anjuna

WHITEPAPER

Breach Prevention for Financial Industry Customers

“Detailed Exploration of Equifax’s Breach of 2017”

Executive Summary

This document analyzes Equifax's 2017 breach, which exposed the personal information of 147 million people. It illustrates how Universal Confidential Computing with Anjuna Seaglass would have limited the damage had it been available in the breach timeframe. Anjuna's data-in-use isolation, attestation, and platform capabilities would have protected Equifax even after the attacker gained initial access by preventing post-access actions like credential access, lateral movement, and data exfiltration.

Data Reference Table:

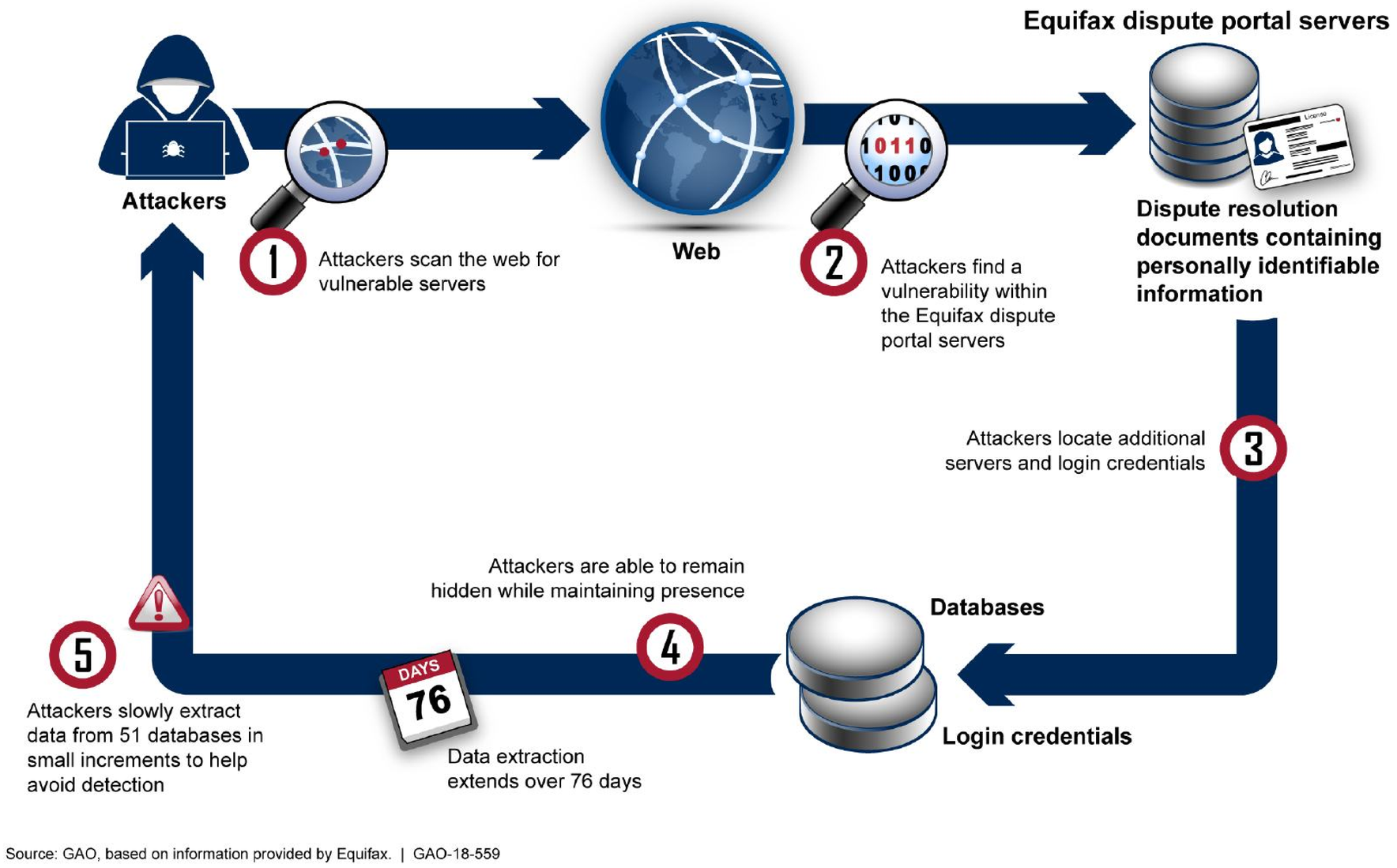
1. Bracy, Jedidiah. "The Equifax Breach, Response, and Fallout." International Association of Privacy Professionals (IAPP), 8 Sept. 2017, iapp.org. This article provides an overview of the breach's discovery, Equifax's response, and the immediate fallout within the cybersecurity and privacy community.
2. InfoTransec. "Analysis of the 2017 Equifax Data Breach." InfoTransec, infotransec.com. This comprehensive analysis focuses on the cybersecurity governance, the specific vulnerability exploited (CVE-2017-5638), and a detailed timeline of events leading up to and following the discovery of the breach.
3. Ontiveros, Victoria. "Equifax Data Breach." Belfer Center for Science and International Affairs, Harvard Kennedy School, 15 June 2021, www.belfercenter.org. This piece reviews the incident and explores the investigative actions taken by governmental bodies, the indictments that followed, and the long-term impacts on Equifax and data protection policy.
4. U.S. House of Representatives, Committee on Oversight and Government Reform. The Equifax Data Breach. 2018, oversight.house.gov. This comprehensive report by the U.S. House of Representatives provides an in-depth investigation into the Equifax data breach, detailing the events that led to the breach, the response from Equifax, and recommendations for preventing similar incidents in the future.
5. Mohaisen, Aziz. Project 2: Systems Security and Malware Analysis. University of Central Florida, 2022, cs.ucf.edu. This document from a university course offers an analytical perspective on systems security and malware analysis, including discussions that could be relevant to understanding vulnerabilities similar to those exploited in the Equifax breach.

