CHAPTER TWO

Characteristics of the Black Market

Black markets emerged as it became increasingly obvious that a lot of money could be made for relatively low investment. The growth of the Internet allowed like-minded individuals to find each other and connect more easily, providing easier access to tools and weapons, as well as to more targets. Barriers to entry were low for those with appropriate access and vetting. The risk was also low (compared with other criminal markets), at least initially, because law enforcement was ill equipped to track it (although they are increasingly getting more effective). The slow adaptation of law to the demands of cyberspace has made for a difficult (and often slow) fight for law enforcement.[1]

The black market is not so much a market as it is a collection of activities that range from simple to extremely sophisticated and operate all over the world, from New Jersey to Nigeria to China and Southeast Asia. Goods and services tend to be reliable (though not always), and implementation and transactions are quick and efficient. These markets are compared by some to underground markets for other illicit goods, such as drugs, with the difference that digital goods carry less risk and can offer greater profit.

When we say *market(s)*, we mean the collection of (skilled and unskilled) suppliers, vendors, potential buyers, and intermediaries for goods or services surrounding digitally based crimes.[2] A *marketplace* is the location in which a market operates—in our case, it is typically virtual or digital.

It is challenging to describe what the entire market looks like. It is too vast, has too many players, is too disjointed, is constantly changing, and, because it is a criminal market, pains are taken to prevent law enforcement from understanding it. People often only have a good handle on their own niche, geography, or product. The remainder of this section delves into the various components of the black market (structure, participants, operating conduits, products, pricing) and provides some commentary on the market's reliability and integrity, sensitivity to external events, and resilience to takedowns. We will paint as encompassing a picture as possible, given the scarcity of available details.

[1] Take, for example, the case of sentencing a high-ranking member of CarderPlanet—almost a decade after his arrest (Farivar, 2013).

[2] A few of these crimes include financial (e.g., account compromise, account credentials, credit card data), nonfinancial (e.g., credentials for eCommerce, social media, gaming), intellectual property (IP) theft, counterfeit goods, defamation, or takedown of sites.

Structure

Hacker markets have evolved over time and now come in many forms. In the early to mid-2000s, they focused on goods and services surrounding credit card data. Then, they expanded to broker credentials for eCommerce accounts, social media, and beyond. These days, some are still dedicated to one product or a specialized service, while others offer a range of goods and services for a full lifecycle of an attack; some are "storefronts" that offer many products but not complete one-stop shopping. Some vendors advertise on multiple marketplaces; others stick to just a few online forums. Even within single forums or stores, there are different tiers of access for various products. Some underground organizations can reportedly reach 70,000–80,000 people, with a global footprint that brings in hundreds of millions of dollars (e.g., carder.su, a now-defunct forum that was dedicated to all aspects of credit card fraud). These marketplaces—particularly the harder-to-access tiers where participants are highly vetted—are often well structured and policed, with their own constitution-like rules and guidelines to follow. That said, plenty of the market does not have rules and regulations—one reason experts say the black market can outpace the legitimate world.

Criminals of multiple skill levels can participate in the black market because targets vary in their hardness (as far as stealing data is concerned, some say individuals tend to be softer or easier targets than organizations). Most players go after any exploitable device, employing "smash-and-grab" techniques, using goods acquired in the more easily accessible channels. Fewer players are good enough to target specific systems, companies, or victims.[3] These more sophisticated, more focused attackers require access to higher tiers or to in-house research and development (R&D) for the most advanced tools and expertise. Those who would carry out targeted attacks may explore peer-to-peer solicitations rather than the more open public forums or chat channels to acquire their desired goods and services. But players of various skill levels often support one another. For example, highly skilled players, through a breach, may capture IP along with data or account credentials. They may then sell the IP to those who deal in corporate espionage, and the data and credentials to other, potentially less-skilled individuals for further exploitation and sale.

But almost any computer-literate person can enter the market. With the increase of as-a-service models and do-it-yourself kits (with easy-to-use administration panels), anyone can create and use variants of similar malware. One can buy credentials, credit cards, and personally identifiable information (PII) without needing to be highly technical. This is increasingly true for those involved in identity theft.

One expert estimates that in the mid-2000s, approximately 80 percent of black-market participants were freelance (the rest being part of criminal organizations or groups), but has declined and is closer to 20 percent today.[4] These freelancers span markets and tiers of varying access. But while an individual is good at one thing, organizations (or well-coordinated

[3] One expert suggested that true targeted attacks are about 5 percent of the market, and the remaining 95 percent are consumer-grade. Although this breakdown has been consistent through time, the whole market is growing exponentially.

[4] Another estimate breaks down the market thusly:

- 70 percent individuals or small groups
- 20 percent criminal organizations
- 5 percent cyberterrorists
- 4 percent state-sponsored players
- 1 percent hacktivists ("pseudo cyberarmies," not Anonymous)

groups of individuals) can combine many different skill sets to accomplish bigger goals with bigger returns. Thus, there has been a tendency for these organizations to grow, as individuals coalesce into bigger groups over time, albeit with exceptions.

Participants

Consistent with traditional economies, the underground market comprises sellers (supply), buyers (demand), and intermediaries (Ramzan, 2013). Buyers take many forms: individuals, criminal organizations, commercial vendors. Intermediaries can act as a third party to verify and validate both products and participants; they can facilitate transactions and safeguard identities by acting as a middleman or a fence. Participants also occupy different levels in the hierarchy of the marketplace, and those at the higher levels typically receive higher compensation. Moving up into the higher and harder-to-access tiers of the market requires extensive vetting that can hinge on personal relationships.

Within these markets, there are often hierarchies and specialized roles: *administrators* sit at the top, followed by *subject-matter experts* who have sophisticated knowledge of particular areas (e.g., root kit creators, data traffickers, cryptanalysts, those who vet). Next are *intermediaries*, *brokers*, and *vendors*, and then the *general membership*. Each member can have a subsidiary cell of associated members.

