Cyveillance
1555 Wilson Blvd., Ste 406
Arlington, VA 22209
www.cyveillance.com

Threats to national cyber infrastructure do not always come in the form of malware, viruses, or unpatched software. Domestic and international organized crime depends on the internet as a significant revenue source, enabling their further growth in cyberspace and “real world” influence.

One particularly active arena of illicit activity online is illegal sale of pharmaceutical drugs. Illegal online pharmacies do not require the mandated face-to-face meeting between patient and caregiver before sending prescription medication to the buyer. The risks to consumers who use online pharmacies are many:

- without appropriate professional medical oversight of the access to powerful presciption drugs, there is a higher risk of prescription drug abuse or death
- the prescription medications may be produced in unregulated factories overseas by manufacturers that are not FDA approved, increasing the chances of substandard or ineffective medications being received
- the “medications” received by the consumer may be counterfeit, causing harm not only because they do not treat the medical condition they were purchased to improve, but because they may be composed of harmful chemicals

The examples above are more than possibilities; documented cases exist of American consumers who were customers of illegal online pharmacies and died as a result. Many more undocumented cases are sure to exist.

Today we will examine illegal online pharmacies and the complicity of American companies which enable their crimes, discuss the risks they pose to American consumers and overall cybersecurity, and make recommendations to make it harder for such criminals to put Americans at risk.

Hosting Companies

Whenever an internet user wants to visit a website, a computer server answers the request and delivers that website to the internet user. These servers can be located anywhere in the world. If you run a website you normally pay a hosting company so that its servers will deliver your website to internet users.

The webmasters of illegal online pharmacies are like any other website owner and prefer hosting companies that are reliable and geographically close to their potential customers

so that connections are generally quicker. Unfortunately, the highly competitive hosting market and lack of consequences for aiding and abetting these criminal operations result in many American hosting companies which are all too ready to offer them hosting services.

There are servers in the United States which host hundreds of illegal online pharmacies. While these companies will accurately respond that their terms of service prohibit such activity, it is the experience of Cyveillance and its peers in the fight for a safer internet that the verbiage in those terms of service are merely window dressing and are very rarely enforced. While there are companies like GoDaddy which will move quickly to cancel or suspend services to illegal online pharmacies, the majority of the hosting industry either does not respond to takedown requests for these unlawful websites or will move so slowly in their response that months can pass before action is taken, allowing the illegal online pharmacies to continue harming consumers. Their general attitude is that the hosting company is not responsible for the content housed on their systems, despite the fact that this position enables illegal activity that causes physical harm.

SSL Certificate Vendors

Secure Sockets Layer (SSL) is a technology which encrypts the communication between an internet user's browser and a website. This makes it safer for internet users to go shopping online, because their credit card information is hidden when it is sent to the website for payment. Webmasters purchase SSL certificates to enable this functionality and this gives consumers the sense that the website is run by a sound merchant to do business with.

Illegal online pharmacy webmasters know that internet users prefer to do business with sites which have SSL enabled. They will pay SSL certificate vendors for certificates that result in the "little lock" icon appearing in the internet user's browser when conducting a purchase. While the presence of the little lock icon may indeed mean that the consumer's credit card information is protected on its way to an illegal online pharmacy, this does not change the alarming fact that the actual act of purchasing prescription medication from illegal online pharmacies is very dangerous, AND legitimate users' credit card credentials find their way to these criminal companies.

Like hosting companies, SSL security vendors generally disclaim any responsibility for the illegal activity they are enabling. A typical phone call to an SSL certificate vendor which requests that the vendor cancel or suspend its service to the illegal pharmacy website will result in the response, "We are not in control of what's on the website; if they meet the criteria for the SSL certificate, we provide it to them". Cyveillance has

anecdotal and documented evidence of this behavior, which is unfortunately the norm even among SSL certificate vendors based in the United States.

It should be noted that a hosting company or SSL certificate vendor may not be aware of the nature of their customers' activity after the services are purchased. Often hosting services and SSL certificates are purchased through largely, if not completely, automated processes and no human may ever review the website where the unlawful activity would be visible. However, once a hosting company or SSL certificate vendor has been made aware of such activity, there is no excuse for the company to continue doing business with the illegal online pharmacy. The situation is even less pardonable because servers which house one form of illegal activity like online pharmacies may also host child pornography or online gambling operations.

Of course, the types of American companies which assist organized crime on the internet are not limited to hosting companies and SSL providers. For example, there are companies which offer online chat services for website visitors to converse with illegal online pharmacy personnel for customer service. Any regulatory and / or legal language to curb this sort of behavior should be written in such a manner to prevent any assistance organized crime may receive online from American companies.

Making Online Criminal Activity More Punishable

Cyveillance employees are not legal experts, but providing services to criminals that enable the commission of a crime would seem to meet the legal definition of what makes an accomplice. This determination would seem even easier to make when these entities are paid for their assistance. However, while morally unjustifiable, today there are virtually no consequences for companies that work with the criminals who sell prescription medications online without a prescription and the behavior of these companies suggest that they feel no pressure to change. While we did focus on illegal online pharmacies here, it is just one example of the bigger problem of American companies turning a blind eye to the illegal activity of their business partners online. We propose that:

1. In addition to federal law enforcement, civic agencies should aggressively pursue punishment for repeated complicity in illegal online activity by American companies. A "three strike rule" may be an adequate model for enforcement.
2. In the same manner that federal and local law enforcement offer "crime solvers hotlines" where citizens can report illegal activity for investigations, there should be a single clearinghouse whereby concerned citizens can report American companies that offer services to illegal activities online to law enforcement for speedy investigation.

Cyveillance understands that the hosting and SSL companies will resist efforts to regulate their activity. However, in the same manner that the Department of Transportation requires safety measures of car manufacturers, in the same way that the Environmental Protection Agency requires safety measures in industrial settings, and in the same way numerous other businesses are regulated to promote social well-being overall, taking measures to protect Americans from danger is not only a noble goal and moral imperative that companies should embrace, but a “low hanging fruit” from a regulatory perspective that will also enhance American cybersecurity. We look forward to further dialogue around what steps may be taken to eliminate cooperation with organized crime online by American companies.