FEATURE HIGHLIGHT

THREATDEFEND® FEATURE HIGHLIGHT: DECOY DOCUMENTS

Attivo NETWORKS

OVERVIEW

Organizations can configure the Attivo Networks® BOTsink® to place specially crafted decoy documents, that include a geo-tagging component, as an inviting target for an attacker. If these documents are examined or exfiltrated and subsequently opened, whether internally or outside of the network, they will "phone home" to give an indication of where they are being accessed. This functionality extends to copies of the decoys as well, showing if they have been exfiltrated and where they have spread. This functionality is especially useful for organizations that are concerned with unauthorized access to certain types of document and are looking to understand where exfiltrated documents are sent as well as what types of information attackers are targeting.

DECOY DOCUMENTS

Attackers often target documents found on vulnerable systems to either gain more information about the environment they are infiltrating or as one of their end-goals. For an intruder, payroll and personnel information can be as valuable as network topologies or an organization's security architecture. In either case, for the defender, being able to identify what documents attackers are interested in and where stolen documents are being sent can provide an organization with valuable insight into the threat actors working against them. This is where the Attivo Networks decoy documents feature comes into play.

PRACTICAL USE

Decoy documents are usually hosted on the Attivo BOTsink deception servers, meaning that organizations don't need to be concerned about normal everyday users encountering or access these documents. The only way that an organization's decoy documents will ever be touched is if a threat actor has entered into the deception network. A security team has full control over what documents are used as decoys, giving them the ability to, for example, place altered or safely redacted copies or facsimiles of valuable documents where they can serve as bait. Carefully choosing exactly what documents (real or fake) are used gives organizations control on the type of information potentially leaked. For additional counterintelligence, the decoy documents can also be stored on production servers or endpoints where access is controlled, to detect potential theft and reuse of valid production credentials or insider activity.

Decoy documents can be in any of several supported formats (currently Microsoft Word and PowerPoint, Adobe portable document format, or zip archive files), giving the organization options and flexibility to craft the most enticing decoys.

Upon threat actor engagement with a decoy document to examine it, or exfiltrate it, the document's geolocation capability will trigger an alert that the information security team can use to identify which document has been accessed and where the access took place.

AVAILABILITY

The Attivo Decoy Documents capability is available across the entire BOTsink family, including physical, virtual, and cloud instances.

ABOUT ATTIVO NETWORKS®

Attivo Networks is #31 on the Deloitte Fast 500TM and has received over 70 industry awards for its technology and leadership. To find out more about why organizations of all sizes and industries are adopting deception technology, visit www.attivonetworks.com for more information or to schedule a demonstration.