Ultimately, there needs to be a cash-out. This is where *mules* and virtual money mule services come into play. They are the ones who use multiple ways to turn the stolen credit card or eCommerce accounts into usable money: e.g., completing wire transfers, shipping goods overseas bought with stolen funds. Mules can be witting participants (well-informed and organized operations), or unwitting (naïve individuals duped into involvement).

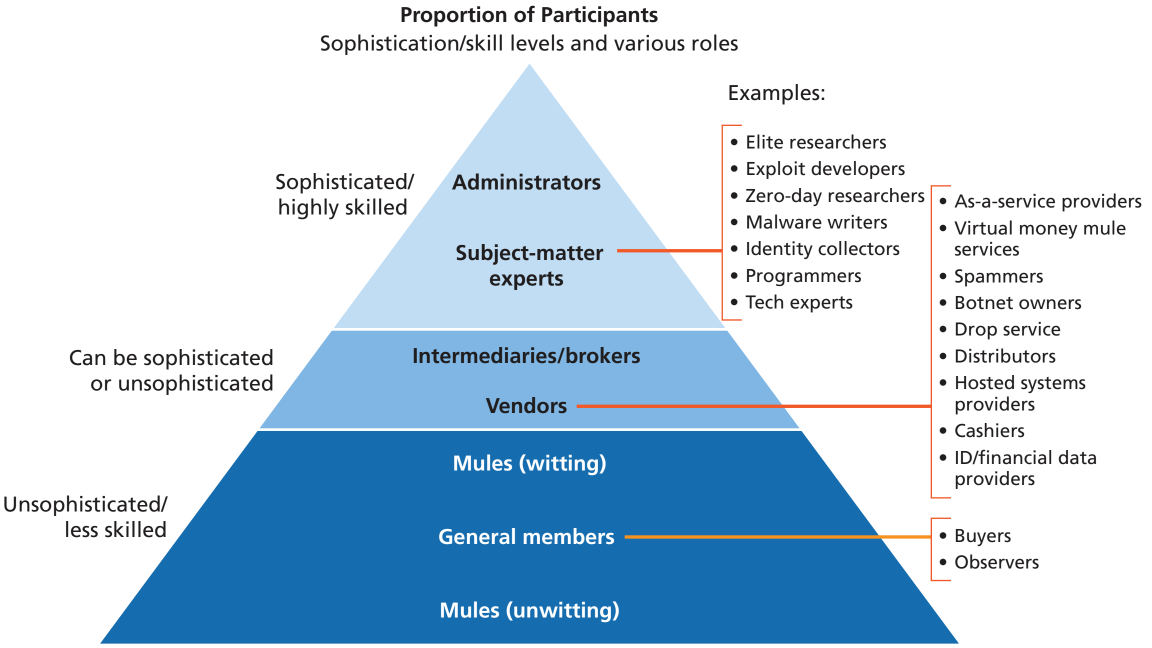
How well players fare depends on their role in the hierarchy, what they sell, their reputation, and their skill level. There is little consensus on which of these factors makes the biggest difference. In general, those higher up in the hierarchy (especially of the card and data rings) are the best rewarded. Similarly, the closer one is to the cash, the more money can be made. One expert noted that witting mules are the “linchpin” of the system, as they tend to be closest to turning “the take” of an attack into actual disbursements of money. Thus, participating as a mule can be lucrative.

Figure 2.1 depicts the different participant levels in the underground market, proportionally. It also shows the sophistication and skill levels, and gives examples of various roles.

No one knows (or is willing to hazard a guess) how many people participate in this market. Similarly, few want to estimate how large the market is, although the general feeling is that it is large, and one expert noted that it generates billions of dollars, at the least.

The number of people participating in the market is likely to increase because it is easier to get involved than it was ten years ago. This is due to the greater proliferation of websites, forums, and chat channels where goods can be bought and sold. An increase in the number of YouTube videos and Google guides for “how to use exploit kit X” or “where to buy credit cards” also facilitates entry into the lower tiers, especially for those who wish to be buyers. Sophistication will continue to rise: Wherever there is a necessity to exploit data (whether it be financial, IP, or something else) there will be highly skilled individuals selling their services. As a result, it is believed that the number of participants, particularly highly skilled ones, has risen sharply

Figure 2.1
Different Levels of Participants in the Underground Market



SOURCES: Drawn from interviews; Schipka, 2007; Panda Security, 2011; Fortinet, 2012; BullGuard, undated.
NOTE: Almost any participant can be a ripper; see text for discussion.
RAND *RR610-2.1*

in recent years, along with the variety of services offered. The level of difficulty and skill also depends on the target: In general, consumers are an easier target than organizations.

As is the case in any market, success for sellers often requires differentiating their product from others. Those who wish to sell hard-to-get, nonfungible goods often require that transactions be done in secrecy, with "double blind" auctions and the use of multiple layers to evade law enforcement.

Although there is a lower barrier to entry for the easier-to-access tiers, getting to the top tier and involved in high-level, sophisticated crimes still requires personal connections and a good reputation, especially for being trustworthy. In the words of an expert who has spent a considerable amount of time in the digital underground, "once you are able to establish yourself, it can be lucrative." Additionally, it can be a badge of honor to survive a purge.

Participants in black markets come from all over the world. Originally, key participants in such markets were former state employees of Eastern European countries who had training and education but were out of work when the Berlin Wall fell (Glenny, 2013). Since then, the sophistication of participants in the black market has soared with the entry of a generation of "digital natives" who have grown up more skilled and can do more things for themselves (i.e., they do not have to hire someone else to reverse-engineer programs or to create an exploit).

In terms of quantity, the leaders in malware attacks are China, Latin America, and Eastern Europe; Russia leads in terms of quality (de Carbonnel, 2013). Different groups operate in distinct spaces. For example, there are Vietnamese groups that mainly focus on eCommerce, whereas a majority of Russians, Romanians, Lithuanians, Ukrainians, and other Eastern Europeans mainly focus on attacking financial institutions. Chinese hackers are believed to focus more on IP.[5] Recently, some groups have partnered across international lines; one expert commented that, "groups that would traditionally never work together are working together."[6] Of late, there has been a migration toward U.S.-based actors becoming more involved; in 2013, almost a fifth of the market was made up of U.S. participants.[7] Many U.S. participants are thought to be involved in financial crime (rather than IP theft).

