Dropbox hack and the password security conundrum

The Dropbox hack is the latest reminder that the end is near for traditional authentication methods. Also in Searchlight: VMware comes at cloud from a new direction.

A lot can happen in four years. A president can serve his or her term; a totally new technology can emerge; a haircut can come back in style; or -- in the case of the Dropbox hack -- your passwords can spend that time circulating the dark web.

This week, we discovered that 68 million user email addresses and passwords were compromised in a hack that took place in 2012 -- significantly worse than originally reported at the time. The credentials have started leaking online.

"What's interesting about this hack is that it highlights how long stolen credentials can lie dormant on the dark web and then rear their ugly heads far into the future, often still valid," said Stephen Cox, chief security architect at SecureAuth, an authentication platform.

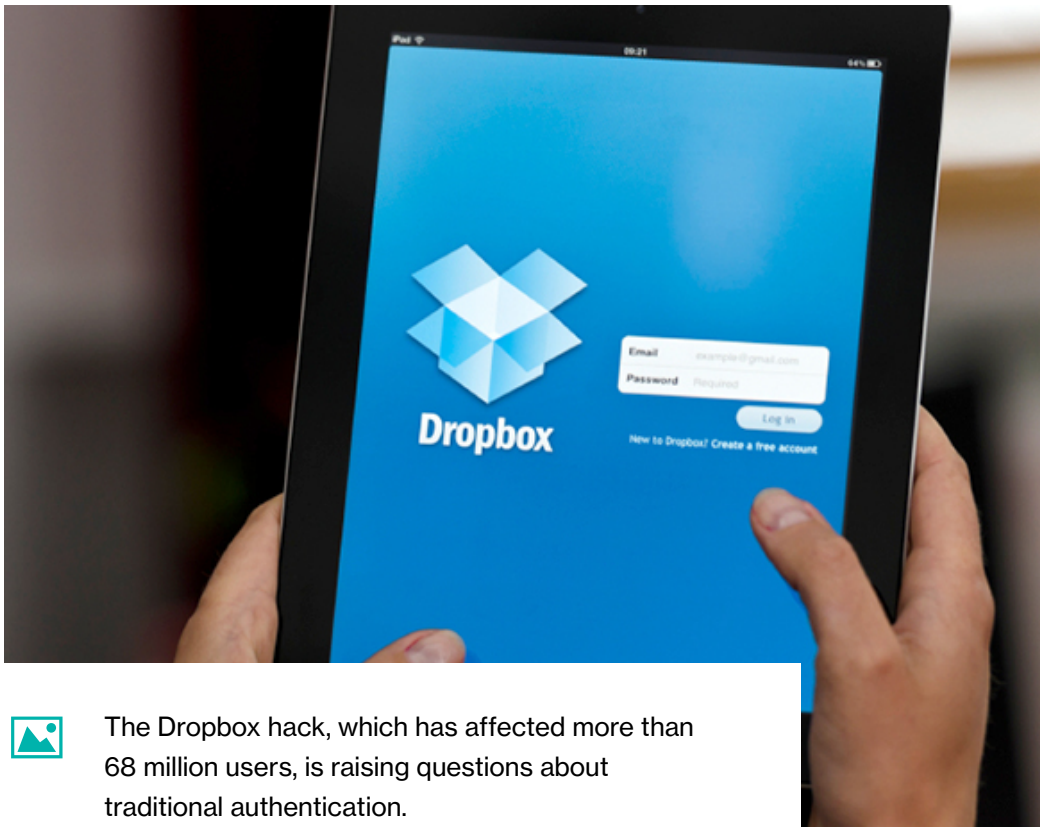
Dropbox has stated that most passwords were encrypted with a strong cipher, but others were not. The cloud storage company sent out notices last week to all users who had not changed their passwords since 2012.

The original Dropbox hack was the result of a Dropbox employee using the same password for both his LinkedIn and corporate Dropbox accounts. The LinkedIn breach -- also in 2012 -- revealed the password and allowed hackers to enter Dropbox's network and gain access to a database with encrypted passwords. The incident raises questions about the effectiveness of traditional password security measures and enterprise security culture.

Security experts say password reuse, unfortunately, is common among us "creatures of habit." [Disclosure: I'm guilty of this.]

"Given the option, people will generally opt for simpler passwords since they are easy to remember," said Michael Isbitski, research director of security and risk management strategies at Gartner. "This holds even truer with the number of applications most of us use on a daily basis, all requiring separate logins."

ISTOCKPHOTO



The Dropbox hack, which has affected more than 68 million users, is raising questions about traditional authentication.

Using authentic credentials to access an account -- also known as account takeover -- has become a popular tactic among hackers, said Travis Smith, senior security research engineer at software company Tripwire. It's less risky for the attacker since using authentic credentials is more likely to go undetected by security tools than other kinds of exploits.

Single passwords' swan song

What can CIOs and IT executives do to prevent account takeovers and password hacks? Making sure employees never use the same password more than once, choose complex passwords and change their passwords more often is a start, said Nathan Wenzler, principal security architect at AsTech Consulting, an independent security consulting company. Password managers are a good tool as well, but they can provide a false sense of security while introducing additional risks, according to John Gunn, vice president of corporate communications at VASCO Data Security.

The consensus among security experts I talked to -- Gunn included -- is that traditional, single-password security measures simply don't cut it anymore; and IT executives need to take note.

"This [Dropbox] incident reinforces the fact that passwords are unsafe at any speed," Gunn said. "Teaching employees to change passwords frequently or use unique passwords doesn't reduce the inherent weaknesses of a 30-year-old, outdated security technology."

