Deception Deployment Strategies : Threat Agnostic vs. Service Agnostic

by Abhishek Singh | Jun 1, 2018 | Blog |

In our previous blogs[1][2], we have shared details of detection of breach campaigns and worms by using Deception. A Distributed Deception Platform (DDP) consists of the breadcrumbs and lures at the endpoint pointing to the honey services in the network. The DDP can be deployed in the network can be done in a variety of ways. In this blog, I will share some of the techniques by which the honey services can be projected in the network.

Threat Agnostic Deployment: In a "Threat Agnostic" approach of deploying breadcrumbs, a network is enumerated to identify the existing services such as SMB, databases in the network. Static Breadcrumbs and Lures are added to the endpoint/web servers pointing to these deception services. In this manner of deploying the honey services in the network, the honey services closely mimic the services in the network. There is a probability that the real services can be accessed by the threat actor, however by increasing the density of the honey services, breadcrumbs & lures, one can ensure that the chances of real services getting accessed by a treat actor in the network remain low.

If there are "m" legitimate services and "n" honey services, then if { [m / (n + m)] <= 0.001}, it will ensure the probability of accessing legitimate services remains less than equal to 0.1 %.

Since threat agnostic approach of projecting deceptions is dependent upon existing

services in the network, it will work well if the primary aim of using deception is to protect the existing services in the network from a threat actor.

Giving an example, in the blog "Deception Centric Architecture to Prevent Breaches involving Web Server," the main aim of the threat actor is to compromise the databases. In such a scenario, it is recommended to deploy the deception services in a threat agnostic manner. This manner will ensure that in the case of a breach, the probability of accessing the honey databases is high leading to the detection of the breach. For further details on detection of the breach, I would encourage the readers to refer to our blog.

Services Agnostic Deployment: In this model of deployment, the deception on the network, breadcrumbs, & lures on the endpoint are spawned or deployed based upon the events from the endpoint or across the endpoints. The events which will lead to the invocation of deceptions for deployment will be referred as trigger events (Also discussed in our previous blog [3]). Some of the conditions which can be used to identify the trigger events are as follows:

* Probability of the occurrence of a trigger event should be more in the malicious files as compared to the clean files. If E denotes the event which is captured during the execution of a file, then it should be ensured { 50% < Probability [E in malicious files] < 100% }.

* The trigger events may fall under the category of Initial Access, Execution, Persistence, Privilege Escalation, Defensive Evasion phases as defined in the MITRE ATT&CK MODEL.

Once these trigger events are reported, specialized decoys that are manufactured based on an understanding of the attacks and breaches need to be deployed.

I will explain the above concept by taking ransomware as an example. Ransomware deletes shadow backup by making a call to "*vssadmin delete shadows /all /quiet*" and drops an executable copy of itself in %APPDATA% folder. The probability of these two events occurring in malicious files is more as compared to the clean files. So if these two events occur, the DDP will raise an alert to project honey mapped drive at the end host and project SMB deceptions on the network. If these honey mapped drive or the SMB deception are touched then alerts will get validated by proprietary algorithms or by an analyst for the possibility of the breach.

Service Agnostic manner of projecting deceptions is in real time and is based upon the trigger events. It provides an inherent advantage that it is independent of the services in the network and is more focused on the threats. So assuming that there is a breach which infects mapped drives and in the environment, and if there are no mapped drives, the DDP will spawn mapped drives and the breach will get detected. Projecting

deceptions in real-time however do require a detailed understanding of the past breaches and attacks. This understanding of the breaches and attacks will aid to identify the trigger events for projecting the appropriate deceptions on the network and on end host.

Conclusion:

Deception is a compelling technology that is capable of preventing breaches and spread of worms. In this blog, we have shared two model of deploying deceptions on the network. Threat agnostic deployment provides the inherent advantage that the since deceptions that are deployed mimic the services of the assets that are being protected, and it is independent of the threats. Service agnostic deployment provides the inherent advantage that since deceptions are spawned independent of the services, it is capable of detecting threats irrespective of the services in the network.

References:

[1] Detection of Breach Campaign using Deception based architecture, https://www.acalvio.com/detection-of-breach-campaigns-by-using-distributed-deception/

[2] Detection of prevalent threats by using Distributed Deception, https://www.acalvio.com/detection-of-prevalent-threats-by-distributed-deception/

[3] Don't be sitting duck, Make your BreadCrumbs & Lures Dynamic.

https://www.acalvio.com/dont-be-a-sitting-duck-make-your-breadcrumbs-lures-dynamic/

TAG Cyber Interview of Acalvio's John Bradshaw

Security Week – Outdated DoD IT Jeopardizes National Security: Report

Archives

July 2018

June 2018

May 2018

April 2018

March 2018

February 2018

January 2018

December 2017

November 2017

October 2017

September 2017

August 2017

July 2017

June 2017

May 2017

April 2017

March 2017

February 2017

January 2017

December 2016

November 2016

October 2016

September 2016

August 2016

July 2016

Categories

Analyst Reports

Blog

Data Sheets

E-Books

Events

In the News

Press Releases

Resources

T-Shirts

Video

Webinars

White Papers

Acalvio provides Advanced Threat Defense (ATD) solutions to detect, engage and respond to malicious activity inside the perimeter. The solutions are anchored on patented innovations in Deception and Data Science. This enables a DevOps approach to ATD, enabling ease of deployment, monitoring and management. Acalvio enriches its threat intelligence by data obtained from internal and partner ecosystems, enabling customers to benefit from defense in depth, reduce false positives, and derive actionable intelligence for remediation.