Business Conduits

Markets must have channels to communicate and conduct business transactions. Not surprisingly, the channels for cybercrime transactions are virtual ones. Channels initially were largely a combination of bulletin-board-style web forums, email, and instant-messaging platforms that support both private messaging or open chat rooms (e.g., some common types include Internet Relay Chat [IRC] Protocol, ICQ, Jabber, and QQ), and email. While these channels are still used today, today's participants also commonly frequent online stores where buyers can chose their desired product, pay with digital currency, and receive the goods without any interaction or negotiation with the seller. This move to mirror legitimate eCommerce storefronts indicates a growing maturity of how business is conducted. It is widely agreed that actors have gotten more sophisticated and innovative in the last four to five years regarding how they interact within these channels—making them more anonymous, encrypted, and hidden. For instance, ICQ chats have been replaced by participants hosting their own servers, sharing email accounts where content is exchanged by saving draft messages, and using off-the-record messaging, the encryption scheme GNU Privacy Guard (GPG), private Twitter accounts, and anonymizing networks such as Tor, Invisible Internet Project (I2P), and Freenet.

Participants frequently alter their communication tactics hoping to stymie law enforcement. More sophisticated participants tend to use cutting-edge tools and technologies more than others. Normally, though, they follow trends. Tor, for example, is a trend, albeit an older one.[8]

Opinions vary on where most transactions take place (it varies with product, participant, or marketplace) as well as where the most valuable interactions take place.[9] Some channels are easy to find; others are by invitation and only accessible after a great deal of vetting. In some forums, members can receive more access and privileges through participating in discussions or contributing tutorials (Paget, 2010). The forums host advertisements, but actual transactions generally take place using encrypted and private messaging, locked-down social media

[5] Note that many other countries are included in the black market; only a few are mentioned here.

[6] For example, one Vietnamese group partnered with Nigerians on a fraud scheme involving stolen eCommerce accounts. In another case, Colombians set up money-laundering "villages" in China.

[7] In the 2006–2007 timeframe, the majority of participants were from Russia, with the United States only a small representation. In 2013, almost a fifth of the market was U.S.-based, ranked third behind Ukraine and Romania.

[8] Here is one case where, in our interview, an expert did not want to describe a newer trend, for fear of tipping the hand of security vendors or law enforcement investigations.

[9] Some see forums "like a Craigslist—no one knows anything; it is just a bunch of idiots talking," where goods that exist in the forums are those that have already been harvested and are just the leftovers. Others say the tools are available in the more restricted, highly vetted forums, whereas data are more publicly available.

accounts, or shared email. The evolution of accessing and interacting with the channels has been dictated by available technology. Before the appearance of the iPhone, there was very little proliferation of mobile platforms and devices with which communications and transactions could be completed anywhere, anytime. The progression of communications tools has grown with the proliferation of technology, and it will continue to be this way.

Channels and tiers are correlated. The black market has several tiers of access, with the higher tiers requiring lots of vetting before they can be entered, or even revealed. Conversely, the lowest tier (often the IRC channels) are considered easy to find, as many are publicly available and open to anyone; rippers (i.e., fraudsters) tend to frequent them, for instance. Markets in the next tier up (considered lower-tier forums) are a little harder to find and often require vetting before entry.[10] Some exclusive forums start as smaller groups where people can cut their teeth and work their way up into the bigger ones. Often, this lower tier exists in such channels as ICQ, Jabber, QQ, et al.[11] The tiers that require less vetting tend to have more financial and counterfeit goods available than sophisticated malware or exploit kits, which are found in upper tiers.

Because the black market is meant to be hidden, it is difficult to get an estimate for the breakdown of market by tier. One expert puts 10–20 percent of the participants in the highly vetted tiers, and 80–90 percent in the lower, easier-to-find tiers. Of all these players in all of the tiers, an estimate is that only a quarter can be considered highly skilled. Others maintain that there are too many variables—freelancers versus organized groups, varying types of threat actors, etc.—to make a reasonable breakdown.

Figure 2.2 shows a rough estimation of the various communications and transaction channels used by participants, for each access tier. Note that these are relative numbers and only estimates.

Language

Although English is the universal language of commerce, it is not necessarily the universal language of this commerce. Some say very little is done in English; sometimes there are English translations to supplement Russian posts, but the forums are generally in Russian or Ukrainian. There are reports of English-only, Mandarin-only, German-only, and Vietnamese-only sites, among others. Nevertheless, phishing, spear-phishing, and other social engineer campaigns are typically done in English, as a majority of potential victims know that language.

