REN-ISAC

November 12, 2013

To: IT Executives and Security Staff

REN-ISAC ALERT: Threat to institutional computer accounts by the Adobe breach

BACKGROUND: In October 2013, Adobe suffered a data breach. Their database of 38 million usernames and passwords was stolen and subsequently posted online [1]. The passwords were encrypted, but the encryption was not implemented according to industry best practices [2]. Also stored with the passwords were the users' password hints in clear text. Many of the hints are weak and easily exploited by third parties. Security experts agree that it will be trivial for miscreants to discover the passwords.

The REN-ISAC has been working with security leaders in higher education to monitor the Adobe situation and understand the impact. Of the estimated 38 million Adobe customers affected, our analysis indicates that there were over 2 million education-related accounts. We don't know how many of the email addresses are attached to active institutional accounts.

Adobe reached out to individual affected users via email. The notification thoughtfully included "[we] recommend that you also change your password on any website where you use the same user ID or password". However, there are reports of non-delivery (it might have been filtered as spam) and users disregarding the e-mail (it might have been thought to be a phishing message). The Adobe notification is imperfect.

Therefore, it's important for campuses to act to protect institutional assets and their end users.

POTENTIAL IMPACT: If the same password used for Adobe System accounts was used for work, school, banking, or other accounts, those accounts may be at risk. Repercussions could range from simple to severe, such as account hijacks to send spam, theft of bank deposits, or hackers gaining a foothold in a place of employment to conduct widespread damaging attacks.

MITIGATING FACTORS: The Adobe database contains a fair number of email addresses that are no longer valid or may have changed hands over time.

RECOMMENDATIONS

Organizations should evaluate the following possible actions in terms of their local risk management culture.

1. Broadly notify your organization about this compromise and instruct affected users [3] concerning an immediate reset of institutional passwords. A User Alert Template that can be freely modified and used is included at the bottom of this communication.

2. Consider forcing a local password reset of institutional accounts related to affected users.

3. Communicate to users concerning the inevitable phishing attempts that will follow.

4. Take heed of this and similar incidents and give thoughtful consideration to:

a. Educating users concerning the dangers of password reuse inside and outside the institution [4][5].

b. Local password length and complexity rules [6] and auditing [7].

c. Password expiration rules. Unless people make an affirmative effort to resync all their accounts, periodically forcing them to change important institutional passwords gives some hope that they won't be using an institutional password for external accounts.

d. Evaluate supporting user password vaults. Vaults permit users to easily create and manage unique passwords across all accounts. Examples include KeePass and LastPass.

e. Industry best practices for password databases and storing [8].

f. Weaknesses of password hints. The password hints exposed in the Adobe breach make it clear that many users create hints that are easily exploited by miscreants ("dog's name" discovered via social networking) or that lead to further compromise ("same as work"). Educate users concerning intelligent use of hints, and evaluate alternatives to password hinting as a method for password recovery for local systems.

g. Multi-factor authentication, at least for important institutional resources [9].

ADDITIONAL READING

Password Advice
https://www.schneier.com/blog/archives/2009/08/password_advice.html

Why passwords have never been weaker - and crackers have never been stronger
http://arstechnica.com/security/2012/08/passwords-under-assault/

REFERENCES

[1] http://helpx.adobe.com/x-productkb/policy-pricing/ecc.html

[2] http://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

[3] The database is available at various Internet download sites. Your staff may already have or are able to locate a copy. If you need assistance, send an e-mail from a verifiable (via institutional web pages) executive (CIO, CISO) address to soc@ren-isac.net.

[4] http://xkcd.com/792/

[5] http://www.zdnet.com/passwords-rotten-core-not-complexity-but-reuse-7000013019/

[6] http://xkcd.com/936/

[7] e.g. http://www.openwall.com/john/

[8] https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

[9] https://wiki.internet2.edu/confluence/display/itsg2/Two-Factor+Authentication

---

Copy of this Alert is available on the REN-ISAC web site at:
http://www.ren-isac.net/alerts/adobe_breach_20131112.html

We'd appreciate your input on additional means to protect from the threat and general feedback concerning this Alert. If you have any questions, please don't hesitate to e-mail us at soc@ren-isac.net.

Sincerely,

Your REN-ISAC Team
http://www.ren-isac.net
24x7 Watch Desk +1(317)278-6630

===== USER ALERT TEMPLATE =====
===== FREELY MODIFY AND USE =====

November 12, 2013

ALERT: Threat to computer accounts due to Adobe security breach

BACKGROUND: In October 2013, Adobe suffered a data breach. Their database of 38 million usernames and passwords was stolen and subsequently posted online [1][2]. Adobe did not protect user passwords to industry standards, and attackers were able to exploit that. Also stored with the passwords were the users' password hints in clear text. Many of the hints are weak and easily exploited by third parties. Security experts agree that it will be trivial for miscreants to discover the passwords.

Of the estimated 38 million Adobe customers affected, analysis indicates that there were over 2 million education-related accounts. We don't know how many of the email addresses are attached to active institutional accounts.

Adobe reached out to individual affected users via email. The notification thoughtfully included "[we] recommend that you also change your password on any website where you use the same user ID or

password". However, there are reports of non-delivery (it might have been filtered as spam) and users disregarding the e-mail (it might have been thought to be a phishing message).

IMPACT: If the same password used for Adobe System accounts was used for work, school, banking, or other accounts, those accounts may be at risk. Repercussions could range from simple to severe, such as account hijacks to send spam, theft of bank deposits, or hackers gaining a foothold in a place of employment to conduct widespread damaging attacks.

RECOMMENDATIONS: We recommend that you take the following actions:

1. CHANGE PASSWORDS IMMEDIATELY. Persons who used the same password for Adobe and other accounts should immediately change their passwords at the other locations and monitor for unusual activity. [Optional: The University will be forcing a change of your institutional passwords [additional local details here]].

2. ADOBE PASSWORDS SHOULD BE RESET only by manually visiting the Adobe website, and not by clicking on links arriving via email, as there is now a concern that there will be a rise in phishing related to this event.

3. NEVER REUSE YOUR INSTITUTIONAL PASSWORD for external web sites or Internet services. If you reuse a password at multiple locations when the password is compromised at one site the miscreants then can gain access to all sites where you've used that password. The best policy is to always use different passwords for different accounts.

4. CREATE STRONG PASSWORDS OR PASSPHRASES [3]. The Wikipedia Guidelines for Strong Passwords [4] is a good starting point.

5. CONSIDER THE USE OF A PASSWORD "WALLET" such as KeePass and LastPass. These tools make it very easy to have a unique password for every web site or service, and to have strong passwords.

6. BE ON THE LOOKOUT FOR PHISHING. Miscreants will be using the Adobe breach as a pretext for phishing.

7. USE INFORMATION THAT IS NOT EASILY GUESSED. When providing password hints use information that is not easily guessed or discovered. For example, if your hint is "dog's name" and you mention your dog on social networking sites miscreants can discover that information.

REFERENCES:
[1] http://helpx.adobe.com/x-productkb/policy-pricing/ecc.html
[2] http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/
[3] http://xkcd.com/936/
[4] http://en.wikipedia.org/wiki/Password_strength#Guidelines_for_strong_passwords

====== END USER ALERT TEMPLATE =====