Hackers launch huge DDoS attack using WordPress websites

Thousands of WordPress websites are being used to carry out a huge cyber attack campaign in the form of a distributed denial of service [DDoS] attack.
Average daily WordPress brute force attacks in April

via sucuri.net
Average daily WordPress brute force attacks

<table>
<thead>
<tr>
<th>Month</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>40,000</td>
</tr>
<tr>
<td>February</td>
<td>36,000</td>
</tr>
<tr>
<td>March</td>
<td>31,000</td>
</tr>
<tr>
<td>April</td>
<td>169,033</td>
</tr>
</tbody>
</table>

via sucuri.net
70,855,411

WordPress Sites in the World
2 miliony kont z Chomikuj.pl na sprzedaż

Millions of LinkedIn passwords reportedly leaked online

Filmweb.pl hacked! Wyciekło 700 000 haseł użytkowników

SECURITY
Last.fm Passwords Also Leaked; Change Yours Now

HACKERS
Hey, Guess What: Your eHarmony Passwords Were Leaked, Too

Poważny błąd w Allegro umożliwiał poznanie haseł użytkowników!
Zappos Says Hackers Accessed 24 Million Customers' Account Details

**HACK**

*Yahoo hacked, 450,000 passwords posted online*

*Sony Hacked Again, 1 Million Passwords Exposed*

*Valve: Hackers Accessed Steam Users’ Encrypted Passwords, Credit Cards*

*Home / Security News / Hackers*

*AMD hacked, staff logins leaked*
8.24 million Gamigo passwords leaked after hack

420,000 Formspring Passwords Compromised in Security Breach

Blizzard's network of more than 10 million hacked

E-mail lists, encrypted passwords stolen in Battle.net hack
100 Million Chinese Usernames, Passwords Leaked in Massive Hack Heist

Hackers Leak 1 Million Accounts from Over 100 Websites Worldwide

YouPorn Hacked And Over 1 Million Usernames and Passwords Leaked

Android Forums hacked: 1 million user credentials stolen
Reliance on passwords is biggest security threat, says hacking expert

Tuesday 29 June 2010 15:01

Passwords are fundamentally insecure and represent the biggest security threat facing organisations, says Jason Hart, senior vice-president for Europe at security firm Cryptocard.

Hart, a former ethical hacker, is able to demonstrate how easily available software can be used by hackers to capture every username and password of any user on a network.

Hackers are able to view the username and password victims type in to access e-mail systems, business systems and cloud services, even those using a secure internet protocol (https) or encryption.

It is impossible to protect anything that connects with the internet through any means against this kind of attack at the protocol level, he said.
Hackers favor authentication-based attacks, report shows

Summary: A suitable password replacement could disrupt or defeat 80% of these attacks, report concludes.
Targeted Attacks, Weak Passwords Top IT Security Risks in 2013

By Robert Lemos | Posted 2013-01-01

Companies should hunt down systems with default passwords and beware that more sophisticated attacks will seek to fool employees, predict two security firms.

The biggest security threats to companies in 2013 will depend on who is attacking the business: Opportunistic criminals will continue scanning for accounts with default or weak passwords, while targeted attackers will refine their attempts to fool employees, business services firm Verizon and security software firm McAfee stated in separate reports.

In the past year, about 90 percent of successful breaches analyzed by Verizon started with a weak or default password, or a stolen and reused credential, which is a trend that will continue, said Wade Baker, managing principal for the company’s RISK team. The company analyzed data gathered from incidents it investigated in 2012 to identify the causes of data breaches.

“Taking all the attacks that happened to larger corporations and government, about 90 percent had weak or stolen credentials,” Baker said. “We see no reason that that trend will change in 2013.”

A year ago, an analysis of the breach of global-intelligence firm Stratfor found that many of the site’s customers had selected weak passwords for their accounts, with one analysis breaking about 10 percent of the passwords in five hours. Other analyses of leaked passwords have found similarly poor password choices, as well as the reuse of passwords across sites.
Web services using two-factor authentication
Web services using two-factor authentication
Two-step verification for Apple ID.

Two-step verification will require you to verify your identity using one of your devices before you can make changes to your account or make an iTunes or App Store purchase from a new device.

You enter your Apple ID and password as usual. | We send a verification code to one of your devices. | You enter the code to verify your identity and complete sign in.
And then, my tumblr just got deleted. Wow. I just added two-step verification to all that allowed.
Compliance

**PCI-DSS**  
(Payment Card Industry Data Security Standard)

**HIPAA**  
(Health Insurance Portability and Accountability Act)

**CJIS**  
(Criminal Justice Information Services Division of the FBI)
“Usernames and passwords, reusable passwords in particular, are terrible ideas. We do a bad job at picking them, we don't change them often enough. What we need is two-factor authentication.

Google offers this freely to all of its users, but we need to, all of us, start addressing that. So if you're gonna build a platform that involves identifying users will you please use two-factor authentication.”

Jozihub Firesie Chat on September 6, 2013, in Johannesburg, South Africa