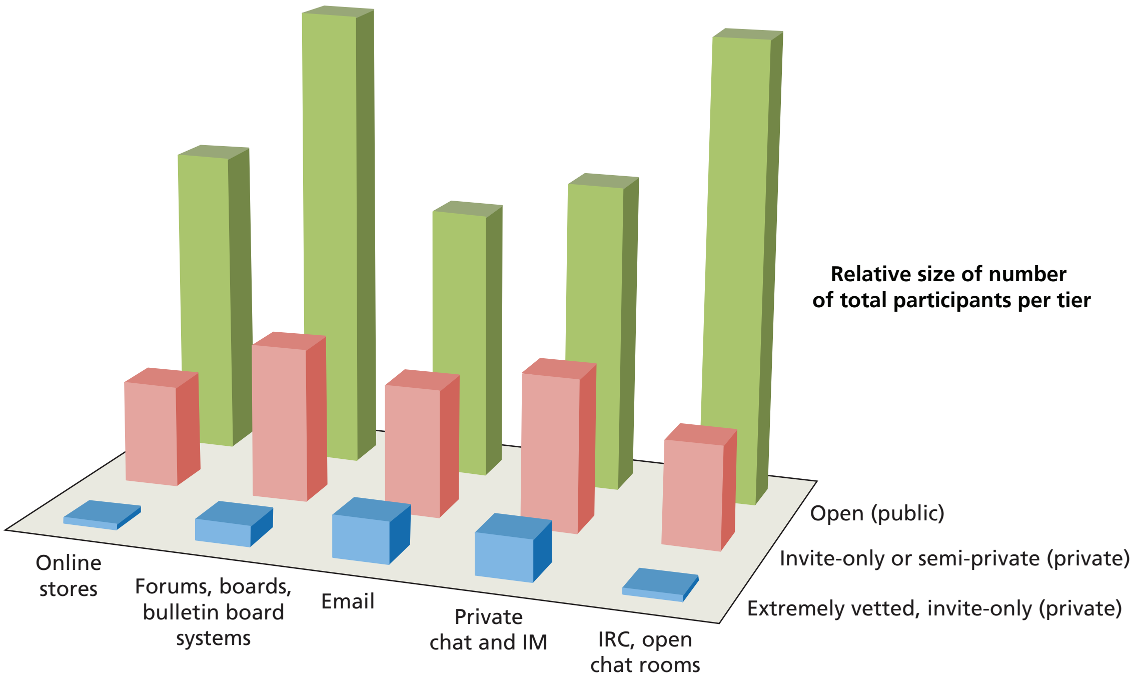
Products

The product slate is quite diverse. Products include both goods (hacking tools, digital assets) and services (as-a-service hacking, digital asset handling). Hacking goods consist of tools that help gain initial access on a target, parts and features to package within a payload, and payloads to have an intended effect on a target. Hacking services consist of enabling services to help scale or deliver a payload, and full-service capabilities that can provide a full-attack lifecycle. There are other goods and services that provide support and ensure the hacking

[10] Some differentiate IRC from next-tier channels, but not all. Take, for example, Herley and Florêncio (2009a) and Fossi et al. (2008).

[11] For example, Fossi et al. (2008), and Gu (2013).

Figure 2.2
Estimate of Various Channels and Tiers Used by Participants



RAND *RR610-2.2*

goods and services function properly and are free from obstacles. These include infrastructure and cryptanalytic services, among others. Digital assets are the output from the successful hacking or hacking services (e.g., financial information, data records, accounts, IP). Digital asset–dealing includes cyberlaundering and facilitating the turning of stolen goods into money.

Table 2.1 describes the main categories of products available.

Although as-a-service offerings have been around for a while, they continue to grow in popularity as new products and technologies burgeon. For instance in 2004, as-a-service models were mainly used for adware and spyware when affiliate business models were coming into play. By 2008–2009, DDoS as-a-service became popular. The market demands more specialized, user-friendly, as-a-service models with easy-to-use interfaces, allowing more participants, regardless of technical ability, to enter the market and get involved—they simply pay for installation and have a service do the work.

Goods and service offerings are becoming much more creative (often cited as a result of the increase of tech-savvy digital natives who participate), limited only by the requirement that buyers for such offerings exist. Products have also become quieter and stealthier. Popular spyware and adware circa 2004, for instance, generated plenty of revenue, but were noisy, and garnered a lot of attention from the security industry. 2009 saw a rise in fake antivirus software, fraudware, and fakeware to steal data and credentials from machines.

Vendors often guarantee their products' lifespan or value—for example, guaranteeing a particular malware variant is good for ten hours before detection by antivirus products, or that a credit card is good for a certain amount of money—and some can track what a customer does with their product to make sure "terms of use" are not broken—a sort of "digital rights

Table 2.1
Goods and Services on the Black Market

Category	Definition	Examples
Initial Access Tools	Enable a user to perform arbitrary operations on a machine, then deliver payloads; can automate the exploitation of client-side vulnerabilities (Zeltser, 2010)	• Exploit kit (hosted or as-a-service) • Zero-day vulnerabilities (and weaponized exploits)
Payload Parts and Features	Goods and/or services that create, package, or enhance payloads to gain a foothold into a system	• Packers • Crypters • Binders • Obfuscation / evasion
Payloads	Imparts malicious behavior, including destruction, denial, degradation, deception, disruption, or data exfiltration	• Botnet for sale
Enabling Services	Assist a user in finding targets or driving targets to a desired destination to use an initial access tool and/or payload; attack vectors and scaling methods	• Search engine optimization services • Spam services • Pay-per-install and affiliates • Phishing and spear-phishing services • Services to drive / find traffic • Fake website design and development
Full Services (as-a-service)	Package together initial access tools, payloads, and payload parts and features to conduct attacks on a customer's behalf; can provide the full attack lifecycle	• Hackers for hire • Botnets for rent • Doxing • DDoS as a service
Enabling and Operations Support Products	Ensure that initial access tools and hacking services (enabling or full-service) will work as needed, are set up correctly, and can overcome "speed bumps" or obstacles	• Infrastructure (e.g., leasing services, virtual private network [VPN] services, bulletproof hosting, compromised sites and hosts) • Cryptanalytic services (e.g., password cracking, password hash cracking) • CAPTCHA breaking
Digital Assets	Digital assets are those items obtained from the target or victim (i.e., the hacked or stolen information)	• Credit card information (e.g., fullz, dumps, card verification value) • Account information (e.g., eCommerce, social media, banking) • Email login and passwords • Online payment service accounts • Credentials • PII/protected health information (PHI)
Digital Asset Commerce and Cyber Laundering	Digital asset commerce and cyber laundering, where appropriate, facilitate turning digital assets into cash	• Mule Services • Counterfeit goods and services (e.g., fake documents, identification, currency) • Card cloners, fake ATMs • Credit card processor services • Forwarding products services

management."[12] For example, a vendor might label and track each install sold, with the ability to shut down anyone who is making too much noise by infecting too many victim machines.

Malware for mobile devices has been growing of late, in part because attacking mobile devices brings in money faster than attacking personal computers. SMS (Short Message Service) Trojans and Fake Installers are the most popular form of mobile malware: They accounted for more than 70 percent of mobile malware as of March 2013, up from 56 percent in 2011 (Juniper, 2013). Such malware does not require extensive customization.

