The Never-Ending Hack

In 2012, Dropbox, the popular file hosting service, was the victim of a largescale cyber-attack during which attackers obtained large volumes of email and password data. It has been recently discovered that the data stolen in the 2012 breach has been leaked and that over 68 million accounts have been comprised.

Implications

Security experts recently obtained files from a hacker database-trading website totaling 5GB in size. The files contained email addresses and passwords for 68,680,741 Dropbox users. In response, Dropbox has forced a password reset for accounts that had not been changed since the 2012 attack and recommended that users be on guard for spam and phishing emails, in addition to other malicious activity.

How Does This Impact Your Organization?

Today's hackers leverage various types of data to build databases that allow them to plot and execute their next assault. Email addresses, user IDs, passwords and other personal details are fed into botnets (computers infected with malicious code) to scan the Internet for vulnerabilities. Employees should be notified that strange or unexpected security emails should be reviewed with caution. Suspicious communications should be brought to the attention of your organization's IT department.

Best Practices

- ✓ Account passwords should change frequently – ideally every 90 days
- ✓ Passwords should contain at least 8 characters, with a combination of alpha, numeric and special characters
- ✓ The same password should not be used for multiple accounts
- ✓ Multi-factor authentication (e.g. tokens) should be used for sensitive information
- ✓ Employees should be vigilante of suspicious email attachments and links and avoid questionable websites

Under Attack and in Need of Expert Emergency Assistance?

Radware Can Help. Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, contact us with the code "Red Button".

Learn More at DDoS Warriors To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security

© 2016 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners. Printed in the U.S.A