

Case Study: Equifax Breach



Case Study: Equifax Breach

- ◆ Equifax History and Growth
- ◆ Incident Details
- ◆ Incident Response Process
- ◆ Lessons Learned



Equifax History and Growth



- ◆ Equifax is an Atlanta based Consumer Reporting Agency (CRA) founded in 1899
- ◆ CRAs collect information about individuals and companies, and sell credit scores and detailed reports to other companies and governments (including the US government)
- ◆ Consumers and companies cannot opt-out

Equifax History





- In 2005 former CEO Richard Smith started **new growth campaign focused on acquiring smaller companies** for their systems and data
- By 2017 CEO boasts about Equifax **data and processing capabilities**
- Aggressive growth also **yielded large amounts of technical debt and security programs were not scaled** to match the growth of systems and data

Equifax Growth

Georgia Tech

Equifax Incident Details

Georgia Tech

February 14, 2017
The Apache Software Foundation received the first report of a vulnerability

March 8, 2017
The Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) sent Equifax vulnerability notice

March 9, 2017
Equifax Security performed an open source component scan to identify any systems with a vulnerable version of Apache Struts – **No results**

The Apache Struts Project Management Committee (PMC) publicly disclosed the Apache Struts vulnerability

- National Vulnerability Database: CVE-2017-5638

March 7, 2017

Equifax disseminated the US-CERT notification via the GTVM listserv process
March 9, 2017

March 10, 2017
First evidence of the Apache Struts vulnerability being exploited at Equifax

- Attackers ran the "whoami" command
- No evidence of relation to May 13th breach

Equifax's Emerging Threats team released a Snort IDS signature rule to attempt to detect Apache exploit
March 14, 2017

March 15, 2017
Equifax received a new signature rule to detect vulnerable versions of Apache Struts from McAfee

- McAfee Vulnerability Manager tool used to scan externally facing systems with new signature twice – no results

The Apache Struts vulnerability was discussed at a monthly meeting hosted by the GTVM team

- Information disseminated to 430 people at Equifax

March 16, 2017

Incident Details: Lead-Up

Georgia Tech

Incident Details: Lead-Up

Georgia Tech

Data Breach: May 13 – July 30, 2017

- Attackers compromise ACIS system leveraging Apache Struts vulnerability and gain access to Equifax network
- Attackers deploy web shell malware on ACIS application servers allowing remote session
- Attackers accessed file share mounted on ACIS application servers and identified unencrypted application credentials stored in configuration file
- Attackers were able to access 48 databases from the ACIS application servers and leverage stolen application credentials to access databases



Georgia Tech

Data Breach: May 13 – July 30, 2017

- Attackers queried databases to learn schemas and identify sensitive personally identifiable information (PII)
- Attackers ran queries to extract the PII of 148 million consumers
- Data returned by queries stored in compressed files and placed in web accessible directories on ACIS servers
- Standard web command then issued from attacker infrastructure to retrieve data files



Georgia Tech

Equifax Incident Response Process

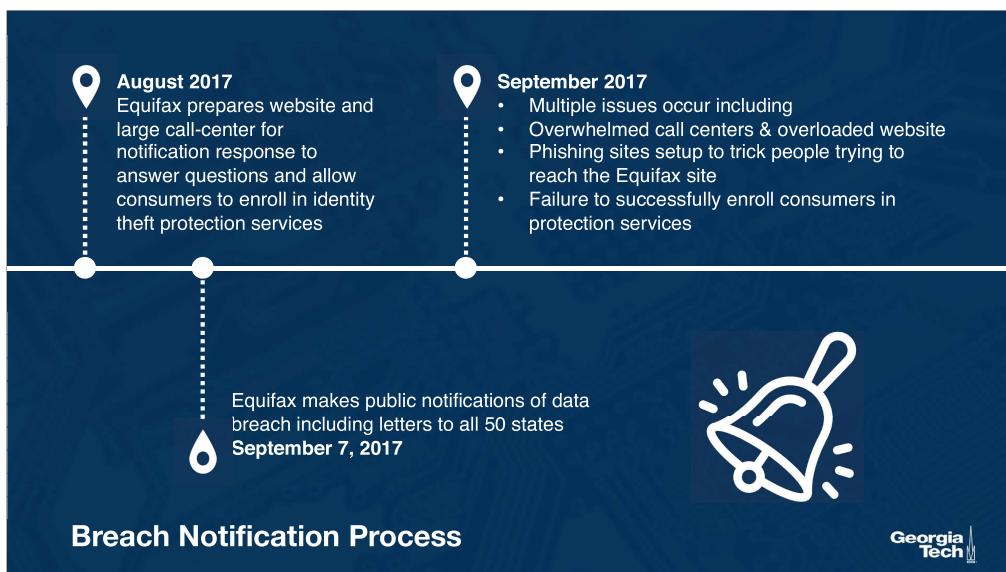
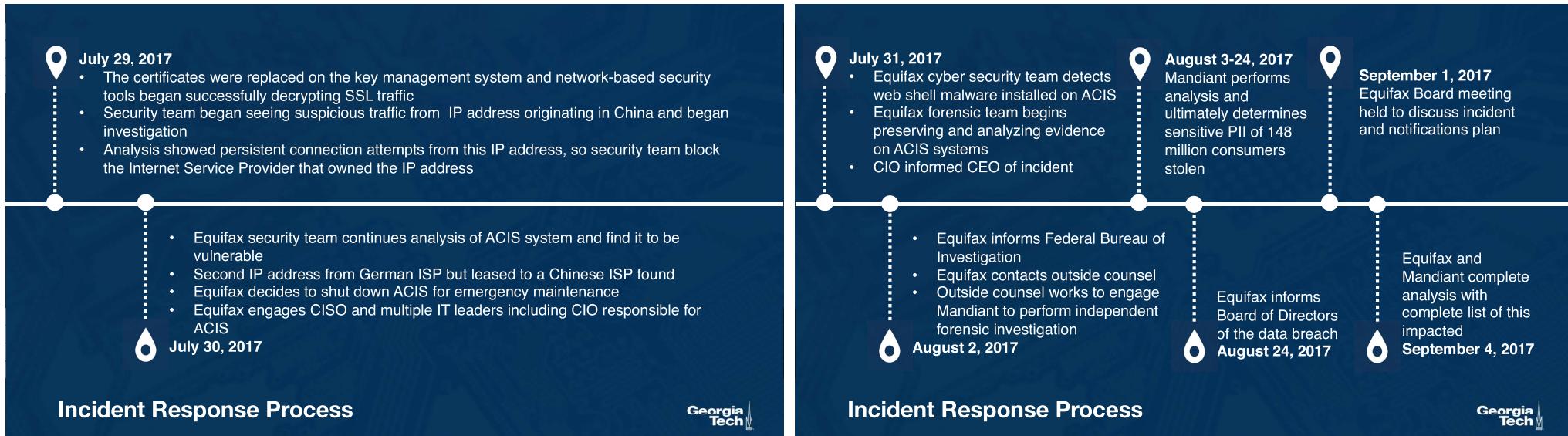
Georgia Tech

Note:

Prior to this incident SSL traffic was not successfully being decrypted by security tools as the the SSL key management system was operating with expired certificates for some time.



Georgia Tech



The following items were noted as **areas of improvement** from the report:



- ◆ Vulnerability management
- ◆ Patch management
- ◆ Certificate management
- ◆ Network segmentation
- ◆ File integrity monitoring
- ◆ Data minimization
- ◆ Technical debt