Some see a shift from opportunistic attacks to targeted attacks, and an increase in nonfungible goods (source code, IP, specific target data or credentials, etc.), while others maintain that opportunistic attacks will continue to be strong.

Finally, business models and financial innovation have grown more sophisticated. For instance, buyers can purchase stripped-down versions of a particular software or tool, or get access to goods for free; if they are happy with the product, they can pay more and upgrade to full versions—called "freemium pricing."

Pricing

The black market can be more profitable than the illegal drug trade: Links to end-users are more direct, and because worldwide distribution is accomplished electronically, the requirements are negligible. This is because a majority of players, goods, and services are online-based and can be accessed, harnessed, or controlled remotely, instantaneously. "Shipping" digital goods may only require an email or download, or a username and password to a locked site. This enables greater profitability.

According to experts, black markets operate the same ways traditional markets do. Easily exchanged goods, such as PII or account data, are prey to the normal microeconomic fluctuations of supply and demand. Often, there is too much of that product available to sell at normal prices. By contrast, stolen-to-order, nonfungible goods—such as new technology designs, details on R&D activities, mergers and acquisitions—can command a very high price, provided that the right buyer exists.

The yield of a product influences its price. A Twitter account costs more to purchase than a stolen credit card because the former's account credentials potentially have a greater yield. Immediately after a large breach, freshly acquired credit cards command a higher price—as there is greater possibility for the credit cards to still be active. But after time, prices fall because the market becomes flooded— e.g., the Target case (Kirk, 2014)— leveling off as the data becomes stale, or if there has been significant time since the last breach. This cycle continues with each new large breach. Access to botnets and DDoS capabilities are cheaper because there are so many more options (same for exploit kits). The price of PII/PHI is falling (although some believe that its value is rising).[13]

Although transactions can be done by means of nondigital currency, sites are moving toward accepting only digital cryptocurrencies, with anonymity and other security character-

[12] For instance, different installs of a product can be tracked to ensure a user is not getting more than what they paid for. For example, if a buyer purchases a package to infect 1,000 machines, but figures out a way to infect 10,000 machines, the supplier will cut the user off or demand payment for the extra infections.

[13] One example is Clarke (2013a).

istics. Various versions of digital currency and digital currency platforms have been around since the early 2000s. Popular ones have been Liberty Reserve (until taken down in May 2013), WebMoney, and Bitcoin. Others include Pecunix, AlertPay, PPcoin, Litecoin, Feathercoin, and Bitcoin extensions, such as Zerocoin. There is no consensus on which form of digital currency, if any, might be a clear leader; many digital currencies are interchangeable. Whichever currency prevails is likely to be chosen for its anonymity, security, and nontraceability.

Exchanges surrounding these cryptocurrencies are increasing in popularity, as are attacks on them. Experts predict that we will soon see more cryptocurrency targeting, DDoS services against cryptocurrencies, and more malware with the sole purpose of targeting wallets and bitcoins.

It is difficult to assess trends for different products; product/price relationships can be quite nuanced and depend on a variety of factors (e.g., brand name, quality of services, renting vs. buying). Although prices range widely—for example, hacking into accounts can cost anywhere from $16 to more than $325, depending on the account type (Goncharov, 2012)—similar products tend to go for similar amounts. Exploit kit prices vary based on whether they are purchased outright or rented for intervals of varied length,[14] what exploits are included, and the quality of services and products offered rather than the quantity of exploits bundled together. Brand-name recognition also plays a role. Services can involve leasing servers, finding traffic, creating a personalized payload (or "cleaning"/obfuscating an already existing payload to avoid antivirus signatures) and setting up infrastructure. See Table 2.2 for (nonexhaustive) examples of prices for exploit kits from 2006–2013, and Table 2.3 and Figure 2.3 for availability of exploit kits. Note these are just a handful of exploit kits that have been available.[15]

Table 2.3 and Figure 2.3 show the number of new exploit kits through 2013. A more concerted effort for trade activity and competition accounts for the 2009 jump. 2012 saw more "interesting" vulnerabilities found and reported—causing an increase in competitors and exploit kits, especially those from Asia (Paget, 2010a).

The cost for data records or credit cards also varies. Account records are more valuable—and hence, more expensive—if more value can be charged against such accounts,[16] they are "newer" to the market (i.e., the account has not yet been closed down by the bank or eCommerce site), or they are rare.[17] After a large breach—for example, the 2005–2006 TJ Maxx/TJX hack, the 2007–2008 Heartland Payment Systems breach, or the recent 2013 Target breach (InformationisBeautiful, undated)—the market may be flooded with data, causing prices to go down; one expert cited a price drop from $15–20/record to $0.75/record over a relatively short period. Prices for credit card data may start at $20–$45/record if supply is limited or the

[14] E.g., renting for a year versus renting for three months.

[15] While they are too numerous to name here, a few notable exploit kits have included: El Fiesta, ICEPack, MPack, GPack, WebAttacker, Fragus, YesExploit, Siberia, Neosploit, MyPolySploit, XCore, UniquePack, LuckySploit, SPack, Liberty, Fiesta, Eleonore, MyLoader, SEO Toolkit, JustExploit Elite Loader, Clean Pack, Shamans Dream, Max Toolkit, CrimePack, FSPack, Sploit25, MultiExploits, Tornado, Limbo, Lucky, Neon, Nuke, Spack, Sploit, Unique, ZoPack, Styx, Neutrino, Magnitude, Sakura, LightsOut, RedKit, Kore, GongDa, et al. More information on several of these exploit kits is available in Parkour (2014).

[16] For example, a credit card with a lower limit, or a low balance in an eCommerce account (e.g., PayPal) is cheaper than the higher-limit signature, gold, or platinum card.

[17] There is not always a steady supply of all types of credit cards. It can depend on where point-of-sale and endpoint terminals (like cash registers) are found to be vulnerable. For example, it may be possible to break into a terminal in Pennsylvania during a time when nothing vulnerable can be found in Germany.

