2015/11/24 Forbes Passwords Leak |

KASPERSKY DAILY

November 24, 2015

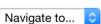
Search

Search

- Twitter
- Facebook
- YouTube
- LinkedIn
- Google+
- RSS

Select Language

- **English**
- Russian
- <u>Español</u>
- German
- Français Italiano
- Portuguese
- Japanese
- LatAm
- Polish
- C Turkish
- <u>Chinese</u>
- Arabic
- UAE
 - Home
 - News
 - Security
 - Products
 - Tips
 - Malware
 - Interviews
 - Projects
 - Contact



Select Language

- **English**
- Russian
- <u>Español</u>
 - <u>German</u>
- Français
- <u>Italiano</u>
- PortugueseJapanese
- LatAm
- Polish
- Turkish
- Chinese
- Arabic
 UAE
- Previous
- Next

Forbes Passwords Leak

2015/11/24

February 19, 2014 Cassie Bodnar Featured Post, News No comments

The Syrian Electronic Army (SEA) has struck again, this time attacking the account records of more than a million Forbes readers and contributors. A total of 1,071,963 users were affected when the database that held their email addresses and correlating passwords was exposed and shared online by the cybercriminals. Three Forbes articles were vandalized and the company's blog went dead as well. But how was the SEA able to strike such a large infrastructure?



It's believed Forbes stored user information in a PHP Portable format. Essentially, this means every password and a random salt, used to slow down attackers, were run through the MD5 algorithm. This algorithm is a popular cryptographic hash function that's commonly utilized to verify the legitimacy of data. Forbes ran 8,192 duplications of MD5 on the hash and password and then stored the results in their database.

The SEA then came in and took this stored information to play what turned out to be a harmful guessing game. They tried out random everyday passwords, like "ABCD," with users' salts, producing a hash, which was then referenced with Forbes' database. When matches were made, passwords were exposed.

Although the passwords were one-way encrypted, Forbes is urging its readers to change their login information, saying:

Essentially, this means every password and a random salt, used to slow down attackers, were run through the MD5 algorithm.

exposed. Please be wary of emails that purport to come from Forbes, as the list of email addresses may be used in phishing attacks. We have notified law enforcement. We take this matter very seriously and apologize to the members of our community for this breach.

The major issue here is the fact that people tend to use the same username and password for multiple accounts. So any Forbes reader who had their information shared publically, that uses the same username and password combination for other accounts, is now at risk for a broader, multi-platform attack.

This is why we cannot caution you enough against this method of operation. If one of your accounts is attacked, the rest are vulnerable, and cybercriminals are well aware of this fact. We therefore urge you to utilize <u>password manager</u>, which allows you to store strong, individual passwords for each of your online accounts, ensuring a breach of one profile will not mean a total loss of information across all of your active platforms.

Facebook 0 9t Google 0 Twitter in Linkedin 0

O' doogle o Twitter III Linkedin o Trackernews o
hackspassword breach About Cassie Bodnar "You can make anything by writing." — C.S. Lewis View all posts by Cassie Bodnar → Leave a Reply Your email address will not be published. Required fields are marked *
Name *
Email *
Website
Comment
I'm not a robot reCAPTCHA Privacy - Terms
FUST CONTINENT

Related Posts

2015/11/24 Forbes Passwords Leak |

Security Week 33: Doors without locks, i...

August 18, 2015



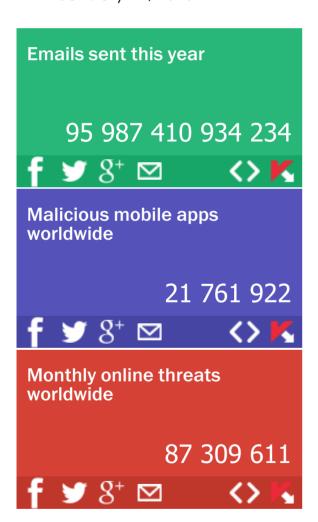
Black Hat USA 2015: The full story of ho... August 6, 2015



Talk Security: Million Dollar Malware, G... April 10, 2015



Remember the Gawker Media Password Breac...
January 22, 2015





<u>2869167</u> Likes

244079 **Followers** @kaspersky

@bumdwarf Sorry on the scam glad the product helped:)
book 9 hours ago

Botus of **Retweet**

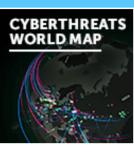
https://t.co/YgBCWYigpb via @threatpost https://t.co/uNqmQCT9yL 9 hours ago

@jwalden74 We will ticket open with sur 10 hours ago Retweet

- 1. 1 2. 2 3. 3 4. 4 5. 5











KASPERSKY # **PROTECTS ALL OF YOUR DEVICES Kaspersky Internet Security** Multi-Device Protection Buy now

Trending Authors



Kate Kochetkova 3,063 post views



Vladislav Biryukov 1,620 post views

Alex Perekalin



640 post views

Jeffrey Esposito 153 post views

Kaspersky Podcasts



How to avoid problems when purchasing security software: study system requirements

When you purchase software, you automatically agreed that your device complies with systems requirements defined by the software vendor. That's why you should always...



Tip of the week: How to protect yourself from online data collection



Talk Security Podcast: Security at Google I/O, the IRS Data Breach and More



Talk Security: Million Dollar Malware, Github DDoS



Talk Security: Kaspersky Lab Security Analyst Summit 2015



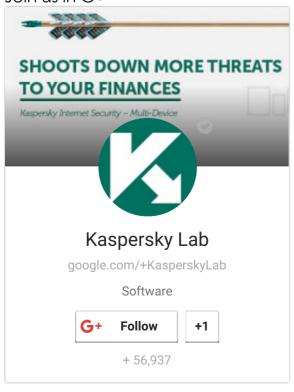


Let's save the world together!

2015/11/24 Forbes Passwords Leak |



Join us in G+



- Products for Home
 - Kaspersky Total Security Multi-Device
 - Kaspersky Internet Security Multi-Device
 - Kaspersky Internet Security 2015
 - Kaspersky Anti-Virus 2015
 - Kaspersky Internet Security for Mac
 - Kaspersky Internet Security for Android
 - Kaspersky Password Manager
 - Kaspersky Security Scan FREE
- Products for Enterprise Business
 - Kaspersky Endpoint Security for Business | Advanced
 - Kaspersky Endpoint Security for Business | Select
 - Kaspersky Endpoint Security for Business | Core
 - Kaspersky Total Security for Business
 - Targeted Security Solutions
- Products for Small Office
 - Kaspersky Small Office Security
- For Software Users
 - Buy online
 - Renew license
 - Get updates
 - Try for free
- Technical Support
 - For home products
 - For business products
- About Us
 - About Kaspersky Lab
 - Why Kaspersky?
 - Press Center
 - Site Map
 - Privacy policy
 - Contact us
 - Legal
- Blogroll
 - Eugene Kaspersky's Blog
 - Securelist
 - Threatpost
 - Kaspersky Business
 - Kaspersky Academy



© 2015 AO Kaspersky Lab. All Rights Reserved.

39A/3 Leningradskoe shosse Moscow 125212 Russia

The authors' opinions do not necessarily reflect the official positions of Kaspersky Lab.