REDSHIELD

Equifax Breach Timeline

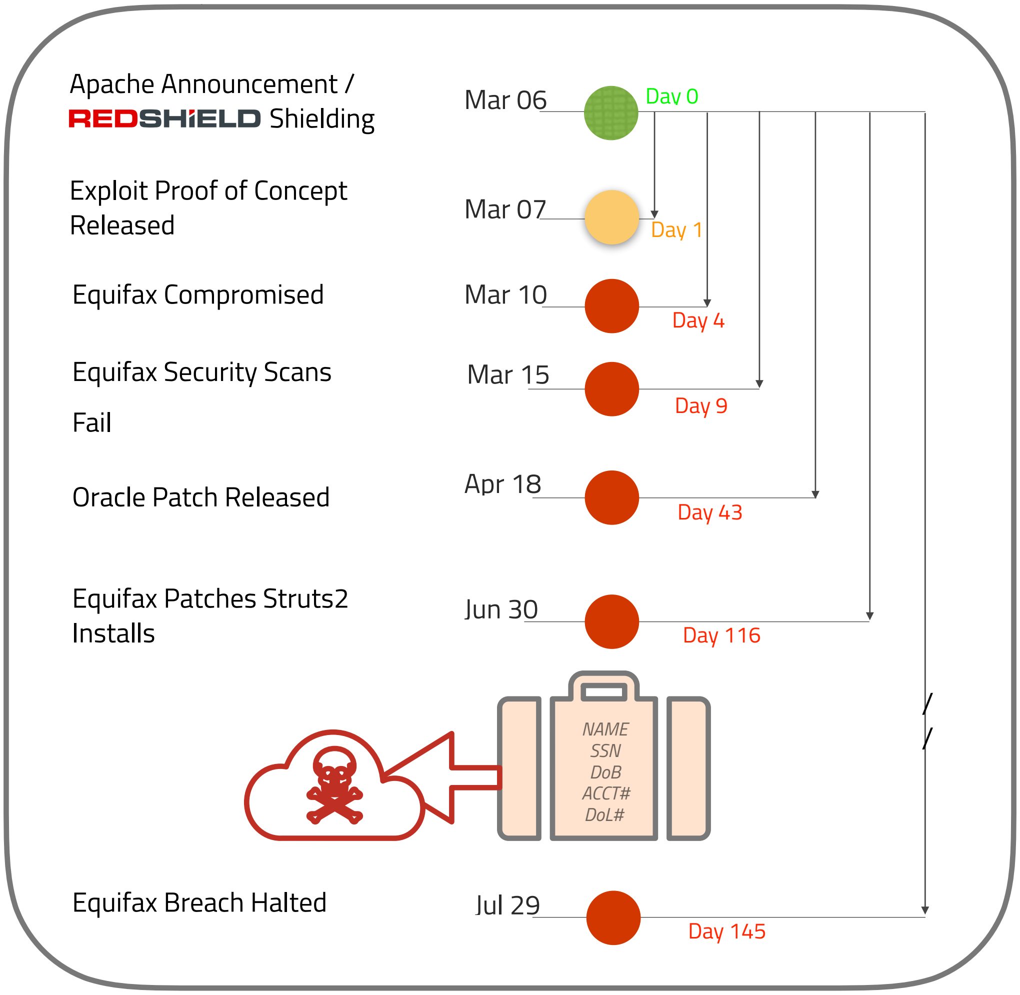
FactSheet

RedShield Security LTD

Mega-Breach discovered July 2017

September 2017 Equifax disclosed a mega-breach of its systems, carried out though exploitation of a web application, which leaked the personal records (Names, Date Of Birth, Credit Card #'s, Social Security #'s, Drivers License #'s, home address, etc…) of over 145M US residents and 400K Brits.

On Mar 6th, Apache announced the Struts2 Bug. On Mar 07th, a proof of concept (PoC) exploit was released to the public. At this point, the Apache Struts2 bug and a working exploit were publicly known. As announced by Equifax, their web application was compromised three days later on March 10th and internal security scans on March 15th failed to identify the existing vulnerable nodes. On April 18th, 43 days after the Apache announcement, Oracle released a software patch to resolve the bug. On June 30th, 73 days after Oracle released the patch, Equifax applied the Struts2 patch. According to the Equifax announcement, the attack wasn't halted for another 29 days leaving Equifax under attack for a total of 141 days resulting in one of the largest breaches of private citizen information in US history.



Breach Timeline

Application Security is a People Problem

...and patching as a strategy, always loses

Web application security and more generally, vulnerability management programs, are comprised of 10% shielding tools, 20% assurance tools and 70% people and process. With a global shortage of IT security professionals, organizations face a task-prioritization battle pitting ***risk vs. resource***. In the case of the Equifax breach the former CEO has testified to the US Congress the breach was caused by the error of a lone employee for not applying a security patch. In this case, the vendor patch was not available until 39 days after the breach! Patching will always be slower than the attackers. So patching as a strategy always loses.

What works?

Secure your hosting environment and application components first, find any issues in application delivery stack, fix what you find and then stay ahead. Sounds simple enough. Under the covers is where it gets more challenging; looking at the more mundane tasks such as regular vulnerability scanning, continually monitoring vulnerability advisories, monitoring systems, tuning defenses, reviewing logs and reporting. The tools are a commodity but this brings us back to the people problem; **only by combining industry leading tools deployed and managed by expert security practitioners, adhering to mature security processes is a successful program possible**. This is surely not the work for a lone employee.

RedShield Customer Experience

RedShield customers enjoy secure software and code remediation delivered as a white glove cloud offering through a combination of tools, application shielding and expert security services 24/7/365.

Findings

- *Having a bug bounty would not have helped as they knew about the bug, only Shielding the vulnerability prior to the vendor patch release would have provided protection*
- *This cannot be attributed to the failings of an individual; no matter what the architecture; immediate and around the clock security can only be delivered by a seasoned team of experts*

In the first 24 hours upon announcement of the Apache Struts2 bug, RedShield analysts under normal process immediately:

- Began working on understanding the exploit
- Determine which customers may be vulnerable
- Perform assurance testing determined whether customers are protected by our existing shields
- If not, develop a shield, deploy and verify effectiveness of controls
- Contact customers and post an announcement under our programmatic Vulnerability Advisory Service

In the case of this Struts2 vulnerability, **RedShield customers were protected by default**. Our analysts concluded our base (4700+ rule) security hygiene policy already provided adequate shielding and an informational vulnerability advisory was published on Mar 7th (Day 1) and distributed to our customers.

Visit us at https://RedShield.co or contact sales@RedShield.co to request a **Free Trial**