Table 2.2
Exploit Kit Prices Over Time

Exploit Kit	Price	Year
Mpack	$1,000	2006
WebAttacker (Do-it-yourself kit)	$15–20	2006
IcePack	$30–400	2007
Mpack	$700	2007
Eleonore (v1.2)	$700 plus $50 for encrypter	2009
Eleonore (v1.2)	$1,500 fully managed by user	2009
Phoenix	$400	2009
Blackhole (v1.0.0)	$700/three months or $1500/year	2010
CrimePack	$400/license	2010
Eleonore (v1.3.2)	$1,200	2010
Eleonore (v1.6 and v1.6.2)	$2,000	2010
Fragus	$800	2010
LuckySploit	$1,000	2010
Yes Exploit (abuse-immunity)	$1,150	2010
Yes Exploit (Standard Edition)	$900	2010
Phoenix (v2.3)	$2,200	2010
Nuclear	$900	2010
Katrin	$25/day	2011
Robopak	$150/week or $500/month	2011
Blackhole (v1.1.0)	$1,500	2011
Blackhole (v1.2.1)	$700/three months or $1,500/year	2011
Bleeding Life (v3.0)	$1,000	2011
Phoenix (v3.0)	$2,200/single domain	2011
Phoenix (v3.0)	$2,700/multi-threaded domain	2011
Eleonore (v1.6.3a)	$2,000	2011
Eleonore (v1.6.4)	$2,000	2011
Eleonore (v1.6.2)	$2,500-$3,000	2012
Phoenix (v2.3.12)	$2,200 / domain	2012
Styx sploit pack rental	$3,000 / month	2012
Exploit kits that employ botnets	up to $10,000	2012
CritXPack	$400/week	2012
Phoenix (v3.1.15)	$1,000-$1,500	2012
NucSoft	$1,500	2012
Blackhole—hosting (+ crypter + payload + sourcecode)	$200/week or $500/month	2013
Whitehole	$200–$1,800 rent	2013
Blackhole—license	$700/three months or $1,500/year	2013
Cool (+ crypter + payload)	$10,000/month	2013
Gpack	$1,000–$2,000	2013
Mmpack	$1,000–$2,000	2013
Icepack	$1,000–$2,000	2013
Eleonore	$1,000–$2,000	2013
Sweet Orange	$450/week or $1,800/month	2013
Whitehole	$200–600/week or $600–1,800/month, depending on traffic	2013

SOURCES: Clarke, 2013a; Fossi et al., 2011; Fortinet, 2012; Goncharov, 2012; Kafeine, 2013a; Krebs, 2013a; M86 Security Labs, 2010; Martinez, 2007; McAfee Labs, 2011; O'Harrow, 2012; Paget, 2010b, 2012; Parkour, 2014.

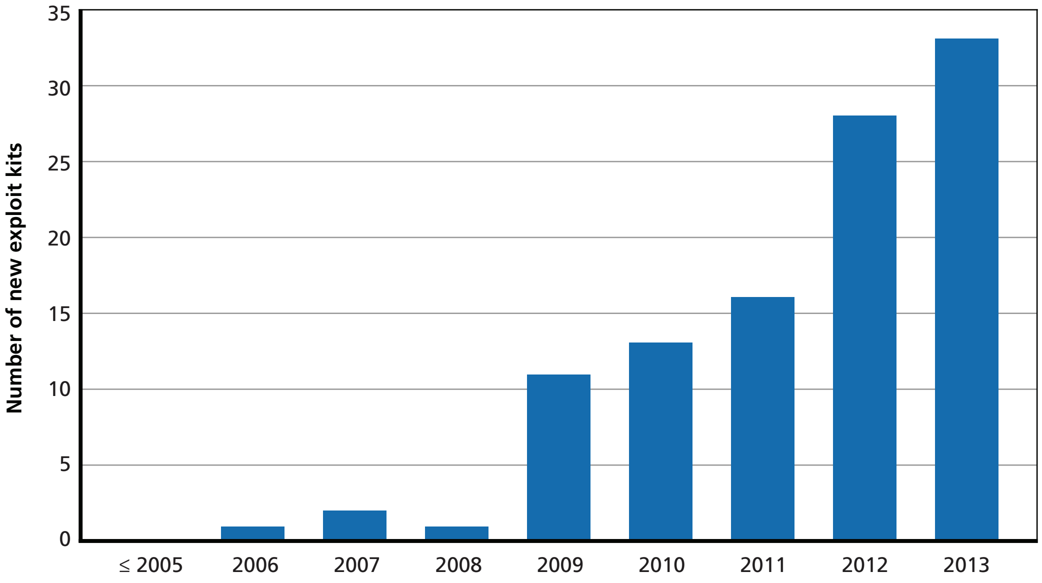
Table 2.3
Proliferation and Variety of Exploit Kits Over Time (non-cumulative)

Year	Number of New Exploit Kits	New Versions of Exploit Kits
≤ 2005	—	—
2006	1	1
2007	2	2
2008	1	1
2009	11	13
2010	13	20
2011	16	24
2012	28	38
2013	33	42

SOURCE: Data drawn from Paget, 2010b, 2012; Parkour, 2014; as well as interviews with Paget and Parkour.

cards are freshly acquired, or \$10–\$12 if there is an influx. Credit cards acquired in the Target breach initially fetched anywhere from \$20–\$135, depending on the type of card, expiration, and limit (Krebs, 2013h). Experts note that high or no-limit cards (e.g., the American Express Black card), or cards with chip and personal identification number (PIN) are more valuable, and can command a higher price, and when the data begin to get stale, it may be "on clear-

Figure 2.3
Proliferation and Variety of Exploit Kits Over Time (non-cumulative)



SOURCE: Data drawn from Paget, 2010b, 2012; Parkour, 2014; as well as interviews with Paget and Parkour.
RAND *RR610-2.3*

Table 2.4
Credit Card Prices Based on Market Circumstance

Credit Card Price	Market Circumstance
$20–$45	Freshly acquired
$10–$12	Flooded
$2–$7	Clearance ("stale" data)

SOURCE: Data drawn from interviews; Krebs, 2013g

ance" for something like $2–$7/record (see Table 2.4). eCommerce accounts (e.g., PayPal or Amazon) can be sold for a fixed price, or based on the percentage of the remaining balance.

