WORLDWIDE: SHADOW ONLINE PHARMACIES CAPITALIZE ON COVID-19 CRISIS

Summary:

Babel Street analysts identified several shadow online pharmacies in the summer of 2019. These pharmacies typically advertise "*no prescription required*" and claim to sell generic versions of certain medications at discount prices. A reevaluation of these pharmacies reveals that some are now advertising drugs that have been mentioned as possible, but unconfirmed, treatments for COVID-19.

BLUF:

- Online US sales increased by 25% over normal volume in March 2020. Shadow online pharmacies seized on the increased activity to sell COVID-19 related drugs.
- Shadow pharmacies are deploying black hat SEO manipulation tactics by using compromised or hacked websites that redirect to the online pharmacy domains, as well as bots to spam the URLs across blogs, forums, and comments in articles to boost their appearance in search results.
- These pharmacies also have adopted more direct tactics, foregoing obfuscation, by employing SEO manipulation and incorporating the names of COVID-19 related drugs directly into URLs. This may signify opportunistic diversification of tactics to take advantage of the current crisis.

Background on Shadow Pharmacies

In November 2019, Babel Street published findings highlighting the illicit practices of some online pharmacies. [1]These pharmacies routinely use a combination of hacked websites and "black hat" search engine optimization (SEO) techniques to manipulate search engine algorithms to drive unwitting consumers to e-commerce platforms. Previous research identified the most commonly advertised drugs (Table 1) as well as common posting tactics used by the pharmacies. This Babel Beacon updates those findings within the context of the COVID-19 pandemic. Analysts sought to answer the following questions: 1) Are shadow pharmacies still employing the same tactics, techniques, and procedures (TTPs), and 2) Are online pharmacies illicitly advertising or selling drugs associated with the pandemic?

Table 1 - *Top drugs mentioned in 2019 search results* **Product**	**# Documents Containing Product w/in Babel dataset**
Tadalafil (generic Cialis)	2563
Sildenafil	1873
Viagra	1782
Vardenafil	1232

[1] https://www-pm360online-com.cdn.ampproject.org/c/s/www.pm360online.com/criminals-are-advertising-your-products-online-thats-a-problem/amp/

Increased COVID-Related Activity and Risk

By mid-March 2020, daily e-commerce sales in the U.S. increased by 25% compared to the beginning of the month—driven primarily by grocery and household good sales.[2]This increase is due in part to stay-at-home orders and social distancing related to the COVID-19 pandemic. Additionally, some consumers are participating in "panic buying" due increased fear and uncertainty associated with the crisis. As a result, illicit cyber actors likely see an opportunity to exploit the increased number of online consumers. As consumers make the shift to online purchasing, they should be aware of the risks in purchasing from questionable or shadow pharmacies. Per FDA guidelines, there are several signs of "rogue online pharmacies." These signs include allowing individuals to buy prescription medicine without a valid prescription, offering very low prices that seem "too good to be true", operating from locations outside of the United States, or offering worldwide shipping[3]. Babel Street analysts have identified numerous questionable online pharmacies with these dubious attributes.

How Illicit Online Pharmacy Activity Works and Current Trends

Using Babel X—a text-based analytic platform—Babel Street analysts were able to determine that shadow online pharmacies, or paid third party spam marketing organizations, are likely acquiring hacked sites to serve as seemingly legitimate root domains for the pharmacies' own suspect URLs. These once legitimate, but now compromised domains, serve as veritable "top cover" for the shadow pharmacy links. The pharmacies then use bots to spread these URLs online. The links are posted to message boards, forums, and in the comments sections of articles and blog posts. Based on the data, it is assessed that authors often share the same post or URLs across multiple threads in a forum.