Introduction

Cyberattacks are executed through a sequence of scouting and exploitation events, sometimes known as a “kill chain.” Universal Confidential Computing with Anjuna Seaglass may not stop an attack from being initiated, e.g., through a misconfigured and vulnerable legacy application. However, the hardware-assisted controls and isolation with hardware-assisted enclaves break the chain of attack to ensure the attacker cannot access other sensitive data or systems even with root privileges. This document outlines the attack sequence and where the exploitation attempts would be mitigated or limited, using the Equifax case as an example.
This breach has been well documented. Anjuna referenced publicly disclosed analysis in this document.

Whitehouse analysis of the attack and Anjuna's impact:

According to U.S. House of Representatives Committee on Oversight and Government Reform:



Source: GAO, based on information provided by Equifax. | GAO-18-559

Figure 1: from GAO Description of attack analysis

May 13 – July 30, 2017 – On May 13, attackers entered the Equifax network through the Apache Struts vulnerability located within the ACIS environment, an internet-facing business system individuals use to dispute incorrect information found within their credit file (the "initial compromise" step in Figure 2 below). Equifax originally built this system in the 1970s to meet FCRA requirements. It operated on a complex legacy IT system housed within a data center in Alpharetta, Georgia.

After entering the ACIS environment through the Apache Struts vulnerability, the attackers uploaded the first web shells, and malicious scripts uploaded to a compromised server to enable remote control of the machine (the "establish foothold" step in Figure 2). Web shells can enable file system and database manipulation, facilitate system command execution, and provide file upload/download capability. A web shell provides a secret backdoor for an attacker to reenter and interact with a compromised system.

