Hacked: Heartland Payment Systems

NATHAN MIXON

PRINCIPLES OF CYBERSECURITY

10/13/2021

Heartland Breach of Trust

- In 2008, Heartland Payment Systems was breached and at the time was the sixth largest payment processor in the U.S (McGlasson, 2009).
- The credit and debit card information of millions of people were stolen.

Hartland Payment Systems Mastermind

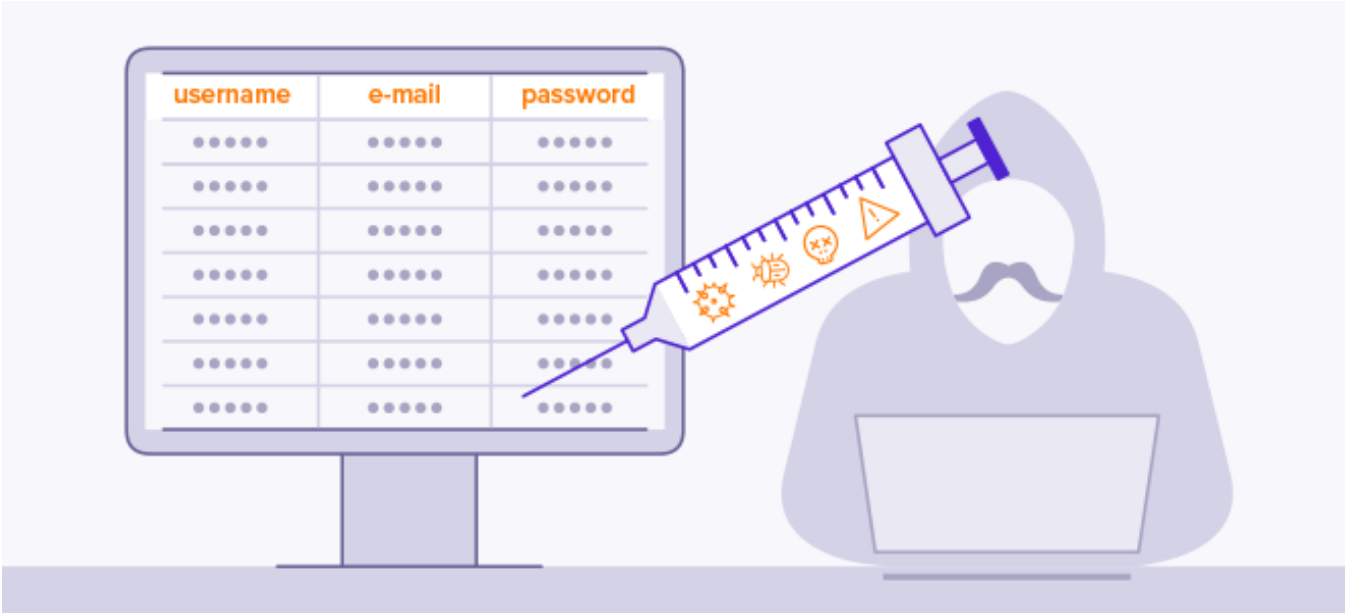
- Albert Gonzalez was at the time a 28-year-old Cuban born criminal hacker.
- He resided in South Florida near Miami-Dade for most of his life.
- Gonzalez worked on both sides of Cyber Crime by both catching criminals and participating in the crime himself (Suddath, 2009).

Gonzalez's Past

- Gonzalez was arrested in 2003 while working as an administrator for shadowcrew.com.
- After his arrest he became an informant for the secret service under Operation Firewall (Verini, 2010).

How it happened

- Heartland was notified by Visa and Mastercard after suspicious transactions and thus hired specialist to investigate.
- Gonzalez and his Russian adversaries used SQL injection to modify code on a web script (Gordover, 2015).
- Through this the hackers were able to duplicate credit and debit cards to then make large withdrawals from atm machines.



Heartland Responds

- After the breach, Heartland upgraded its security measures to end-to-end encryption. Heartland's CEO Robert Carr called it, "the highest level of beta security in the marketplace" (McGlasson, 2009).
- Heartland also upgraded its networks and servers to earn its PCI DSS compliance back.

Heartland's Big Mistake

- "Data, including card transactions sent over Heartland's internal processing platform, is sent unencrypted, he explains, "'As the transaction is being processed, it has to be in unencrypted form to get the authorization request out'" (McGlasson, 2009).

Overall Outcome

Albert Gonzalez was sentenced to 20 years to in jail.

Heartland lost its PCI DSS compliance for 4 months.

Heartland lost more than $200 million dollars (Gordover, 2015).

References

- Gordover, M. (2015, March 19). *Lessons learned from the 2008 heartland breach*. Proofpoint. Retrieved October 12, 2021, from https://www.proofpoint.com/us/blog/insider-threat-management/throwback-thursday-lessons-learned-2008-heartland-breach.
- McGlasson, L. (2008, January 21). *Heartland Payment Systems, Forcht Bank Discover Data Breaches*. Bank Information Security. Retrieved October 10, 2021, from https://www.bankinfosecurity.com/heartland-payment-systems-forcht-bank-discover-data-breaches-a-1168.
- McGlasson, L. (2009, October 8). *Heartland breach: Inside look at the plaintiffs' case*. Bank Information Security. Retrieved October 12, 2021, from https://www.bankinfosecurity.com/heartland-breach-inside-look-at-plaintiffs-case-a-1844.
- Suddath, C. (2009, August 19). *Master Hacker Albert Gonzalez*. Time. Retrieved October 12, 2021, from http://content.time.com/time/business/article/0,8599,1917345,00.html.
- Verini, J. (2010, November 10). *The Great Cyberheist*. The New York Times. Retrieved October 11, 2021, from https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html.