Ray Morris

08 December 2019

Equifax Breach Teaches How to Eliminate Identity Theft

Background

In 2017, credit reporting company Equifax announced one of the most severe data breaches in history. Over 145 million Americans were affected, with more victims in the UK (Equifax, *Equifax Announces Cybersecurity*). The census bureau reports there are 240 million adults in the US, most US adults were affected in the Equifax breach. Names, social security numbers, birthdates, and some credit card numbers were breached (Equifax, *Equifax Releases Details*). Widespread discussion of cybersecurity policy including Congressional hearings and proposals for new laws followed.

This breach involved failures at several levels, defense-in-depth in reverse. Perhaps the most commonly mentioned failure was a vulnerability in the web framework used, Apache Struts. The CVE was known and protective actions were available by March 8 (Lenart). Equifax stated the breach occurred from May 13 to July 30 - months after Equifax could have applied the security patches. Equifax states that their security team was aware of the vulnerability in March. This breach would not have occurred if Equifax had applied these security patches promptly.

Krebs reports that the stolen credit card data was for transactions doing back to at least December 2016. Equifax was storing credit card data for historical transactions in a way that was accessible to the attackers, which would violate PCI requirements (Krebs).

The company stated they detected unusual activity on July 29 - after the attackers were downloading data for ten weeks. Proper monitoring and detection was not practiced. Further, disclosure was not made for five weeks after, leaving a long gap during which consumers and others were not warned to take protective actions.

Diamond Model Analysis

Little is known about the adversary, though certain characteristics can be inferred from their capabilities. The capabilities imply certain infrastructure. Victims include Equifax itself and the consumers.

Victim

Victim analysis can be broken down into victim personas, victim assets, and victim susceptibilities (Caltagirone et al. 16). Equifax, one of three major credit reporting agencies, is in the business of storing data which assists banks and others in deciding whether to extend credit to people and businesses, and at what interest rate. This data includes which credit accounts people and business have had, whether any payments are late, and the recent balance owed. Equifax has a complex IT network. The victim databases contain data on millions of Americans, both individuals and businesses (Equifax, Equifax Announces Cybersecurity). The data is a tuple used by banks and others to identify and authenticate an individual - name, social security number, and date of birth (Committee on Financial Services). These items are the primary data points used to commit identity fraud, according to House testimony. The social security number is considered as secret yet shared with many organizations - employers, banks, credit card companies, etc. This understanding of the victim asset can be leveraged when considering which types of policies may be helpful.

Victim susceptibilities include the technical vulnerability in the Struts web framework, CVE-2017-5638, which allows attackers to execute arbitrary commands due to improper exception and error handling (Lenart). The victim web site was the online dispute portal for Equifax. The victim system did not include controlled patch management, as evidenced by the fact that this vulnerability continued in the Equifax environment despite the fact that patches had been released on March 18 (Lenart). According to Equifax testimony before the US House, this was because the victim organization had not assigned patch management to a defined team and the organization had no process to verify patches had been completed. Equifax lacked accounting of which software they had

deployed in their environment, leading to difficulties in ensuring the software was properly patched (Luszcz).

Capability of the adversary

The attacker had the capability to scan the internet for vulnerable systems. Equifax executives testified to the US House that commercial vulnerability scanners at the time did not reliably detect vulnerable systems. According to the Senate subcommittee report, competing CRA Experian stated that after one commercial scanner did not detect it reliably, they followed up with another commercial scanner which *did* find the vulnerable systems. The attackers may have had greater detection capabilities than Equifax by using a more effective scanner.

The adversary had the capability to understand how to make practical use of the vulnerability, executing the desired commands. They also had the capability to effectively use the operating systems, databases, and other systems in place.

The attackers also had the capability to scan within the Equifax internal network for sensitive data on open file shares without being detected (Permanent Subcommittee on Investigations 46). According to the Senate subcommittee report, Equifax admins left shared database passwords unencrypted on open shares. The attackers had the capability to locate these, then extract sensitive data from the victim databases. In this author's recent experience, performing this type of scanning for passwords on accessible shares is a time-consuming process with many false positives. Attackers may have had the capability to spend many hours filtering through false positives and determining which data can be accessed. Standard detection tools such as Netwrix and Darktrace would have alerted on such scanning, in the experience of this author.

Some analysts have commented on the attacker's capability to exfiltrate the data without detection. It should be noted that the exfiltration was detected as soon as expired certificate was renewed in the detection system (Government Accountability Office 14). Thus, the attacker only had

the capability to avoid detection while the detection systems were broken due to the expired certificate.