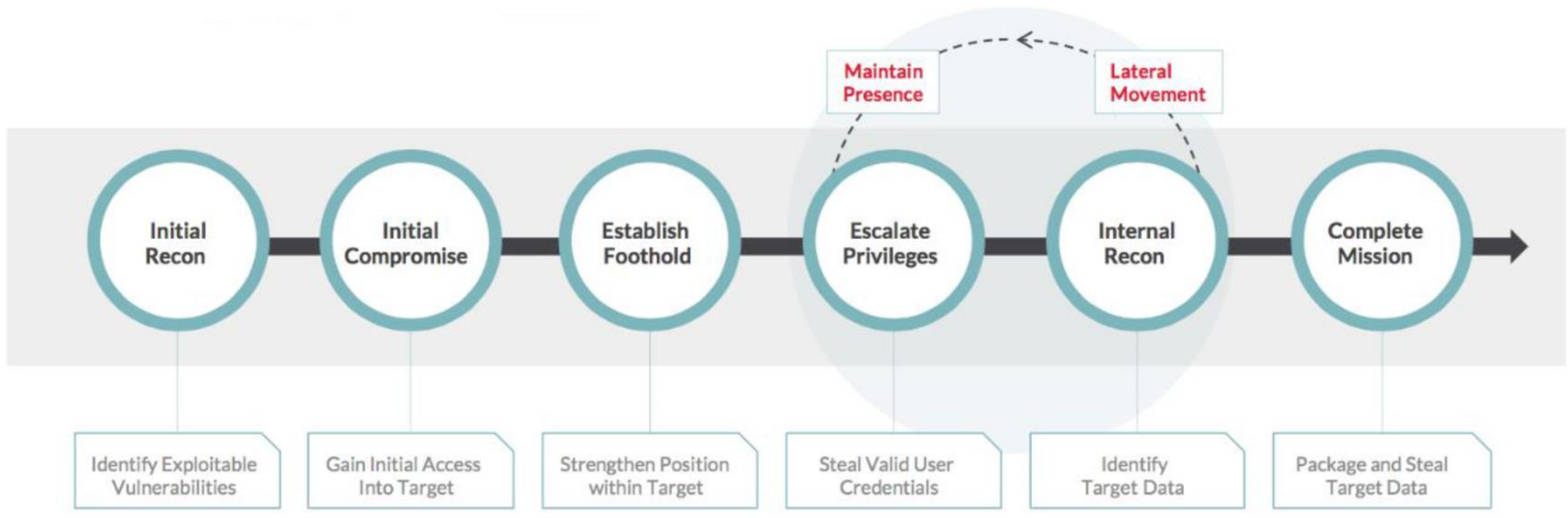


Figure 2: Lifecycle of an Attack

The ACIS environment comprised two web servers and two application servers, with firewalls set up at the perimeter of the web servers. Attackers exploited the Apache Struts vulnerability on the application servers to bypass these firewalls.

The potential impact of Anjuna Seaglass on the initial vulnerability

The point of entry was an unpatched server whose vulnerability allowed code to be injected and run, gaining the attacker's root access to that system. Seaglass does not change how an application works and would not have impacted the initial application vulnerability.

How the scenario would have unfolded after initial attack

From the analysis: Upon penetrating the network, the attackers deployed web shells on various application servers, enabling them to execute commands directly. This assault involved the use of around 30 distinct web shells. Mandiant has indicated that the deployment of these web shells could have been detected through file integrity monitoring, which would alert administrators to unauthorized alterations within the network. During this episode, Equifax's ACIS system was unprotected by file integrity monitoring. pp31-32

Using Anjuna Seaglass for workload isolation:

In the Equifax breach, the first step after finding a vulnerable application flaw to exploit, was then escaping from the application to the OS to get root privileges. With Webshells installed with root privileges the attacker then attacks workloads, data and files on the initially compromised host. Anjuna Seaglass runs isolated workloads in secure enclaves. The CPU hardware prevents unauthorized access to the workloads, so even though the attacker escaped from one workload to the OS, with Anjuna the attacker would not have been able to access other workloads and compromise them or access any of the data or secrets that those other workloads were processing. This would have greatly reduced the ability of the attacker to move any further with their attack. It is likely that the credentials discovered in this step of the attack, if Anjuna Seaglass was in use, would not have been compromised.

