Severity:
HIGH

CTM360®
Powered by EDX LABS
Subsidiaries: PENTEST360 | DMARC360 | MG360

WORDPRESS PHARMA HACK

BY SARA KHALAF

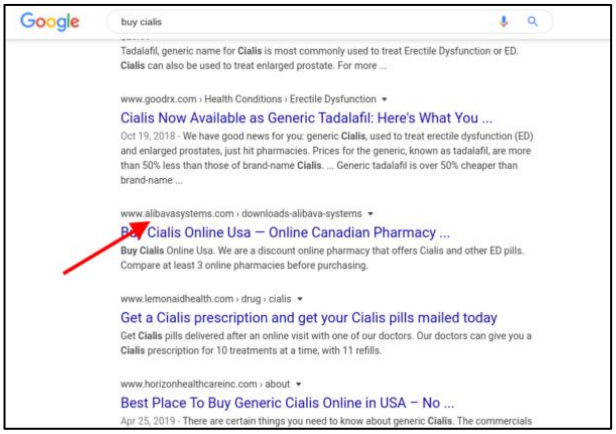
Date: 5th November 2020
Category: Website Vulnerability

THREAT TARGETS:	POSSIBLE IMPACTS:	TARGET AUDIENCE FOR CIRCULATION:
● Websites running on WordPress	● Website hijacking ● Website defacement ● Search engine delisting	● Website Administrators ● IT Security Teams

Pharma Hack is an exploit targeting WordPress sites using SEO spamming. Hackers inject the site with content related to pharmaceuticals in order to lure users who are looking for drug resellers either to purchase without a prescription or get a cheaper price. Attackers hijack well established sites to bypass Google's efforts in delisting websites offering to engage in illegal drug sales.

How to identify if a website is Pharma hacked?

Pharma Hacks can be tricky to discover because the hack is not visible to the website owner. The only way to view these are through search engines when a user is looking for specific drugs. Hackers target sites that rank high and have a massive amount of traffic for better earnings prospects.



Google
buy cialis

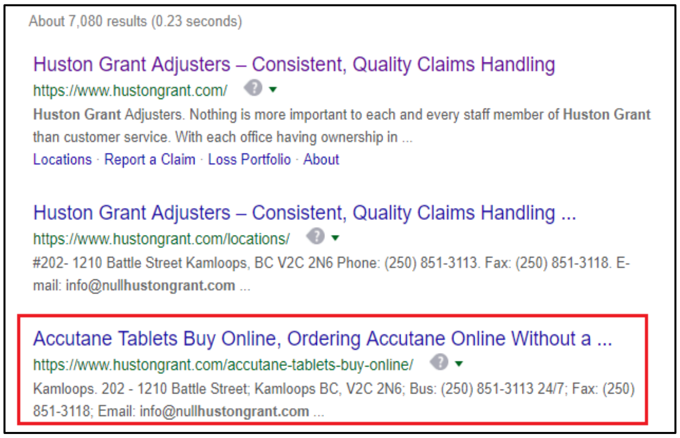
Tadalafil, generic name for **Cialis** is most commonly used to treat Erectile Dysfunction or ED. **Cialis** can also be used to treat enlarged prostate. For more ...

www.goodrx.com › Health Conditions › Erectile Dysfunction ▾
Cialis Now Available as Generic Tadalafil: Here's What You ...
Oct 19, 2018 - We have good news for you: generic **Cialis**, used to treat erectile dysfunction (ED) and enlarged prostates, just hit pharmacies. Prices for the generic, known as tadalafil, are more than 50% less than those of brand-name **Cialis**. ... Generic tadalafil is over 50% cheaper than brand-name ...

www.alibavasystems.com › downloads-alibava-systems ▾
Buy Cialis Online Usa — Online Canadian Pharmacy ...
Buy Cialis Online Usa. We are a discount online pharmacy that offers Cialis and other ED pills. Compare at least 3 online pharmacies before purchasing.