Infrastructure

The primary information available about the infrastructure used is that the data was being exfiltrated to an IP address in China (Permanent Subcommittee on Investigations 3). The attackers were using the general internet infrastructure and unknown infrastructure in China. No special hardware or other infrastructure requirements are noted as being required to exploit the weaknesses used by the attackers.

Adversary

The adversary was sending data to China, so they were either in China or operating from elsewhere through a proxy in China, going in and out through the Great Firewall. Western investigators never reported finding large portions of the data offered for sale on the dark web. Therefore, some have speculated that the government of China sponsored the breach to use the information for espionage. However, other explanations are the adversary:

- chose not to sell it after realizing it was top-priority case for government investigation
- sold a small portion for a few million dollars and that was enough
- sold some or all privately and quietly, not on the dark web publicly
- sold it within Asia, where westerners didn't see it

There are many possibilities other than the Chinese espionage theory. Following the trail of the attackers into China, starting with the Chinese IP address, is difficult.

Social-Political

Considering the adversary-victim relationship, Equifax holds a product which is of use to cybercriminals. Names, birthdates, and social security numbers were stolen because these data

items enable identity fraud. Credit history was not taken. This may inform analysis of the likelihood that the purpose was espionage (EPIC). The attackers took only data required to commit identity fraud. If there were strong evidence that the attack was sponsored by the government of China, much could be said about the relationship between China and the US victims. There is no persuasive evidence.

Equifax provides an attractive target to cybercriminals due to holding a huge volume of this data. The attacker persisted for months to exfiltrate 143 million records. Understanding the product, or useful data, provided by the victim is important because reducing or eliminating the value of the product will a) reduce the frequency of attacks and b) reduce the damage when attacks do occur.

Technology

Standard technologies used by most web sites were used. TLS encryption of the connection, intended to increase security, instead facilitated the breach by preventing the IDS from immediately detecting it (Government Accountability Office 14). Poor https certificate management caused immense harm to the confidentiality of information, by eliminating the availability of the IDS in this scope.

Governance Layers and Policy

Organizational

The Senate and House reports, referenced above, mention several improvements that could be made at the organizational level. Competing CRAs had better patch management, facilitated by an inventory of installed software. While Equifax had a policy that systems should be patched properly, their implementation systems did not ensure that policy was followed. While organizations should follow best practices, ensuring that best practices are always followed is an impossible task. Historically, best practices recommendations have primarily been at the level of individual computing systems, networks and organizations. That has been thoroughly covered by others without preventing

attacks; this paper will not focus on solutions at the organizational level. The Equifax security team realized the intrusion when they saw traffic going to China; they don't do business with China. Some organizations which don't do business with China or Russia block the IP ranges of these countries, becoming invisible to scans for coming from these nations.

Industry

At the industry level, PCI and other organizations issue requirements and guidelines regarding cybersecurity. While these are undoubtedly helpful and reduce the number of smaller attacks, they did not prevent the multiple breaches at Equifax. This is another area that has been well-covered elsewhere and so will not be our present focus. Rather, the industry level will be revisited in combination with the national level as a policy proposal is presented.

National

The Senate report recommended a requirement for prompt notification of breaches and a national cybersecurity information sharing system. Because the company made no effort to comply with existing notification laws in the 50 states, it's not clear that a national notification law would have been any more effective. Similarly, information-sharing systems already exist, both public and private. Arguably, vendor-based aggregation such as Cisco Talos may be more effective than the federal systems. In any event, the information was shared with Equifax - they were informed of the vulnerability, and of the need for protections such as patch management, IDS, etc. It may be more effective for the federal government to work with industry on a simpler solution to identity theft, discussed below.

Transnational

It is unknown whether the Chinese government actually sponsored the breach or turned a blind eye. One might expect that if the IP address involved had been traced to an allied country such as the UK or Australia, such a government would provide more assistance with the investigation. It is

probably not possible to compel China to investigate and then provide forthright answers. While the United States can communicate to China that cyber attacks are further damaging the relationship, effective transnational solutions in this regard are not possible at this time. Improved relations with China may involve cultural and other interchange over many years. This involves many issues outside the scope of cybersecurity, and cannot reliably be accomplished, particularly in a reasonable period of time.

A Proposal

The reason Equifax and many other organizations have been attractive targets is because they hold the social security number and birth date of many people. Knowledge of these two items is used as both identity and authentication when applying for bank accounts, credit, other valuable resources (Committee on Financial Services). This usage gives the information its black-market value. The social security number, in particular, is used for authentication, much like a password - a password that is handed out to many organizations, never changed, re-used everywhere, and routinely stored in plaintext. In short, it is not a secret, yet it is routinely used for authentication, as a password would be. It’s not a password if you give it out to many parties. This simple truth is the fundamental cause of identity theft and identity fraud. Social security numbers of most Americans have been breached, yet SSN is treated as authentication.

