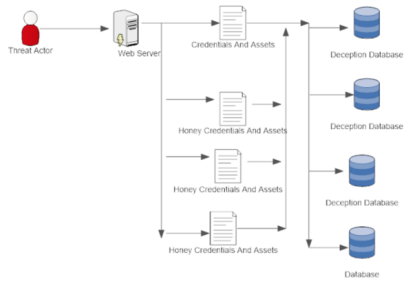
Deception Centric Architecture to prevent Breaches involving WebServer.

by Abhishek Singh | Dec 11, 2017 | Blog |



Web Server is becoming one of the critical vector which have been exploited by a threat actor to breach an organization. Breach at Equifax is one such example, affecting 143 million customers. In this breach, a threat actor could access the internal network and exfiltrate the confidential data by exploiting a vulnerability in a Web Server[1]. The blog first presents one of the flow of steps in a breach which involved web server as an entry vector. The blog then presents the deception based architecture which can be used to detect and divert a threat actor to the deception and engagement platform.

As a part of the first step a web server gets compromised which

Search

Recent Posts

MarketWatch – This 18-Year-Old's Hacking Side Hustle Has Earned Him $100,000 — And It's Legal

BrightTALK – TAG-Cyber's Ed Amoroso Interviews Acalvio

3 Minutes Until the Apocalypse – Technical White Paper

TAG Cyber Interview of Acalvio's John

can be done by exploiting remote code execution vulnerability [2] or a SQL injection vulnerability. The next steps involve involves identifying the high valued assets such as databases, FTP servers in the organization which is connected to the web server.

Figure 1.0 China Chopper WebShell Code

These databases or FTP servers are then accessed either by compromised credentials or by brute force attempts leading to accessing these high-value assets. Figure 1.0 shows the code from china chopper web shell used to connect and perform queries to the SQL server.

Figure 2.0 View for a Threat Actor for a Breach involving Webserver

Deception centric solution as a part of first step involves placing breadcrumbs and honey flows from the web server. These breadcrumbs and honey flows are strategically crafted as per the understanding of the past breaches and the malicious files used by the threat actors. The solution then projects deceptions such as SQL server, FTP server inside the network. In the case of a breach, a threat actor will accesses these breadcrumbs and will gets diverted to the deceptions such as honey databases, honey FTP servers, etc. preventing the real assets storing critical data. The probability of deceptions such as Honey Databases, FTP

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

servers getting legitimately accessed via breadcrumbs at web server is negligible. Hence any access of deception via breadcrumbs on the web server becomes an instant indicator of breach with a probability close to 100%.

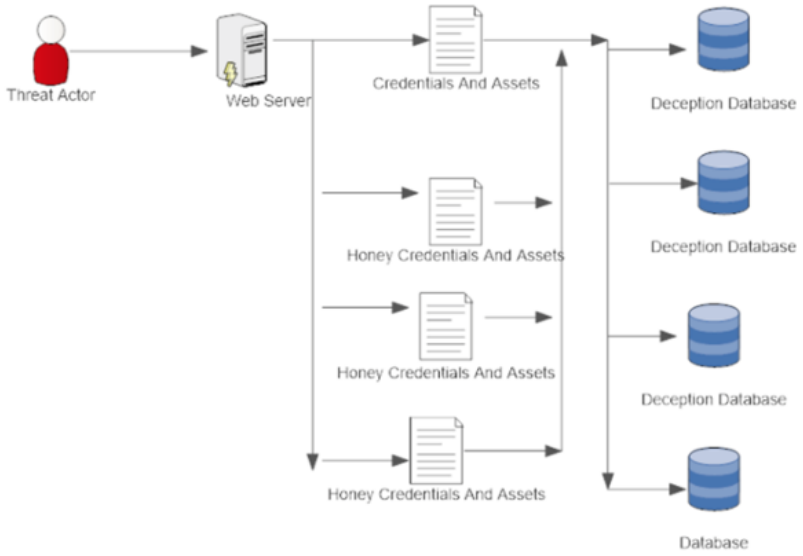


Figure 3.0 View for an Threat Actor having deceptions in case of breach.

Web Servers are one of the critical assets which have actively been used by threat actor for breaching an organization and compromising the critical data. Distributed deception centric architecture provides a definite manner for detecting breaches which involve web server as an initial entry vector. The architecture also ensures that there is no extra computational overhead on the web server making it a recommended or rather a must detection architecture to prevent the breach involving web servers as an entry vector.

References:

[1] Equifax officially has no execuse, https://www.wired.com/story/equifax-breach-no-excuse/

[2] Responding Attack on Apache Struts, https://www.fireeye.com/blog/threat-research/2013/08/responding-attacks-apache-struts2.html

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.