In addition to using bots to post links to the shadow online pharmacies, most of the links used do not *appear* to be nefarious, or even related to a pharmacy, but the legitimate-appearing-domains are likely hacked sites. As the URLs are spread, it boosts SEO results (prioritization in search results) for the online pharmacy. Of the URLs reviewed, once someone clicks on the main, seemingly legitimate link, the page redirects to the online pharmacy page. For example, Babel Street analysts determined that at least three separate online pharmacies were tied to one compromised URL of a legitimate church website (Figure 1). After following the link associated with the church website, users were redirected to one of the three websites below.

Figure 1: Online Pharmacy Sites Tied to Compromised URL

Babel X's quick search feature, Find X, provided additional insights into registration and hosting IP information for the identified pharmacy domains above. Further, one of the hosting IP addresses appears to host approximately 43 other websites–the majority of which appear to

[2] https://www.digitalcommerce360.com/2020/04/01/us-ecommerce-sales-rise-25-since-beginning-of-march/
[3] https://www.fda.gov/consumers/consumer-updates/how-buy-medicines-safely-online-pharmacy

be online pharmacies. Most of the pharmacies identified though Babel X advertise the sale of generic drugs and often offer discounts or bonus pills with orders. Some sites even claim to be FDA approved.

COVID-Specific Drug Activity

An April 2020 KrebonSecurity article indicated online pharmacies have seen dramatic increases in the sale of pandemic-related drugs such as hydroxychloroquine, and in some cases COVID-19 drug sales now rival primary products such as Viagra and Cialis.[4] In light of this shift, Babel Street revisited the collection results from the summer of 2019 to see if the previously discovered online pharmacies had shifted TTPs and changed the types of drugs advertised in response to COVID-19. Upon review, it appears that the previously identified online pharmacies, for the most part, continued their previous practices. To examine the topic further, Babel Street analysts built new searches to identify if and where some of the drugs mentioned as potential COVID-19 therapies appear for sale online.

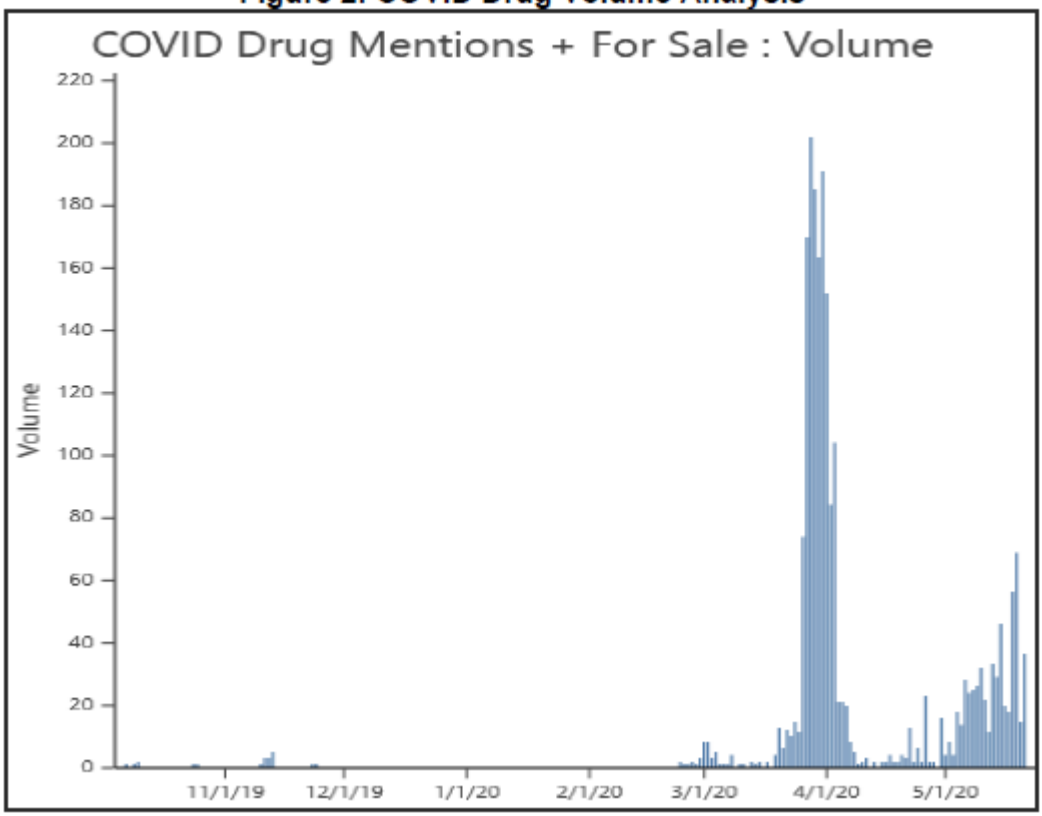
In March and April 2020, the FDA issued five new internet pharmacy warning letters. The letters were related to the offer of "drug products for sale in the United States and that these products are intended to mitigate, prevent, treat, diagnose, or cure COVID-19." The specific drugs mentioned included: Ritonavir, Ritomune, Lopinavir, Lopimune, Fluvir, and Antiflu.[5] Additionally, there have been reports on the anti-malaria drugs, Plaquenil (hydroxychloroquine) and Aralen (chloroquine), as possible therapies to treat COVID-19; although this has yet to be confirmed as an effective treatment.

