Topic: Security

Find out if your data was leaked in the Adobe hack

Summary: *Adobe's database was hacked on October 3, impacting an estimated 150 million Adobe*
a simple way to see if you're affected.

By Violet Blue for Zero Day | November 11, 2013 -- 23:27 GMT (23:27 GMT)
Follow @@violetblue

Wonder if your email address, password, credit card information or more was leaked to the world when Adc
was hacked last October?

If you've gotten your email address anywhere near an Adobe product past or present, then the answer is: p

Recent reports reveal that Adobe's stolen database held around 150 million user accounts (http://nakedsecurity.
/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/) - and not the 2.9 million (/article/adobe
2-9m-customer-accounts-have-been-compromised/) Adobe originally reported, or the 38 million (/article/adobe-security-brea
affected-closer-to-38-million-users/) Krebs on Security later reported.

Entities both friendly and malicious are crawling all over the data. Much of what we're learning about the breach has come from independent researchers not affiliated with Adobe.

Facebook, Diapers.com and Soap.com are currently mining Adobe's hacked database (http://krebsonsecurity.com/2013/11/facebook-warns-users-after-adobe-breach/comment-page-1/) file to find their own users and tell users they've been compromised by the breach - but you can find out on your own.

See if your info is in the file stolen from Adobe

Dutch student Lucb1e (https://twitter.com/lucb1e) made a handy search tool out of the data (http://www.lucb1e.com/?
where the security conscious can find out if their personal information is in the file being passed around onl

To use Lucb1e's Adobe hack search tool (http://www.lucb1e.com/credgrep/), enter in a partial email address (or a
address).

Then, either re-check the page or have the results emailed to you - Lucb1e recommends that you have the
emailed.

The results are not instant.

Lucb1e explains, "Searches will not be performed all day. You can submit a search query, but it will not be p
instantly. Instead, I'll run all searches twice a day or so."

When you run his search tool:

> It will tell you what information exists in the file for your email address, and email you the report if y
>
> Based on the encrypted information it can see in the password, it will tell you certain information abc
> password that it can deduce, like the approximate length of it.

What if your results come up positive?

If you're in the file change your passwords immediately (if you haven't already done so).

"9,334 of these rows contain a @purdue.edu email address"

Paul Ducklin at Sophos [Naked Security] wrote (http://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disas sized-cryptographic-blunder/),

> A huge dump of the offending customer database was recently published online, weighing in at 4GB compressed, or just a shade under 10GB uncompressed, listing not just 38,000,000 breached record 150,000,000 of them.
>
> As breaches go, you may very well see this one in the book of Guinness World Records next year, wh make it astonishing enough on its own.

The stolen file contained both active and inactive accounts for "numerous Adobe products" (examples inclu Photoshop, ColdFusion, CreativeCloud).

The file holds Adobe IDs, email addresses, (encrypted) passwords, credit/debit card numbers, expiration da (Personally Identifiable Information) and more.

At this time, it is believed that the file's passwords have not been cracked.

Yet this belief veils little more than a race to the encryption key, as this week we learned that Adobe's pass unlocked with a single key.

Ducklin wrote,

> The use of a symmetric cipher here, assuming we're right, is an astonishing blunder, not least becau both unnecessary and dangerous.
>
> Anyone who computes, guesses or acquires the decryption key immediately gets access to *all* the pa in the database.

We can only imagine how much money that key is worth now.

Is it safe to use Lucb1e's search?

Lucb1e writes,

> I temporarily store your IP address, the search query and the search result.
>
> This data is stored for 48 hours. After that, all your data is permanently erased.
>
> If you tick the 'email results' box, you receive 1 email. Storing your IP is for security reasons. If som submits ten thousand searches at once, it automatically blocks that.
>
> Who can access this data? Me and only me. And the Dutch government if they do a formal request (v hours, after that it's permanently gone like I said before), but I've never received such a request, no expect to. Also be sure to use https if you're concerned about that kind of thing.

Lucb1e had an interesting time creating his search tool, and received helpful feedback from his co-Reddito (http://www.reddit.com/r/technology/comments/1pu79d/has_your_data_been_leaked_in_the_adobe_hack/) on making it faster ar efficient.

He documented the process in Searching 10GB of data As A Service - lessons learned (http://www.lucb1e.com/?p interesting series of his own "Training Waves."

> The day before yesterday I launched a service where you can check whether you were included in th accounts hack. I had the file, it could be grepped for stuff in about 30 seconds, and I thought "hey, c might want to do this too". And so I started coding.
>
> My parents would be home soon and we'd go out for dinner, but I wanted it done. (...)
>
> (...) I started mashing another script together which connected to the server, got some search querie the queries in batches on my laptop's local database, and posted the results back to the server.
>
> This was epicly fast.
>
> Then I multithreaded it.
>
> This was super epicly fast.

He concludes with three excellent lessons, the last of which includes:

> Test and **think** before putting something out there.
>
> Don't rush too much.

Let's hope Adobe reads that bit, and takes it to heart.

Topics: Security, Cloud, Servers

About Violet Blue

Ms. Violet Blue (tinynibbles.com, @violetblue) is a freelance investigative reporte and cybercrime at Zero Day/ZDNet, CNET and CBS News, as well as a noted sex She has made regular appearances on CNN and The Oprah Winfrey Show and is r interviewed, quoted, and featured in a variety of publications that inclu... Full Bio

Follow @@violetblue Contact Disclosure

Kick off your day with ZDNet's daily email newsletter. It's the freshest tech news and opinion, served

Join the discussion