Cyveillance
Minding your business on the Net

Providing Only
100% Relevant
Internet Intelligence

Online Distribution of Counterfeit Pharmaceuticals

A Cyveillance White Paper

Prepared by:
James V. Green and Brian H. Murray
Cyveillance, Inc.

October, 2001

CONTENTS

INTRODUCTION

While the online counterfeit issue poses a serious threat to pharmaceutical companies, best practices are emerging to manage the risk.

Consumers are increasingly replacing a trip to the pharmacy with a more convenient click on the Internet, where they find Web sites offering impressive variety and availability, competitive pricing, and a positive customer experience. In today's highly competitive environment, online pharmacies are attracting new customers by offering convenience and a sense of privacy difficult to achieve at a local pharmacy. For these reasons and more, Forrester Research projects that online prescription sales will grow to 9.2 percent of the market by 2004.[1]

Unfortunately, the Internet is also a burgeoning channel for the distribution of counterfeit drugs. The World Health Organization estimates that seven percent of the world's medicines are forgeries, resulting in revenue losses to the pharmaceutical industry of more than $30 billion annually.[2] Antiquated regulatory and enforcement systems, globalization, and a lack of corporate vigilance have resulted in an online environment where counterfeiting crimes go largely unpunished, all but ensuring that the Internet will comprise a disproportionately large share of industry's losses.

> **"With the introduction of Internet sites selling prescription drugs with almost no regulatory framework, the environment and the incentive for using fake drugs, making fake drugs and selling them directly to consumers is obvious."**
>
> Rep. John Dingell, U.S. House of Representatives, 2000

With the number of consumers purchasing prescription and non-prescription pharmaceuticals online rapidly increasing, the cost of genuine pharmaceuticals rising, and the sophistication of counterfeit production and distribution growing, the availability of counterfeit pharmaceuticals online is poised to skyrocket above the already alarming rates. Government agencies and global organizations such as the International Chamber of Commerce (ICC) have recognized the scale and urgency of the dangers associated with the online distribution of counterfeit pharmaceuticals. While the issue poses a serious threat to the pharmaceutical industry, best practices are emerging to manage the risk.

1 Enos, Lori, U.S. States Target Illegal Online Pharmacies, E-Commerce Times, March 31, 2000.

2 Pasternak, Douglas, Knockoffs on the Pharmacy Shelf: Counterfeit Drugs Are Coming to America, U.S. News & World Report, June 11, 2001.

WHAT'S AT STAKE

The risk to public health is clearly the greatest concern associated with the distribution of counterfeit drugs online, as suspect Web sites circumvent established procedures meant to protect consumers. But even in cases where counterfeit sales do not pose health threats, drug companies can incur significant costs as a result of lost sales and brand dilution. Media coverage of contaminated or counterfeit drugs can substantially undermine public trust and brand image, alienating customers and weakening revenues for years to come.

The sale of counterfeit pharmaceuticals also dilutes the revenue of other businesses in the pharmaceutical value chain and threatens to undermine relationships with legitimate distributors. There is an expectation that manufacturers will proactively maintain the integrity of their distribution channels. If pharmaceutical companies do not exercise reasonable precaution against counterfeiting, they may also expose themselves to liability or even run afoul of the law.

ATTACKING THE PROBLEM

"Increasingly, manufacturers will be required by law enforcement agencies to exercise due diligence in protecting their products from being copied."
Peter Lowe, Assistant Director of the ICC's Counterfeiting Intelligence Bureau

To successfully combat counterfeiting in the 21st century, a company must develop and maintain a comprehensive, multidimensional strategy that includes the Internet as a core component. With billions of pages on the Internet, it can be a daunting task to identify, analyze and prioritize online pharmacies. While the number of e-Commerce Web sites selling drugs online has been reported to be in the thousands, there are other pharmaceutical outlets on the Net that easily raise that number to the tens of thousands. In addition to commercial Web sites, drug-related transactions are routinely made through personal Web pages, auction sites, Usenet newsgroups, Internet relay chat channels, and email.

Given the breadth and complicated nature of the problem, the challenge then becomes identifying the pharmacies and prioritizing efforts to achieve the greatest impact with limited resources. While commercial search engines and manual surfing can uncover a limited number of pharmacies, this approach to identifying sites is both inefficient and ineffective. Proprietary data mining and analysis technologies are commercially available that can be programmed specifically to monitor the Internet for suspect pharmacies.

Last year the U.S. Food and Drug Administration (FDA) devoted over 10,000 staff-hours per month to investigate Internet sites for online distribution of counterfeit pharmaceuticals.[3] As evidenced by the FDA's efforts, once suspected online pharmacies are identified, there remains the considerable task of confirming that the site is engaged in distributing the counterfeit

[3] Dingell, John D., U.S Food and Drug Administration Arguments to the Commerce Committee, U.S. House of Representatives Commerce Committee, February 11, 2000.

Best practices for managing the counterfeit pharmaceutical problem include covert marking systems for unequivocal authentication.

pharmaceuticals. The effort is further complicated by the fact that sites distributing counterfeit products are more apt to employ tactics similar to those used in the porn industry that cast an even broader net and hinder enforcement efforts. For example, single pharmacy sites may lie at the hub of dozens of other re-direct sites or be one of many "mirror" (duplicate) sites. Such networks may be erected specifically to elude authorities or to fool search engines and divert customers.