First lateral movement to File Server:

***Analysis**: After establishing web shells, the attackers navigated to a mounted file share containing plain-text application credentials within a configuration file database. This breach was facilitated by Equifax's insufficient restrictions on accessing sensitive files across its outdated IT infrastructure, which contradicted Equifax's own security policies. p32*

Using Anjuna Seaglass to prevent lateral movement:

There are two important elements of the attack that happened next. 1st the attacker moved laterally to a file server, and there got access to more credentials that enabled them to access a variety of databases. Discussion of the credential protection will be later in the document.

Focusing on the attackers lateral movement first, the isolation properties that prevent an attacker from getting into a secure enclave on a machine, if an attacker moves to another machine in the network, any workloads on those machines are also isolated and thus protected from attack. Enclave isolation prevents access to the kernel from outside the enclave. By facilitating the isolation, Anjuna Seaglass effectively creates barriers to these secure zones from authorized access. This isolation form provides a preventative measure against potential attackers moving laterally and gaining access to other systems.

Using Credentials from each server to find more servers and credentials:

***Analysis:** Despite the ACIS application's requirement for access to merely three databases to fulfill its business objectives, it was not separated from other unrelated databases. Exploiting this, the attackers accessed 48 distinct databases beyond the ACIS environment, conducting around 9,000 queries and accessing vast amounts of sensitive information. p32*

The attackers also used metadata analysis to identify tables containing personally identifiable information (PII) and extracted data from these tables. Notably, the PII was not encrypted, exacerbating the breach's severity. pp32-33

The attackers stored the PII data output from the 265 successful queries in files. The attackers compressed these files and placed them into a web-accessible directory. Then, the attackers issued commands through the tool Wget – a standard system utility allowing users to issue commands and retrieve content from web servers – to transfer the data files out of the Equifax environment. The attackers used the web shells to exfiltrate some data. The attackers used an estimated 35 different IP addresses to interact with the ACIS environment. p33

Using Anjuna Seaglass to eliminate exposed secrets:

At every step in the process, the attackers searched for exposed secrets to enable them to compromise additional systems. A key feature of Anjuna Seaglass is using the Confidential Computing feature of Attestation. While a workload is starting, Anjuna will ask the hardware to generate a signed report of the workloads measurements. The signed document is verified to be authentic via a attestation service before the workload is allowed to start. Anjuna Seaglass uses attestation to prove the identity of a workload and then inject secrets into the enclave. This solves the secret zero issue plaguing many Enterprise applications. In the Equifax breach, initial secrets such as the file server credentials and database credentials were available to attackers in plain text on the disk. Anjuna Seaglass brings a modern approach to management of secrets by using a methodology for injecting secrets and remotely attested files that can be decrypted via the enclave that has been allowed access. This approach also facilitates a higher level of security awareness and offers better preventative measures for leaking credentials in code and configurations.

Another use of attestation is to prevent the ability of an attacker to persist changes into a workload. As the initial attack vector remains in place, preventing persistence is important, as it would likely slow attackers, but would not stop them.

Attestation of applications in Anjuna Seaglass prevents modification of the sensitive workload. Restarting (easy to do with Openshift) guarantees that nothing has been modified. Attested application mechanisms are shielded against unauthorized modification, effectively encapsulating the workload in a secure and verifiable state. Using technology platforms like Openshift and restarting applications is a straightforward process that allows the rehydration of applications to be verified. By guaranteeing that the application remains unmodified from its last verified state, Anjuna Seaglass plays a critical role in maintaining the sanctity of the application workload and, therefore, fortifying its defense against potential security breaches or integrity compromises.