Analysts examined where these specific drugs were mentioned for sale online with "no prescription required." The analysis used the multi-lingual ontology capabilities within Babel X to scour open and dark web data for drug sales, returning broad results across languages and name variants for the same drug. For example, the search of one term, "Aralen" leverages 175 unique representations across 27 languages.

Volume analysis (Figure 2) of the specific COVID-19 drug mentions indicates a spike from mid-March to early-April. In April, there was a decline in the number of terms mentioned—perhaps due to increased enforcement or supply and shipping shortages. However, by mid-May, pandemic-related drug mentions were significantly increasing once again. This could be an indication of one or many shadow online pharmacies spamming COVID-19 related drug links.

[4] https://krebsonsecurity.com/2020/04/unproven-coronavirus-therapy-proves-cash-cow-for-shadow-pharmacies/
[5] https://www.fda.gov/drugs/drug-supply-chain-integrity/internet-pharmacy-warning-letters

Figure 2: COVID Drug Volume Analysis



URL analysis for the COVID-specific collection also revealed the emergence of a more direct TTP employed by the online pharmacies offering COVID-related drugs. Some of the COVID-19 associated URLs continue to use hijacked root domains for obfuscation and redirection; however, several sites have begun to include the specific COVID-19 related drug names in the root domain name. These URLs are new sites created to sell these newly popular drugs online. For example, domain analysis in Babel X shows that https://hydroxychloroquinesale.com, was created on 10 April 2020 and https://plaquenil200.com was created on 21 March 2020.

Further review of the top mentioned URLs revealed that although some of the domain names are different, and eschew the obfuscation identified in the 2019 analysis, the URLs resolve to many of the same shadow online pharmacies that have been around for years, such as Pharmacy World. The online pharmacies simply changed the domain name to the COVID-19 related drugs. This may signify that these actors have judged the potential reward from selling COVID-19 related drugs outweighs the potential risks associated with a more obvious online posture.

Conclusion and Outlook

Shadow online pharmacies remain active and seek to exploit the COVID-19 pandemic for financial gain—often using established TTPs. Consumers need to be wary and pay heed to the red flags of shadow pharmacies lest they be financially bilked and subjected to potentially

ineffective or dangerous drugs. This Babel Beacon provides a brief overview of some of the online pharmacy activities; however, there are still many unanswered questions. Additional networks, TTPs, and markets could be revealed upon further review.

Author: ***Ms. Brittany Mason*** *is a Senior Solutions Specialist for Babel Street. A career analyst, prior to joining Babel Street, she served for several years as a Staff Operations Specialist at the Federal Bureau Investigation.*