The good news is that the use of these questionable tactics and the presence of certain content can provide an indication that a site is engaged is suspicious activity. Searching for specific clues that indicate a site is more likely to engage in illicit activity is an effective way to prioritize follow-on investigative efforts. With limited resources, it is wise to target enforcement activities on the most suspicious sites. Some examples of criteria that may signal that a pharmacy is suspect include the following:

- Product offered below cost or at unreasonably low prices
- Sites that are not a registered domain but part of a larger community, such as personal pages hosted by an Internet service provider
- Use of jargon and vernacular that may be reserved to "insiders" in the counterfeit pharmaceutical community
- Sites that utilize overly aggressive capture tactics more common to the porn industry such as re-directing, "typo-piracy", "mirror sites", "mouse-trapping", or "spawning"
- Lack of secure transaction capability or absence of a stated privacy policy
- The presence of advertisements for a "new cure" for a serious disorder, or undocumented claims of "amazing" results
- Sites that are based outside of the country whose customers are targeted by the site
- Presence of misspellings or derivatives of the proper drug name
- Sites that do not provide a domestic address and phone number for customer service, or whose contact information does not match the site registration information
- Sites that prescribe a prescription drug for the first time without a physical exam or that sell a prescription drug without a prescription

Technologies such as those employed by Cyveillance can facilitate the review and prioritization of suspect pharmacies based on these and other criteria. Such an approach is the most efficient and effective way to cover the most ground and flag suspicious sites for further investigative action. An automated solution is also critical to monitoring other online environments, such as Usenet newsgroups, where counterfeit pharmaceuticals are promiscuously promoted and distributed. The more popular pharmaceuticals have dedicated Usenet newsgroups that include hundreds of promotions, links to online pharmacies or personal sites, and purchase information.

To illustrate with a real example, an online pharmacy recently spammed Usenet newsgroups with messages in an attempt to drive traffic to their site. The messages promote "instant purchases with no prescription required" and attempt to prey upon public fear by promoting the availability of drugs to treat Anthrax. Apart from questionable customer acquisition tactics, the pharmacy site would still be considered suspect in that it does not provide contact information other than email, does not have a stated privacy policy, offers low price medications without a prescription, and is registered to an individual operating outside of the country where it is selling pharmaceuticals.

Once the suspect online pharmacy is identified, analyzed, and prioritized, the remaining steps to success are to acquire, test, and validate the product's authenticity. In cases where an agency, association, or pharmaceutical company is ordering from a suspect online pharmacy, it is naturally to the investigator's advantage to use a post office box or other disguised address to reduce the chance the online pharmacy may recognize the investigator.

After a sample of the suspect product is obtained, the authenticity must be tested. In addition to overt protection devices such as holograms and tamper seals, best practices for managing the counterfeit pharmaceutical problem include forensic fingerprinting. A company like Biocode, a leading provider of anti-counterfeiting solutions, can provide the technological expertise and experience necessary to effectively manage covert marking and product authentication. Armed with unequivocal forensic evidence, the manufacturer is ready to take legal action.

CONCLUSION

Identifying, analyzing and prioritizing online pharmacies are substantial undertakings, as evidenced by the number of agencies and level of effort currently engaged in this pursuit. Pharmaceutical companies are exposing themselves to significant risk and placing themselves in a competitive disadvantage if the online counterfeit issue is not addressed with the full capabilities and attention of the organization.

Attacking the online distribution of counterfeit pharmaceuticals is a challenge that can be met by leveraging the capabilities of proprietary technology, including automated data mining and analysis, combined with forensic fingerprinting. Leveraging state-of-the-art commercial tools will assure the highest possible return-on-investment in efforts to eradicate the online distribution of counterfeit pharmaceuticals.

About Cyveillance, Inc.

Cyveillance, Inc. helps companies address critical business issues by delivering 100 Percent Relevant Intelligence™ mined directly from the Internet. Cyveillance's solutions enable businesses to capture revenue by taking control of their brand identity, digital assets and corporate reputation online. Cyveillance configures its proprietary technology with client-specific parameters to locate and categorize unstructured content, transforming the Internet into a critical resource for strategic analysis. Cyveillance's hosted solutions are available in multiple languages and designed to serve its growing list of Global 2000 organizations.

About the Authors

James V. Green, Strategist in the Client Services Department at Cyveillance, Inc., is responsible for managing the delivery of Internet intelligence for pharmaceutical industry clients. Prior to joining Cyveillance, James served as a senior consultant with Booz-Allen & Hamilton's Information Assurance Technology Analysis Center. James earned an M.S. in Technology Management from The University of Maryland and a B.S. in Industrial Engineering from The Georgia Institute of Technology.

Brian H. Murray, Senior Director of Client Services at Cyveillance, Inc., is a leading expert in the rapidly evolving area of Internet intelligence. Brian is responsible for providing strategic direction to the Client Services Department at Cyveillance, including all aspects of customer satisfaction and service delivery operations. Prior to joining Cyveillance, Brian led the launch of an e-Business service offering as a Manager in the Compliance Risk Management Practice at PricewaterhouseCoopers L.L.P. Brian earned an MBA from the Darden School at the University of Virginia, a Masters of Engineering from The Johns Hopkins University and a B.S. from Syracuse University.

Cyveillance®
Minding your business on the Net

For more information, please contact:

Cyveillance, Inc.
Toll Free: 888.243.0097
Tel: 703.351.1000
Fax: 703.312.0536
www.cyveillance.com

UK
Tel: +44 20 7556 7040
Fax: +44 20 7556 7001