As Gartner's Isbitski noted, the frequency of large-scale password leaks only helps further fuel the adoption of multifactor authentication, a burgeoning password security technique.

"Since many users now possess smartphones which can receive SMS messages, [multifactor authentication] is a cost-effective way of adding an additional, effective layer of security," he said.

Since the Dropbox hack in 2012, the company has made multifactor authentication mandatory for all internal systems, something security experts agree is a step in the right direction.

"Two-factor authentication should be mandatory and [include] an opt-out option so users themselves have to make the decision not to use it," said Joseph Carson, head of global strategic alliances at Thycotic, a Washington, D.C. provider of privileged account management solutions.

Biometrics is one form of multifactor authentication that's on the rise, making verification less burdensome on the user and more secure than ever, according to Gunn. But Isbitski is not convinced biometrics authentication is ready for the main enterprise stage yet.

"Biometrics-based authentication systems are difficult to deploy on a large scale because of hardware requirements, aren't widely adopted due to technical limitations, or encounter resistance from users because they are considered too invasive," he said.

While security professionals continue their push to evolve the password and test the validity of biometrics in authentication, hackers continue to exploit existing vulnerabilities. That's why the more authentication options out there for IT executives to explore the better, according to Conrad Smith, CISO at Bitium, a cloud-based identity and access management provider.

"With the diversity of cybercrime and the cost of data breaches continuing to increase, the stakes are too high not to diversify your security tactics," he said.

Getting schooled on password security

Human error is a greater threat than any external threat, said Roman Foeckl, CEO at CoSoSys, a global data loss prevention software company. Leveraging current password security technologies and procedures are important in helping reduce human error, but the issue goes deeper.

Security experts I talked to agree that educating both employees *and* executives is key to reducing security incidents and sparking a cultural shift in the way organizations approach password security.

"In order to establish a company culture focused on security, it's vital for top management to lead the way by 1) conducting -- and participating in -- awareness trainings; 2) establishing and enforcing effective security practices; and 3) setting the tone by holding one another accountable," said Reg Harnish, CEO at security provider GreyCastle Security.

The responsibility to get security right is shared among both IT and the business, said Ankur Laroia, solutions strategy and security leader at Alfresco Software, a business software platform.

In order for awareness programs to be effective, Ajit Sancheti, CEO at Preempt Security, a company specializing in breach detection and response, suggests that training must be more than theoretical rhetoric; it has to be in real-time and tied to actual security incidents, like the Dropbox hack.

With major breaches at Myspace, Tumblr, LinkedIn and Dropbox revealed so far this year, that shouldn't be too hard.

CIO news roundup for week of Aug. 29

There was other tech news this week besides the Dropbox hack. Here are other stories we tracked:

- VMware tweaks cloud strategy one more time. CIOs concerned about cloud provider

lock-in may have less to worry about following VMware's announcement of its new Cross-Cloud Architecture Monday at the annual VMworld conference this week. Cross-Cloud Architecture is designed to provide customers with the "ability to manage, govern and secure applications running across public clouds, including AWS, Azure and IBM Cloud," according to a press release. SearchCloudComputing's Trevor Jones characterized the announcement as an acknowledgement that "VMware's previous strategy to keep everything within its ecosystem didn't match the realities of an emerging multicloud world." The company also introduced Cloud Foundation -- a collection of existing VMware software that includes vSphere, Virtual SAN, NSX and SDDC Manager -- which offers the company's software-defined data center "as a service." VMware has partnered with IBM and will initially roll out Cloud Foundation to IBM's public cloud by the end of September.

- Russian hackers behind voter database breaches? The Federal Bureau of Investigation has gathered evidence that foreign hackers were responsible for two recent attempts to breach voter registration databases in Illinois and Arizona, *Yahoo News* reported Monday. The Bureau warned election officials in the U.S. to enhance security measures ahead of the presidential elections in November. In the Illinois case, information on as many as 90,000 voters may have been compromised by the cyberattack. In the Arizona case, hackers only managed to steal the username and password information of a single election official. This follows the news of hackers breaking into the Democratic National Committee servers in June.

- IoT security trends. According to a new study from Microsoft, security is the top impediment to enterprise IoT adoption through 2017. "Many organizations are hesitant to tap into the power of the IoT due to the complexities and risk associated with managing such a diverse -- and sometimes unclear -- environment," the company said in a blog post. The study estimates that more than 25% of all cyberattacks will target the IoT in 2020, but predicts companies will be spending just a little more than 10% of their security budgets on IoT. In another survey conducted by digital security and compliance services firm Tripwire, 78% of respondents expressed concerns about the weaponization of IoT devices for use in distributed denial-of-service attacks. The survey of 220 information security professionals at the Black Hat USA 2016 conference showed that only 30% of respondents believed their organizations are prepared to handle IoT-related security risks, and more than 50% said their companies cannot correctly track the number of IoT devices on their networks.

- Machine learning to treat cancer. Google DeepMind -- Alphabet's London-based artificial intelligence division -- has announced a partnership with the radiotherapy department at

University College London Hospitals NHS Foundation Trust. The project aims to create an algorithm that can speed up the "segmentation" process that helps differentiate between cancerous and healthy tissues when treating head and neck cancers. The researchers hope machine learning will help reduce the process from four hours down to one hour per patient. "Our collaboration will see us carefully analyze anonymized scans from up to 700 former patients at UCLH, to determine the potential for machine learning to make radiotherapy planning more efficient," the company said in a blog post. Through the partnership, researchers will also seek to develop similar radiotherapy segmentation algorithms for other parts of the body.

Assistant editor Mekhala Roy contributed to this week's news roundup.