THE GREY MARKET - A SHADY BUSINESS

by Krishna M. Singh

INTRODUCTION

The grey market referred to in this presentation is a market that deals in stolen or counterfeit products.

SOME EARLY DEFINITIONS

Stolen goods traded in the grey market range from canned food, cigarettes, apparels, electronic goods and semiconductors.

Counterfeit goods are goods which infringe trademark or copyright rights of legitimate owners. In the trademark infringing category are most branded apparels, perfumes and footwear.

Copyright infringing goods include all kinds of computer software, books, movies and music.

A seller refers to a person who steals goods or makes counterfeit goods which are then sold in the grey market.

A middleman refers to a person who transfers counterfeit or stolen goods from the seller to the buyer. It will be worthwhile to note that there may be many middlemen in a single transaction between a buyer and seller.

PEOPLE INTERESTED IN THE GREY MARKET

There are several groups of people who are keenly interested in the grey market. They are

- Those who steal or rob and sell these stolen goods in the grey market.
  - Those that manufacture or produce counterfeit goods and sell into the grey market.
- Those who want to buy goods in the grey market for better bargains or for more profit when they resell. We will call these people knowledge buyers. They are aware of what they are buying.
- Middlemen who put sellers in touch with buyers or transfer the goods from buyer to seller with a profit.
- Law enforcement agencies.
- Security managers or enforcement officers of companies.

POWER OF THE BUYER

The grey market thrives because there are buyers.

Some buyers are fully aware that they are purchasing stolen or counterfeit goods. Others however, may be unaware of this knowledge.

Without buyers there is no grey market.

SELLING IN THE GREY MARKET

Goods that come into the grey market are brought in either by middlemen or those who commit crime (like robbery).

The grey market is always inhabited by middlemen who are ready to take any kind of stolen goods. They are able to find buyers who want to dispose of their stolen goods. Many of the crimes are committed because of the knowledge that there are ready middlemen who will take the stolen goods for sale at the grey market.

Middlemen have ready buyers whom they contact when a particular type of stolen product is available. Middlemen are constantly looking to expand their markets. Hence they continue to look for new buyers all the time. Sometimes middlemen have confirmed orders for certain goods for which a crime is then committed.

In order to sell the stolen or counterfeit products, middlemen will have to 'advertise' either by word of mouth through reliable contacts, or through some type of media likes the newspapers or even the Internet.

HOW SELLERS IN THE GREY MARKET ARE IDENTIFIED

Grey market sellers can be identified by the following means:

- Visiting known grey market operators
- Acting on information received
- Checking advertisements in newspapers
- Surfing the Internet

THE CYBER GREY MARKET

The Internet has brought about changes, which can be used to our advantage. Now you can search and identify grey markets not only in your own backyard but also worldwide. Seamless borders move products very quickly from location of crime to location of demand within 24 hours.

Grey market products are now advertised on the Internet. In some instances suspected products can be easily identified as counterfeit or stolen either through pricing or through

other clues posted on the Internet. Steps are then made to bring the seller into the open and work from there.

It is not uncommon for grey market operators to sell only via the Internet. In such cases the seller may not be visible at all because payments are transacted over the net and the product is delivered right to the buyer's doorstep. Buyer and seller never meet.

In most cases, however, sellers look for buyers only after the stolen or counterfeit products come into their hands. The seller, in such situations, cannot remain completely invisible

International connections and seamless borders have also made it possible for grey market operators to be in one country and the goods to be sold in another country altogether. In such instances, once payment has been made, the grey market operator will advise the 'goods custodian' to deliver the goods to the buyer.

IDENTIFYING CYBER GREY MARKETS

Identifying cyber grey markets requires diligence and consistency. You have to constantly surf the Internet for potential sellers of any product that interests you. Some organizations even have a full time staff just surfing the Internet for such products on sale.

It is actually quite easy to identify products on the Internet as being either counterfeit or stolen. Most of the sites will provide a pricelist of their products. These prices are normally a giveaway as the advertised product may sell below the cost price of the original product.

Where a potential site is identified as trading in stolen or counterfeit goods but some doubts exist, you can always seek clarification or information by emailing the seller and asking relevant questions. Almost all sites have email contact addresses.

POTENTIAL APPROACH METHODS

Once you have confirmed that a particular site is dealing in stolen goods, you will have to work out potential approach methods. Methods vary according to country and product. Generally, though, here's what you can do:

Create a Pretext Identification Centre

This identification centre must be at a place where sellers know that the requested for, is in demand. This is crucial. Your plan will fail if the location is improperly identified.

For example, if a potential "buyer" located in Singapore, Malaysia or Thailand wants to buy 'cheap' software from a seller in Europe or the US, an experienced seller will

immediately smell the rat. This is because these sellers know that cheap software is obtainable only from this part of the world.

With regards to divulging personal identification, this depends upon circumstances.

If you are tracking a seller who operates from your own country, you may use fictitious identification.

If, however, the seller is in another country, you may have to use legitimate identification. This is because in the event that you personally have to travel to meet them, you will have to travel on your own passport and register in hotels under your real name.

Whatever identification you choose to use, remember that it must allow the seller to make contact with you through the telephone, fax, or at least by email.

Make Enquiries

Through the use of the Internet, you can get yourself on many sellers' mailing lists. You will be surprised at the range of items available on the Internet, and the ease with which the sellers will provide you with pictures and full details of the products.

If a seller is a potential target, you may have to make purchases once in a while to keep him interested in you.

You can also gain his/her confidence by recommending other buyers on the Internet who may be interested in his products.

Work With Law Enforcement

Sting operations are a common strategy adopted by several law enforcement agencies to trap grey market sellers. This is an operation where a front is set up to buy stolen or counterfeit goods. The operation may last for months before the final swoop is made.

