2014 Cyber Attack on eBay

Search

Idris Noori, Manusha Patabendi, Ali Malik

Target

145 MILLION ACCOUNTS COMPROMISED

- **What was compromised:**
  usernames, encrypted passwords, phone numbers, physical addresses and date of birth

- **What was not stolen:**
  financial info (stored separately and encrypted)

Why Ebay?

- Ebay has been described as the “golden goose”
  - large user base
- Other great targets
  - Amazon - 244m active accounts, each with credit cards attached.

    Apple’s iTunes - 800 million users, most have credit cards attached to their accounts.

Information not encrypted

- Not Encrypted
  - Customer name
  - Encrypted password
  - Email address
  - Physical address
  - Phone number
  - Date of birth
- Not only not encrypted — but stored in plain text
- It's shocking that eBay would choose not to encrypt that kind of sensitive information

Protection of information

- If billion-dollar companies want us to give up our personal information, shouldn't we make sure they are going to protect it?
- Credit cards and banks
  - Offer protection against fraud.
  - That same type of protection isn't available for identity theft
- Industry standards
  - Around how payment information can be stored and secured.
  - Time to treat personal information with similar reverence

Threat on other accounts

- Encryption
  - Allows eBay to see your actual password.
- Password hashing
  - Allows eBay to check if the password you enter is correct or not, but doesn't allow eBay to get the plaintext of your actual password
- EBay was using encryption, which is the more easily broken
- Many consumers use the same password on multiple sites
- The attackers will quickly take over accounts across the web wherever a user reused their username and password on another site

Agent

- Group known as "Syrian Electronic Army" (SEA) claimed responsibility
- eBay did not confirm
- Motivation for attack: Hacktivism, not criminal

Event

Search

- The database, which was compromised between late February and early March
- Wasn't detected by the company until early May
- Company announced the cyber attack 2 weeks after discovery (!)

On May 21st - 2014

Search

5.21.2014 Tag: eBayInc.

eBay Inc. To Ask eBay Users To Change Passwords

eBay Inc. (Nasdaq: EBAY) said beginning later today it will be asking eBay users to chan passwords because of a cyberattack that compromised a database containing encrypted and other non-financial data. After conducting extensive tests on its networks, the compa no evidence of the compromise resulting in unauthorized activity for eBay users, and no e unauthorized access to financial or credit card information, which is stored separately in e formats. However, changing passwords is a best practice and will help enhance security f

Information security and customer data protection are of paramount importance to eBay I regrets any inconvenience or concern that this password reset may cause our customers. customers trust us with their information, and we take seriously our commitment to maint secure and trusted global marketplace.

Cyberattackers compromised a small number of employee log-in credentials, allowing unauthorized access to eBay's corporate network, the company sa with law enforcement and leading security experts, the company is aggressively investigating the matter and applying the best forensics tools and practic customers.

Method of Attack

Compromised 3 Employee login credentials

Possibilities

- Social engineering attack
- Web application vulnerability
- Cookie re-use vulnerability

Shell On eBay Server

Search

Fallout

- eBay criticized for not informing customers of data breach quickly enough
- They took 2 weeks after the discovering the breach
- Users were advised to change passwords
- Three US States (Florida, Illinois, Connecticut) launched a joint investigation into the attack, with the Federal Trade Commission (FTC)

Impact on Customers

Search

Vulnerable to indentify theft, could eBay users' identities be up for auction on the black market?

So what does a compromised eBay account go for? Here are the associated values in the cyber underground for compromised eBay accounts:

- 0-5 Feedbacks = $0.2 + mail = $1
- 6-20 Feedbacks = $1 + mail = $5
- 21-50 Feedbacks = $3 + mail = $15
- 51-70 Feedbacks = $5 + mail = $20
- 71-100 Feedbacks = $7+ mail = $30
- 101-300 Feedbacks = $10 + mail = $40
- 301-600 Feedbacks = $18 + mail = $55
- 601-1,000 Feedbacks = $25 + mail = $70
- 1,001-2,000 Feedbacks = $40 + mail = $100
- 2,001-4,000 Feedbacks = $60 + mail = $150

Exploiting Stolen Accounts

- Seller accounts in good standing used to trick customers into buying fraudulent goods
- Buyer accounts in good standing exploited to claim big Paypal refunds after purchases are made

Extent of attack

- "In some cases you go in and find the smoking gun immediately. Other times, it takes a few days or even a few weeks," said Kevin Johnson, a cyber-forensics expert
- Other information my have been comprised
- Has not brought to our attention
- Possible backdoors

Incident Response

- "That's really poor incident response“ (David Kennedy)
- Many were "disappointed" with eBay's response to the breach
- This is all over the news but nothing from Ebay
- Best Practices:
  - Have a message pop up when users log in, telling them about the breach and forcing password changes.

Scope of Responsibility

- Following high-profile breaches at other companies, including
  - Target Corp
  - Neiman Marcus
- Authorities are serious about holding companies accountable for securing data
- The investigation by the states will focus on eBay's measures for securing data
- These attacks are betrayals of customers and that they won't be tolerated

Questions

Search

- **How did this information breach occur?**

  Employee accounts were compromised to gain unauthorized access.

- **Why is it a bad idea to recycle passwords?**

  Stolen passwords from one site can be used on another to gain unauthorized access, even after password is changed on the attacked site.

- **What can customers do to protect themselves once their account is compromised?**

  Change password on attacked site, and on any other site which the same password is used. Review CC and bank statements often, check your credit report every few months, and never click on email links asking for CC or Social Insurance numbers, passwords, or other sensitive information.

References

- http://securityaffairs.co/wordpress/21838/hacking/ebay-paypal-hacked-syrian-electronic-army.html
- http://thehackernews.com/2014/05/worst-day-for-ebay-multiple-flaws-leave.html
- https://twitter.com/CEHSecurity/status/469718659313979393
- http://www.darkreading.com/attacks-breaches/ebay-breach-is-your-identity-up-for-auction/a/d-id/1269162
- http://www.wired.com/2014/05/ebay-demonstrates-how-not-to-respond-to-a-huge-data-breach/

References

- http://bgr.com/2014/05/27/ebay-hack-145-million-accounts-compromised/
- http://www.reuters.com/article/2014/05/23/us-ebay-cybercrime-idUSBREA4M0PH20140523
- https://www.netsparker.com/blog/web-security/learn-ebay-database-hack-attack/
- http://www.forbes.com/sites/ryanmac/2014/05/23/as-ebay-notifies-users-of-hack-states-launch-investigation/
- http://www.ebayinc.com/in_the_news/story/ebay-inc-ask-ebay-users-change-passwords
- http://en.wikipedia.org/wiki/Syrian_Electronic_Army

ebay

Thank You!

Search