed [prescribed and statistically valid methodology](#) whereby the masqueraders were given a scenario of what kind of information to steal, but not how to steal it. They were left to their own devices to find and exfiltrate their quarry. None had sufficient time to succeed in stealing the files they acquired and were prepared to bundle and exfiltrate.

Figure 1. Time to Detection for Each Masquerader



Allure Decoy Documents:

- Detected 98% of masqueraders
- Generated one false positive per week
- Achieved detection within 10 minutes

Allure Decoy Documents Versus Risk

According to the [Ponemon Institute 2018 Cost of Data Breach Study](#), sponsored by IBM, there is a 28% chance a business will suffer a breach within the next two years, resulting a \$3.6 million loss based on the average cost of a data breach. That's pretty good odds. 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. Without Allure, there is 0% chance for early detection given current products deployed, leaving companies subject to the 197 day standard.

If Allure Decoy Documents are 100% effective in early detection under 30 days, an enterprise stands to lose nothing. At 98% accuracy, based on the DARPA sponsored study, that leaves only a 2% variable. The worst case, average savings using Allure Decoy Documents is \$1 million. Allure's approach is proven to catch masqueraders quickly, early in their attacks before succeeding in stealing high-value data and documents.

Want to learn more?

Contact info@alluresecurity.com today.