If you want to set up a sting operation in order to build a case, you will first have to identify the supply source. To do this, you will have to work with your local law enforcement agency so that a prosecution can follow after a successful sting operation.

To ensure your sting operation is a success, you can request for the grey market products to be shipped to a location where the law enforcement agency is more amenable to prosecution.

CONDUCTING AN ONLINE STING OPERATION

Now let's look at the steps you need to take to carry out a successful sting operation on the Internet.

1. Set up Operation Base

For an online base, you will need to have Internet access and an e-mail address.

Email

You should have a minimum of two e-mail addresses. The first one can be derived from a source in your host country or state, and the second can come from any number of free alternatives such as Yahoo.

The free ones are the best ones to use for fictitious identification as these sites have no way of identifying you other than from the information which you provide when you register.

For example: You live in Singapore and log on to Yahoo with your current internet subscriber. You then go to 'mail' and register for an e-mail address. When you are asked for your contact details and company name, you can provide any fictitious information you desire, i.e. you can say that your company is located in Hong Kong or California USA.

Be sure to use addresses and telephone numbers that would be used in those locations, although they do not have to be correct as no one actually verifies them.

From that time on, you can search the Internet and anyone you want to communicate with can be given these surreptitious contacts. You merely have to go to that Yahoo e-mail address periodically to see if you have received any mail. At the point in time when you want to make direct contact, you can refer them to your associate, (this would be yourself at your regular e-mail in your host country).

Mobile Phones

Mobile phones also come in handy. If you want it to be known that you or your business is in, for example, India, you can subscribe to any one of the Indian phone companies. Auto roam will connect you to wherever you are and make the seller believe that you are in India.

2. Surf the Internet

Once you have all this in place, you are ready to go surfing for the bad guys. There are hundreds of Business to Business (B2B) boards on the Internet that connect buyers and sellers. Many of them are global in nature while some are country specific or region specific. Most of them have categories for the products offered and wanted, which will make your search much easier.

The primary concern you must have when soliciting information from these locations is that in most cases you must register on the website to access the buyers' and sellers'

contact details. Whatever details you provide when registering will usually be provided to the buyer or seller when you attempt to contact them. Once you have registered, you should send a draft enquiry email to yourself to read how convincing your email to the potential sellers sounds.

3. Make Enquiries

Now that you have all this done, you can start making specific enquiries for whatever products you wish to find. There are some important rules you should follow when doing this.

a. Always start with a ruse that you can justify in the event you start communicating directly with a seller of counterfeits.

You should keep you story simple and allow for change whenever possible. Also let them think you are (or want to be) a wholesaler which allows for the flexibility of not having shops or specific locations they can check on.

b. Do not ask for specific counterfeit items unless they are offered by the subject of your enquiries.

For example, if you want counterfeit Microsoft products, ask for software in general first and see if they offer the Microsoft to you. Once you have determined what they will sell, you can be more specific.

c. Do not profess to be an expert on the products you are attempting to purchase unless you have the knowledge to deal with communication on that level.

What you should say is that you have a potential buyer for certain products and are attempting to locate these products for this buyer. So, in the event that you are asked questions about the product that you cannot answer, you can always buy time by saying you will revert to your 'buyer' for feedback and confirmation.

If you are not knowledgeable about the products, you can ask specific questions of the seller that were purportedly requested by your buyer. This will save you from having to respond immediately with details you may not know.

d. Be prepared to purchase and accept samples from the seller.

Most sellers will require you to pay for the samples and shipping costs. You should be connected to any number of payment programs such as Pay pal which allows you to pay by e-mail through your Pay pal account (www.paypal.com). You can also request for their banking information so that you can wire the funds to them. This is accepted procedure.

A note of caution - do not pay by credit card as you are dealing with criminals who may use the information you provide, for their illegal benefit.

You should have a location available at which to receive the samples. If you wish to have your location remain anonymous, you can use a postal mailbox service which will accept parcels on your behalf.

SOME DIFFICULTIES

The Faceless Seller

Sellers in the grey market do take some precautions to remain unidentified. Transactions on the internet can be completed without the buyer and seller ever meeting each other. This would not be helpful in a sting operation. However, such a transaction will not totally valueless as some amount of information can be developed about the seller and this could take you to the next level of the operation.

Mistaken Identity

There are genuine sellers on the Internet who ply goods, mostly apparels, cheaply as they are over-runs, old stock or cancelled orders. Some grey market sellers will also put out counterfeit or stolen products for sale claiming them to be over-runs, old stock or cancelled orders. This can create some difficulty and you would have to clearly ascertain if the goods are genuine or not before making your move.

CONCLUSION

The grey market in the cyber world has brought about new challenges for law enforcement officers and private investigators involved in such work. It will be no surprise that in time to come the bulk of dealings of stolen products will be done in the cyber world. The grey market operates see a lot of benefits in dealing from the cyber world – greater reach to the client base and less risk of detection. We have to rise to the challenge.

About the Author

Mr. Krishna M Singh has 16 years experience with the Singapore Police Force during which he also attended training at the FBI National Academy, Quantico, Virginia, USA. In 1980 he took up the position of Security Manager in National Semiconductor Asia Pacific for the next 10 years. Since 1989 he was hired as an investigator to several security companies and subsequently turned himself as consultant to several multinationals. Today he runs his own consulting company.

He is an accomplished speaker with extensive knowledge, networking and experience in grey market investigation.

(This paper was presented at the 2 nd Security Practitioners' Meet on 28-29 October 2002 at the Cititel Hotel, Mid Valley, Kuala Lumpur, Malaysia).