Stolen credit card data from Europe and the United Kingdom are more valuable than data from U.S. cards for several reasons:[18]

- There is typically a delay when a card is processed in a foreign bank, so more can be charged before the bank figures it out.
- European cards often have higher credit limits.
- Many European cards (with their chip and PIN with signature system) are normally thought to be more secure that their U.S. counterparts (signature only) and are correspondingly more valuable if they can be broken and put on the black market.

IP is harder to put a value on because it can be so unique, and generally requires a specific buyer. IP can be inadvertently acquired as a byproduct of an intended goal, or can be specifically sought. There are those in the market who sell services to go after IP for a specific buyer, and those who advertise IP as a secondary gain, and who may struggle to find the appropriate buyer.

Reliability and Integrity

The black market continues to put great stock in reputation, at least within the harder-to-access tiers. Thanks to an increase in takedowns (of sites, groups, tools, or individuals), participants have labored to loosen the correlation between virtual identities and real identities. Thus, markets have seen more anonymous currencies and encrypted and stealthy communications. More of the market is hosted on darknets and through VPN services. While this trend does not affect reliability of products (some say it will make it stronger because only the highly vetted make it in), it reduces the accessibility and availability of the market. It also leads to much more intense personal vetting.

The validation of person, product, and payment can all be tricky in underground markets. Buyers and sellers validate each other through reputation, personal relationships, middlemen, or intermediaries (e.g., forum administrators). Sellers may provide demo versions or a sample of their goods. While it is a black market and thus harder to validate payment, it is also

[18] They are followed by countries like Australia, Singapore, and Middle Eastern countries; experts note that most Eastern European or African cards are not considered to be of much value.

a relatively small community—at least in the highly vetted, more elite tiers—where bad apples (e.g., rippers) are more quickly detected.[19]

Vetting entails either having credentials and getting vouched for by members in good standing, or proving oneself (e.g., by getting good reviews on a product presented for examination). Being vetted into the most elite tiers offers great rewards. Those accepted have access to everything they might need. Much of this vetting is based on preexisting cultures, communities, and connections. But the vetting process moves at a deliberate pace; people are particularly wary of those who promise products or services that sound too good to be true. Some members know each other on a personal level, having interacted in gaming forums or even in person; they often speak the same language (see, e.g., Qing, 2011). Some experts say such markets exist in private (e.g., ICQ-type) chat channels; others maintain they exist only in forums; still others say they exist in both, with advertising done in forums but actual transactions conducted via instant messaging. And channels may be open for less than a day to conduct business before administrators tear them down.

Vetting was rare in the early days; it was easy enough for an actor to just want to get involved, and be included. Today, vetting is more robust,[20] and the cost to entry is higher, as takedowns increase and as law enforcement and security companies get more successful at infiltrating the black market. This trend is typical of any move-countermove relationship between offense and defense. More aggressive vetting, especially for access to the high-quality sites and tiers, will mean less accessibility for newcomers, who may be viewed as suspicious. Transactions in the darknet will likely increase, which means it will be harder to get involved if one is not already, and harder for law enforcement to find these marketplaces.

Product and brand reliability also remain important.[21] As a general rule, products and services sold in black markets reliably do what they purport to do. The problem of product *integrity* comes when those reliable goods have additional unwanted "features" (e.g., a backdoor for exploit kit creators to access later). These types of features tend to show up in the lower-tier markets. Thus, performing due diligence on a product, vendor, or service is important; this may require buyers to find a due diligence service or to be tech-savvy enough to investigate matters themselves.

Because contracts in black markets cannot be legally enforced, they are constantly plagued by *rippers*, who do not provide the goods or services they advertise, and are an exception to product reliability. Rippers tend to get reported and then often quickly removed. Although

[19] There is some disagreement on how rampant scams are—but it mostly has to do with which markets and tiers are being discussed:

- Herley and Florêncio (2009b) focus on the lowest market tiers (IRC channels) and states that there are lots of rippers in this market, making it a lemon market. (See also Fisher, 2009.)
- One expert we interviewed stated that the markets that anyone can easily find (e.g. IRC / lowest tier) are rife with a high percentage of rippers. Of the other markets, the lower tier is approximately 30 percent rippers, whereas buyers in the higher tier rarely get ripped off.
- Another expert we interviewed stated that there are very few bad people; while the networks can comprise several thousand people, they stay relatively small and tightknit because most business is reputation-based.
- A general consensus among many of the other experts interviewed stated that, "if you can be scammed, you will be scammed," wherever you might be.

[20] One expert noted that different markets for various goods (e.g. financial data, IP, exploit kits) have their own ways of vetting.

[21] Some say these elements are similar to the noncriminal world, in that there will always be some who care about branding and some who do not.

they can easily access new channels under new names, it takes time to re-establish a reputation, which inhibits cheating. One estimate suggests that about 30 percent of the sellers (at least of financial data) are rippers, and the success rate of getting money back after being ripped off is only 15–20 percent. Unsophisticated or newer buyers are most often the ones cheated. For the most part, this happens in the lower, easier-to-access, less-vetted tier, as well as the parts of the black market that deal with credit cards and financial data, where rippers are prevalent.

Sensitivity to External Events

Different pieces of the market react differently to outside events (e.g., natural disasters, revelations to Wikileaks, or releases of new operating systems). Front-page news items are often used in spear-phishing campaigns (e.g., "click this link to donate to victims of Haiti earthquake") raising the number of potential victims. Conversely, unrest in a certain part of the world can take people there out of the market (e.g., some vendors of credit card data from Egypt were less active during unrest). This can raise the price of products as the supply decreases.

