MessageLabs®

Be certain

WHITE PAPER

The Online Shadow Economy:
A Billion Dollar Market For Malware Authors

Maksym Schipka, Senior Architect of Development

Introduction

Malware, meaning computer viruses, trojans and spyware, is about money. The teenagers who wrote viruses have grown up and now they're trying to make money. The shadow Internet economy is worth over $105 billion. Online crime is bigger than the global drugs trade. There is a sophisticated online black market with tens of thousands of participants. Collectively, online criminals are using the techniques of the free market to subvert and corrupt legitimate online business.

Dot.com entrepreneurs of crime

Maksym Schipka, Senior Architect at MessageLabs, has been spending a lot of time exploring this criminal underworld. He has been looking at Russian websites, chat forums and exchanges because he understands the language and because they are the most active. However, there are similar online markets in other countries. In the shadow economy, people boast of making $10,000 a day and while this may be bravado, people are making good money in the shadow economy. With little chance of being caught and so much money at stake, it is little wonder that "a huge number of people are involved," according to Schipka.

Division of labor

The big surprise is the level of specialization and the sophistication of the market. Picture a mall: some shops sell clothes, some sell food, others sell books and so on. Each shop is specialized and dedicated to one type of product. For each type of product, there are several shops competing to offer better prices and better service. This is what the shadow economy is like.

Let's look at one online crime and see how it breaks down into a series of specialized trades. First, malware writers create new viruses, spyware, and trojans to infect computers. For as little as $250 you can buy a custom written malware and for an extra $25 a month you can subscribe to updates that will ensure your malware evades detection. The vast majority of malware authors do not distribute it themselves. In fact, they make great play of offering their software "for educational purposes only" in the hope that this offers some immunity from prosecution.

A malware middleman buys malware from a programmer and uses the services of a botnet owner to spread it. A botnet is a remotely-controlled network of computers that have been infected by a virus. Typically, they are poorly protected computers belonging to innocent people around the world. You may have a bot running on your PC now and not know it. These computers give botnet owners the computing horsepower and network connectivity to spam out millions of emails or send out hundreds of thousands of trojan attacks or host a malicious website. Once the malware has spread, the middleman can sit back and start to collect stolen information and identities.

The middleman sells the stolen identities to make money. A full identity sells for around $5. This includes full name and address, a passport or driving licence scan, credit card numbers and bank account details. Credit card numbers sell for 2-5% of the remaining credit balance on the cards in question. Identity thieves offer their customers a high level of service. For example, you can buy identities sorted by country, industry, role; and credit cards sorted by remaining balance.

There is another category of middleman who specializes in turning stolen credit card identities into cash. He will buy credit card information and then use a "drop service." A drop is someone who receives goods purchased with a stolen credit card. Some are criminal fences; others are unwitting dupes doing it for cash. A middleman buys goods from online shops – typically cameras and portable computers – and then ships them to drops. The drops, in turn, post them on or sell them immediately for cash. This is how a stolen credit card is laundered.

Scammers scammed

They say there's no honor among thieves. This is also true of the shadow economy. Fraud and rip-offs are so common that a system of guarantors and escrow accounts has emerged. For example, a drop service provider might offer a guarantee to an identity thief that they will be paid their cut of the sale of any goods, even if individual fences don't pay up.

Similarly, guarantors will provide an escrow service. For example, a buyer will transfer payment to the guarantor and the seller will transmit the virus code or the credit card numbers. If the goods

There is a sophisticated online black market with tens of thousands of participants. Malware authors can produce new, unique malware every 45 seconds in order to keep it undetected.

check out the funds are released. Typically, these guarantors take 2-3% of the transaction value for their services. The emergence of these services shows a developing sophistication in the market, driven by economics more than technology or the demands of organized crime. It also shows there are participants who value their long-term reputation. These are worrying signs.

Continuous improvement

Another sign of growing sophistication is the continuous improvement in the quality of products on sale in the shadow economy. Malware writers work hard to test their products against anti-virus software. They offer guarantees that a given virus or trojan will not be detected using current anti-virus programs. If vendors update their software, then the malware author will supply a new version.