www.lemonaidhealth.com › drug › cialis ▾
Get a Cialis prescription and get your Cialis pills mailed today
Get **Cialis** pills delivered after an online visit with one of our doctors. Our doctors can give you a **Cialis** prescription for 10 treatments at a time, with 11 refills.

www.horizonhealthcareinc.com › about ▾
Best Place To Buy Generic Cialis Online in USA – No ...
Apr 25, 2019 - There are certain things you need to know about generic **Cialis**. The commercials



About 7,080 results (0.23 seconds)

Huston Grant Adjusters – Consistent, Quality Claims Handling
https://www.hustongrant.com/ ▾
Huston Grant Adjusters. Nothing is more important to each and every staff member of **Huston Grant** than customer service. With each office having ownership in ...
Locations · Report a Claim · Loss Portfolio · About

Huston Grant Adjusters – Consistent, Quality Claims Handling ...
https://www.hustongrant.com/locations/ ▾
#202- 1210 Battle Street Kamloops, BC V2C 2N6 Phone: (250) 851-3113. Fax: (250) 851-3118. E-mail: info@null**hustongrant.com** ...

Accutane Tablets Buy Online, Ordering Accutane Online Without a ...
https://www.hustongrant.com/accutane-tablets-buy-online/ ▾
Kamloops. 202 - 1210 Battle Street; Kamloops BC, V2C 2N6; Bus: (250) 851-3113 24/7; Fax: (250) 851-3118; Email: info@null**hustongrant.com** ...

Key indicators that a site has been infected with the hack would include an unusual decrease or increase in traffic for no apparent reason. Google might remove your site from the search results for suspicious behavior. To help identify those scams you can use a security plugin to scan your site or opt for a manual scan which could be more challenging.

Common WordPress Vulnerabilities

WordPress themes and plugins unfortunately are flawed with vulnerabilities. Even though patches are released as an update, there is a possibility of clients running outdated versions. WordPress has tried to resolve this issue using the Auto-update feature.

WordPress site owners tend to use 'easy to remember' username and passwords or retain the default username 'admin'. This along with not implementing Two Factor Authentication invites brute force attacks.

Many website owners still run on HTTP and not HTTPS, which makes intercepting connection on the website easy for attackers. It is vital to install SSL certificates.

Hackers look for highly ranked websites such as banking websites that attract a high volume of traffic, in order to use the website for further goals such as spreading malware, hacktivism, adding bandwidth to bot networks used in DDOS attacks or merely for practice runs. The lack of sensitive information on your website does not ensures your safety. Instead you need to take the necessary security measures to ensure your protection against attacks.

Recommendations

- Update to the newest version of your CMS along with the plugins
- Always use and download legitimate themes and plugins and make sure the auto-update is enabled.
- Set complex credentials for login along with Two Factor Authentication (2FA).
- Make sure SSL Certificates are installed.
- Identify and block any unusual traffic.

References:

https://arstechnica.com/information-technology/2020/09/hackers-are-exploiting-a-critical-flaw-affecting-350000-wordpress-sites/
https://blog.sucuri.net/2020/06/find-fix-wordpress-pharma-hack.html
https://blog.sucuri.net/2020/02/pharma-hack.html
https://www.clearhaus.com/blog/pharma-hacking/

Disclaimer

The information contained in this document is meant to provide general guidance and brief information to the intended recipient pertaining to the incident and recommended action. Therefore, this information is provided "as is" without warranties of any kind, express or implied, including accuracy, timeliness, and completeness. Consequently, under NO condition shall CTM360®, its related partners, directors, principals, agents or employees be liable for any direct, indirect, accidental, special, exemplary, punitive, consequential or other damages or claims whatsoever including, but not limited to: loss of data, loss in profits/business, network disruption…etc., arising out of or in connection with this advisory.

For more information:

Email: monitor@ctm360.com Tel: (+973) 77 360 360