Impact of Anjuna from an MITRE Perspective:

While the entry point is clear, as it has been well reported that the attackers identified a server with an unpatched version of Apache Struts, the MITRE framework provides an important structure to diagnose not just an exploited vulnerability in an application but the lifecycle of the attack leading to the massive amount of compromised data. We will use the MITRE threat model to examine the compromise and show where Anjuna could have limited the attack's impact at a high level. Further details of the attack for additional reading can be found in this document.

- **Execution (T1059)**: This is when an attacker finds a way to run malicious code on a victim's system. In this scenario, the initial exploitation of the Apache Struts vulnerability would allow attackers to execute code on the vulnerable server. Anjuna's confidential computing environment does not eliminate defects in applications that create opportunities for execution. Anjuna significantly reduces the attack surface that an attacker can exploit. By using Anjuna Seaglass, workloads run on isolated enclaves eliminating both the OS from the attack surface as well as memory attacks on the application itself thwarting many common execution vectors.
- **Lateral Movement (T1021)**: Lateral movement is using one compromised asset to then attack another on the network. Using the extracted credentials, the Equifax attackers moved through the network to gain access to additional systems and search for sensitive information. Workloads in Anjuna Seaglass are running in isolated environments so that even with root access, an attacker cannot access a workload or it’s data while it is in a secure enclave. Eliminating access to the OS and eliminating memory attacks, this isolation would have significantly hindered the attackers' ability to move laterally.
- **Credential Access (T1110)**: Attackers look for credentials, to masquerade as legitimate services and users. At Equifax, the attackers accessed and extracted unencrypted credentials stored in a configuration file. This access was a critical step that enabled the extensive damage that followed. Anjuna's approach to encryption extends beyond data at rest to include data in use. This means that even if attackers were to gain access to a system, the credentials they find would be encrypted and, thus, unusable. By encrypting data-in-use, Anjuna creates a “walled garden” barrier against credential theft, directly addressing the vulnerabilities exploited in the breach. This protects sensitive information and significantly reduces the attackers' ability to exploit compromised systems further.
- **Persistence (T1060)**: Once an attacker identifies a vulnerability, their goal often shifts towards ensuring continuous access to the compromised system. This typically involves embedding malicious code within the system's binaries or scripts, creating a backdoor that remains open even after the system is rebooted. However, Anjuna's security framework introduces a formidable barrier against such persistence strategies. By enforcing strict integrity guarantees measured during launch of a workload, Anjuna ensures that only unaltered, verified software runs within a trusted execution environment (TEE). This safeguards against unauthorized modifications to the image launch and workload.

Conclusion

This comprehensive analysis of the Equifax data breach highlights several critical threats in cybersecurity, calling out the need for organizations to adopt advanced protective technology and heighten security protocols. Zero day attacks will always exist. With Anjuna Seaglass, you can get proactive protection that prevents attackers from accessing an application's memory. The use of attestation allows an integrity guarantee to prevent the application from being modified, or from having to keep credentials and sensitive data on files in the clear. The isolation properties prevent an attacker from being able to spread from the initial attack point to other locations.

This breach was facilitated by multiple systemic vulnerabilities, including insufficient file integrity monitoring, outdated IT infrastructure, a lack of effective encryption, and inadequate network segmentation, and it underscored the importance of a holistic approach to securing sensitive workloads. Anjuna takes a more modern and focused approach to isolation, encryption, and verification to help pave a path to a more secure future by leveraging application-specific attestation (fingerprint) for encrypting sensitive data via policies. Anjuna Seaglass's platform could have significantly migrated the risk highlighted by this breach.

About Anjuna Seaglass

Anjuna Seaglass™ is the world’s first Universal Confidential Computing Platform, capable of running applications in any cloud with complete data security and privacy. Anjuna Seaglass isolates workloads in a hardware-assisted Trusted Execution Environment that intrinsically secures data in every state – in use, at rest, and in transit – to create a zero trust environment.

Get Started

REV-0624

anjuna®

www.anjuna.io