Although newer operating systems and browsers tend to be more secure against attacks, their introduction does not affect black markets immediately because developers (and their kits, programs, and products) tend to focus on the plentitude of older systems with unpatched software. When the newer systems are targeted, malware developers make sure their tools are up to date with the latest releases (e.g., can get past the latest antivirus) and can affect as many users as possible.

Resilience

The black market acts much like a traditional market; profit drives people to innovate and keep pace with rapidly changing technology. As more targets (users, companies, etc.) increase their digital connections and points of presence, the market keeps pace. Whatever is new or novel for the traditional consumer—from mobile devices to cloud solutions and new social media platforms—offers new entries for attack and will thus have a counterpart exploit on the black market.

Another facet of resilience has been the black markets' ability to survive the recent increase in takedowns, which have little effect on the size or composition of the black market. As one entity goes down, another takes its place, often within days. Although suspicion and "paranoia" spike among participants, and some countermeasures are enacted (such as stronger encryption, more vetting, increased stealth, etc.), the market just hiccups and returns to normal, albeit a somewhat less accessible and less open version of normal.

Several factors explain the recent increase in takedowns:

1. **Law enforcement has gotten better over the last ten to 15 years.** Those now coming into law enforcement have grown up comfortable with technology and computers. Training in the digital world has gotten better for law enforcers all over the world, making them stronger as an entity. Overseas partnerships and cross-pollination of ideas have also improved law enforcement—although perhaps more so at the federal

level. Leadership in law enforcement, intelligence, and the Department of Defense has accorded cyber top priority and moved resources accordingly.

2. **Suspects are going after bigger targets (and thus are attracting more attention).** Since roughly 2002, attacks have shifted from opportunistic one-offs (going after whoever may be unsecure) to attacking companies. Companies, now that they understand they are targets, are more willing to work with law enforcement, and the public-private partnership has gotten better.
3. **Crimes involving digital goods are proliferating.** In 1998, few crimes involved the digital realm (in the single digits). Starting at the turn of the century (2000–2001), more crimes were digital (about half). Now, almost everything involves a digital aspect. Because so much more crime has a digital element, law enforcement has more opportunities to encounter crime in cyberspace and learn from such encounters.

But law enforcement may become a victim of its own success. More arrests and takedowns lead to more media coverage, and hackers become more aware of the opportunities provided by black markets. Further, those already in the market grow smarter as they learn from law enforcement's investigative techniques.

Additionally, the consequences of takedowns are transitory. Consider the following:

Liberty Reserve

- Takedown: May 2013[22]
- Other Currencies Used: Immediately
- Immediately thereafter, several other types of digital currencies were up and running, [23] but so far without a clear winner.[24]

Blackhole Exploit Kit (and Cool Exploit Kit)

- Author / Administrator Arrested: October 2013
- Other Exploit Kits Up and Running: Almost immediately.[25]
- The Blackhole Exploit Kit was the most popular as-a-service exploit kit from the time it launched in late 2010 to the arrest of its author (developer and maintainer). In 2012, more than half of the web threats were cited as from Blackhole (Howard, undated). While no clear winner has emerged from Blackhole's takedown, there are plenty of viable candidates.

Silk Road

- Takedown: October 2013 (the alleged chief operator, Ross Ulbricht, was arrested)[26]

[22] See Krebs (2013b) on the takedown.

[23] See Krebs (2013c) on different types of digital currencies.

[24] Krebs compares it to the number of peer-to-peer systems that popped up after the takedown of Napster in the 1990s.

[25] There was a quick move from Cool Exploit Kit (a more exclusive version of Blackhole Exploit Kit) to Whitehole Exploit Kit (Segura, 2013); Arrest of alleged Blackhole Exploit Kit author, Paunch, led to reduction of spam campaigns using Blackhole Exploit Kits—but other spam took its place (Manly, 2013); Magnitude Exploit Kit replaced Blackhole (Kovacs, 2013b); Neutrino, Kore, and Nuclear Pack also remain popular exploit kits (Kafeine, 2013b)

[26] The operator assumed the moniker "The Dread Pirate Roberts."

- Version 2.0 Back Up: November 2013 (under a different Dread Pirate Roberts)[27]
- The Silk Road, a marketplace mostly known for illicit drugs, also dealt in items such as stolen credit cards and other records. Silk Road 2.0 is still finding its footing.

Carder.su

- Takedown: March 2012[28]
- Other Forums in Its Place: Almost immediately
- Carder.su trafficked in credit card and other stolen financial information. Other markets such as carderplanet, carder.pro, badb.su, etc. existed before, during, and after carder.su (Krebs, 2012; Krebs, 2013d).

Vietnamese ring dealing with identity theft and stolen eCommerce accounts

- Takedown: 2012 (Leyden, 2013b)
- After the arrest of 14 masterminds of an elaborate ring involved in selling identities and eCommerce accounts (e.g., PayPal, Amazon, etc.), other (lower) members of the group stepped up to continue operations (Krebs, 2013g).

One reason takedowns only temporarily affect the black markets is that even if a tool, forum, group, or individual gets taken down, the vast majority of what is used does not get taken down, too. For example, exploit kits are not generally proprietary, and other groups can use them or build their own based on leaked or released source code. In fact, takedowns may be beneficial for the market as the removal of a popular product allows others to vie for its now available market share. The decline of Blackhole Exploit Kit is one example of this.

Perhaps another reason that takedowns have not seriously dented the market is that many countries condone hacker activity that is illegal in the United States. One Russian hacker was arrested, let out on a technicality, apologized to, and is now connected to the government. Although Russian officials may have a good idea of what is happening, as long as they can point to fraud in other parts of the world—especially in the West—they tend to let things slide (de Carbonnel, 2013). China also tends to turn a blind eye, although there are reports of cracking down on some fraudsters.

But not all countries are like that. To give a few examples, Vietnam is very helpful, and other Eastern European countries (e.g., Romania, Ukraine, Poland) can be selectively helpful (perhaps, on Ukraine's part, to retain its option to rejoin the European Union).

[27] See timeline in Antilop (2014).

[28] See Ritter (2012); Warner (2009); Warner (2012); and United States of America vs [redacted], (2012).