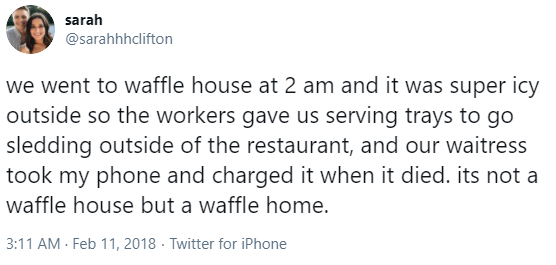
Chad Ballay

CYBR450-342

11/22/2020

Week 1 – Recent Breaches

*As an arbitrary reason I’m choosing Huddle House because Waffle House is the superior late night study location. This iconic tweet actually is from the nearby Waffle House and demonstrates the better experience. That and there are just so many breeches that I had to have some deciding factor.*



[*https://twitter.com/sarahhhclifton/status/962615171922448384*](https://twitter.com/sarahhhclifton/status/962615171922448384)

On February 1st 2019, Huddle House posted a security alert on the main page of their website disclosing a security breach affecting their POS terminals. The press release disclosed that this breach wasn’t detected internally and instead had been identified by the credit card processor and in accordance with PCI rules they were required to engage a Payment Card Industry Certified Forensic Investigator. (*Huddle House System Security Compromise*)

I lead with that first detail to point out that the Data Protection Notice that eventually did come out is frustratingly vague on details but is at least going to be reliable on what information it does convey. (*Any Meal. Any Time. Breakfast, Lunch, Dinner.*)[/](https://www.huddlehouse.com/data-protection-notification/)

**WHO:** Anyone who used debit/credit cards at the 341 locations between September 15, 2017 and March 1, 2019.

**WHAT:**  Malware deployed to the affected POS systems captured information from the magstripe reader. Some of this data is account number, expiration date, CVV code and service code.

**HOW:** One of the many POS vendors they contract with had been breached and in turn this allowed the criminals to deploy malware to the POS systems specific to that vendor.

This is about the limit of facts that were consistently related about this breech. The rest is educated guesswork.

1. More indemnification required on the vendors. Now would be the time to require the undisclosed vendor to up the indemnification coverage they maintain since Huddle House probably now realizes how expensive cleaning up a breach is. I don’t often advocate of letting no good crisis go to waste but this is a good time to prepare for the next crisis.
2. Tighter penalties for contractual failures. This goes along with #1 but more as a motivator for the vendor to have leverage to change their own internal process.
3. Without know the details I don’t know specific technical remedies. But my assumption would be that the vendor lost control of their codebase. Unreviewed/approved code changes made it into their code base. Audit and addressing of deficiencies.
4. Another attack surface would be their build process. It’s less likely due to the build process being more difficult to manipulate. Audit and address any decencies.
5. A very extreme attack surface would be the deploy/maintain procedures that the vendor had in place. Since Huddle House says all locations were affected, I don’t see that as likely but it is something to at least audit to be sure.
6. The duration of this breech gives me pause. Either this malware was amazingly hidden or the Huddle House and this vendor’s internal audit process missed multiple opportunities to have found the malware. I’ve become a strong adherent to taking the blameless postmortem approach of focusing on the how something failed and then fixing the why it failed so it can’t happen again.
7. During these investigations the hard work of building a disclosure and concerns feedback mechanism needs to be done. In any complex codebase there are multiple points of failure. The involved workforce is going to by virtue of this one breach be suddenly more aware of other more troubling aspects of the codebase. Directing this into a pipeline that creates actionable tasks will help prevent the net data breach.
8. Finally, the message needs to be clear. Data breeches will occur again. How the company and the Indvidual's of the company respond is what dictates the impact. Equifax survived disclosing PII data for ~half the country. Their stock price and market share is higher than it was previously. Getting the workplace culture to shift the goals from perfect but static defense to dynamically active defense will also help with future security aspects.

**Sources**

Any Meal. Any Time. Breakfast, Lunch, Dinner. (n.d.). Retrieved November 23, 2020, from <https://www.huddlehouse.com/data-protection-notification/>

Huddle House. (2019, February 01). Huddle House System Security Compromise. Retrieved November 23, 2020, from <https://www.prnewswire.com/news-releases/huddle-house-system-security-compromise-300788262.html>