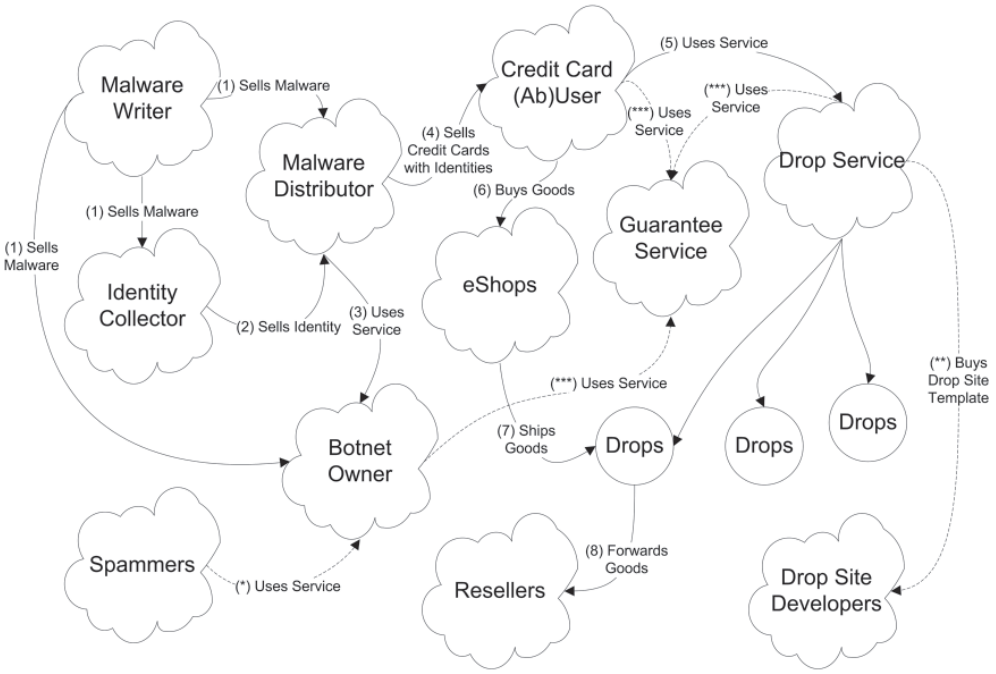
Conventional anti-virus programs rely on "signatures" to detect malware. A signature is similar to a DNA fragment that identifies the virus and separates it from legitimate data. Anti-virus programs scan email attachments and other files to check that they contain no known signatures. As new malware comes to light, anti-virus vendors issue signature updates. However, they can only find a new signature after a new virus is in the wild and is released on the Internet. Worse, malware authors can also download the signatures and test their creations against the latest updates. Schipka's research suggests that malware authors can produce new, unique malware every 45 seconds in order to keep it undetected.

This is where the MessageLabs service is so valuable. As malware developers get more sophisticated, they find it easier to stay one step ahead of signature-based detection. MessageLabs uses signatures, but also has a second line of defense: its proprietary Skeptic™ engine. This heuristic scanner can detect malware without signatures. Moreover, the bad guys can't buy it and use it to test their malware. The only people who have access to Skeptic are MessageLabs and the only people who benefit from it are MessageLabs customers. Ultimately, says Schipka, "The only thing you can rely on is very good, well-managed heuristic detection."

The free market and the future of online crime

The shadow economy has all the attributes of a traditional economy – division of labor, price competition, marketing and so on – accelerated to Internet speed and carried out online. Adam Smith, the pioneering political economist, in his Wealth of Nations, foresaw that the division of labor could increase productivity and quality. Similarly, competition drives down prices and tends to drive innovation. While it is interesting to observe these classical economic principles at work, they hold a terrible warning: malware is going to get more common and more virulent. Companies that rely on the Internet and email, need the best protection they can get.

Division of labor in the shadow economy




MessageLabs®

Americas
AMERICAS HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA
T +1 952 830 1000
F +1 952 831 8118

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong
T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 14
90 Arthur Street
North Sydney
NSW 2060
Australia
T +61 2 9409 4360
F +61 2 9955 5458

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712
T +65 6232 2855
F +65 6232 2300

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
1 Great Portland Street
London, W1W 8PZ
United Kingdom
T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands
T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Culliganlaan 1B
B-1831 Diegem
Belgium
T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
Feringastraße 9
85774 Unterföhring
Munich
Germany
T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

www.messagelabs.com
info@messagelabs.com