Identity theft would be solved in large part if authentication were by a secure method. Breaches involving SSNs would do far less damage. Lohstroh points out that in many cases what is actually needed is not identity or authentication per se, but an assertion, or signed claim. When applying for a car loan or mortgage, the potential underwriter wishes to be assured that the applicant has at least a certain amount of money in their bank account. The bank could send a signed assertion that “the holder of this token has at least $X on deposit”. The applicant would generate this assertion using their bank credentials and 2FA so authenticators are not shared. The SAML protocol is a well-

known and widely supported protocol which can provide these kinds of trusted assertions. Lohstroh proposes a protocol similar to SAML, designed to address the issues around identity theft.

Major banks may implement their own signing and be trusted in their own right. For smaller banks or other organizations networks may be established similar to (and perhaps sponsored by) existing inter-bank networks such as Visa, Plus, and Pulse. Requesters may choose to trust major employers to sign employment and income verifications; smaller employers may have such data signed by ADT or another well-known payroll provider.

The industry can establish the SAML-like protocol for securely exchanging information during a credit application. Signed assertions would replace using social security number as the authenticator. A credit application would involve relaying data only accessible to the legitimate account holder, using the credentials for each data provider. Security standards around this protocol could be drafted and enforced by the industry similar to PCI enforcement.

National or state policy could be that consumers are not presumed responsible for payment on accounts opened without effective authentication. The fact that an applicant knows someone's social security number does not prove who opened the account and so does not make the consumer liable for the debt. Unlike policies which mandate that businesses act against their own interests, this policy would make use of the company's desire for profit. The desire to be able to collect would be incentive to have effective authentication for new accounts, thereby greatly reducing identity theft.

Much discussion of policy proposals in this area overlooks the simple fact that identity theft is possible only because a person's SSN, which many companies have, is used to authenticate an application, as if it were a secret password. What is needed is effective, modern authentication for new accounts.

Works Cited

Altmayer, Olivia A. "THE TIPPING POINT – REEVALUATING THE ASNEF-EQUIFAX SEPARATION OF COMPETITION OF DATA PRIVACY LAW IN THE WAKE OF THE 2017 EQUIFAX DATA BREACH." Northwestern Journal of International Law & Business, vol. 39, no. 1, 2018, pp. 37-58. ProQuest, http://prx.library.gatech.edu/login?url=https://search-proquest-com.eu1.proxy.openathens.net/docview/2185008263?accountid=11107.

Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. *The diamond model of intrusion analysis*. Center For Cyber Intelligence Analysis and Threat Research Hanover Md, 2013.

EPIC Electronic Privacy Information Center.*Equifax Data Breach*. https://epic.org/privacy/data-breach/equifax/.

Equifax. *Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation Of Cybersecurity Incident*. https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821.

Equifax. *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes* https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

Krebs, Brian. “Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop.” K*rebs on Security*, https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/.

Lenart, Lukasz. *S2-045 - Apache Struts 2 Wiki*. Apache Software Foundation, 19 Mar. 2017, https://cwiki.apache.org/confluence/display/WW/S2-045.

Lohstrohm Marten. *Why the Equifax Breach Should Not Have Mattered*, 2017.

Luszcz, Jeff. “Apache Struts 2: How Technical and Development Gaps Caused the Equifax Breach.” *Network Security*, vol. 2018, no. 1, 2018, pp. 5–8., doi:10.1016/s1353-4858(18)30005-9.

Tantleff, Aaron K. "Equifax Breach Affects 143M: If GDPR were in Effect, what would be the Impact?" Journal of Health Care Compliance, vol. 19, no. 5, 2017, pp. 45-46. ProQuest,

http://prx.library.gatech.edu/login?url=https://search-proquest-com.prx.library.gatech.edu/docview/1963073683?accountid=11107.

United States, Census Bureau. *U.S. Census Bureau QuickFacts*. https://www.census.gov/quickfacts/fact/table/US/AGE295218.

United States, Congress, House, Committee on Financial Services. *Examining the Equifax Data Breach*. United States Government Publishing Office, 5 October 2017.

United States, Congress, Senate, Permanent Subcommittee on Investigations. *How Equifax Neglected Cybersecruity and Suffered a Devastating Data Breach*. Staff report.

United States, Government Accountability Office. “Data Protection Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach, August 2018.