13

Cybercrime: The Evolution of Traditional Crime

Raj Samani

> "Cybercrime is a growth industry. The returns are great, and the risks are low. We estimate that the likely annual cost to the global economy from cybercrime is more than $400 billion."[1]

While the actual figure may be debated, there is no question that cybercrime is a growth industry. It seems the only debate we have regarding the growth of cybercrime is whether it is an evolution of traditional crime or a revolution. Making this distinction is based on one's perspective; having worked within this industry for some time now, I would argue that the former conceptualization of cybercrime—as evolutionary—is most accurate. However, when compared with crimes that have been wreaking havoc for centuries (e.g., smuggling, theft), their transition to or dependency on the cyber domain started overnight, and might seem to justify characterizing this transition as revolutionary. Regardless of this distinction, criminals that have adopted a digital arm are netting enormous sums of money. Take, for example, the recent case entitled Operation *Carbanak*, in which financial institutions were reported to have lost $1 billion through an "Advanced Persistent Threat" (APT).[2] Though the name "Advanced" infers sophistication, the reality is that these banks were initially infected by nothing more than an employee receiving an email with a link to a malicious site. In fact, what is even more worrying is that this simple approach of infection is behind most of the breaches that we hear about on a daily basis.

The opportunities cybercrime present have caught the attention of traditional criminals; now "traditional Mafia groups are increasingly outsourcing their specialist operations to highly skilled freelance cybercriminals who promote their services on hidden websites."[3] These new partnerships have altered the modus operandi of traditional criminals. According to Rob Wainwright, director of Europol, "We're seeing a move away from the traditional model of organised Mafia-like structures that are very hierarchical.… They make use of this industry of criminals with a particular service or product to feed to organized crime groups. It's the same as the legitimate commercial world: outsourcing is what happens."[4] The outsourcing of cyber-related operations means that the barriers for becoming a cybercriminal are probably at the lowest ever. The reduction in these technical barriers is important, because when combined with the huge revenues, as well as the ability to perpetrate a crime in another country without ever leaving your desk, the perfect storm for society is created. In this case, the introduction of such factors means that every business, and every user is susceptible to digital crime. This may seem like overstating

the issue, after all not every person is online; however, recent cyber-attacks have even disrupted the availability of electricity in thousands of homes in Eastern Europe.

This chapter will survey a limited sample of the novel cyber techniques that have made the cyber domain easily accessible to those with criminal intent, and a danger zone for legitimate actors, both official and private. However, this is only part of the story, because any such cyber-attack, and certainly those that involve the theft of data, will result in criminals being in possession of huge amounts of sensitive information. One question that is often asked is, "What to do they do with this stolen data?" Answering this question is particularly difficult as we are not privy to deals criminals may have with one another; however, in many cases this data is stolen without a prearranged buyer. In these circumstances, we can clearly see this data being sold in online marketplaces. What is even more remarkable is that much of this data is sold on the Surface Web—the same internet that you and I use every day—using the same popular search engines. It is important to make this distinction, because this chapter focuses on the accessibility of tools that facilitate cybercrime; therefore, easily getting to these tools becomes important. The hosting of these tools will vary; some of which are available on the Surface Web, others are within Dark Web, and some of which are in the Deep Web. In many cases, the latter two are used interchangeably but strictly speaking this is inaccurate. To be clear, the "Surface Web" refers to the portion of the internet that can be accessed via the standard browser, and found with a normal search engine. The "Dark Web" refers to those sites that can still be accessed via a normal browser, but are not searchable via search engines. Finally, the "Deep Web" refers to a portion of the internet that is hidden on purpose and cannot be accessed via a standard web browser. Accessing this portion of the internet requires a specialized web browser, which can be easily downloaded onto standard operating systems. Once downloaded, the user can then use this browser to access sites on this hidden portion of the internet.

Cybercrime-as-a-Service

Describing the emergence of a marketplace for those wishing to carry out cybercrime in one chapter is no simple task. There are a lot of sellers selling all manner of products to a range of buyers. The following, therefore, only provides a sample of the types of products available, but does so within four categories:

1. *Research-as-a-Service.* Unlike other categories, buying in research does not have to originate from illegal sources; there is room for a gray market. Take, for example, the *Carbanak* case study referred to above; criminals clearly had email addresses of their victims. Buying such lists is a simple task that can be done by commercial companies selling what they call "marketing databases."
2. *Crimeware-as-a-Service.* Once criminals have identified their target, in many cases they will attempt to install malicious software on the victim's computer. This could be with the intent to steal using malware, which incorporates the

identification and development of the exploits used for the intended operation—and may also include development of ancillary material to support the attack.[5] This category also includes the availability of hardware that may be used for financial fraud (e.g., card skimming) or equipment used to hack into physical platforms.

3. *Cybercrime Infrastructure-as-a-Service.* Once the toolset has been developed, cybercriminals are faced with the challenge of delivering their exploits to their intended victims. An example is rental of a network of computers to carry out a denial-of-service (DoS) attack. Other examples are included within the text below.
4. *Hacking-as-a-Service.* Acquiring the individual components of an attack remains an option; alternatively, there are services that allow for outsourcing of the attack entirely. This path requires minimal technical expertise, although it is likely to cost more than acquiring individual components. This category also supports the availability of information to be used for identity theft, for example, requesting information such as bank credentials, credit card data, and login details to particular websites.

While many services within the cybercrime ecosystem will fall within the preceding categories, there are many more that will not neatly fit within these descriptions. There is no intention to attempt to define every possible service, particularly because the environment is fluid and new products and services emerge on a constant basis. The intention of this chapter is to demonstrate the ease with which anybody has the ability to become a cybercriminal through illustration of the ecosystem and of the "as-a-Service" (aaS) nature of cybercrime today. Furthermore, it will focus on the sheer scale and volume of stolen data becoming available for sale as an indication as to the problem cybercrime has become for us as a society.

Cybercrime Exposed

In 2013, I co-authored a report entitled, "Cybercrime Exposed" that presented this burgeoning economy and provided examples where cybercrime is replacing or evolving from traditional crime in multiple ways. Even in the short time since that paper was published, the cybercrime market has grown tremendously. This chapter might be considered as an update to the earlier report, addressing the subsequent reports that considered other factors such as payment and cashing out.[6]

The central question that both "Cybercrime Exposed" and this chapter seek to address is: Are we witnessing a fundamental transformation of traditional crime, and if so, what are the characteristics of the criminal activities replacing it? The Federal Bureau of Investigation (FBI) reported a decline in physical crimes, such as bank robberies, in 2012, as opposed to cybercrime, which has increased significantly.[7] In the report, it was reported that there were 5,000 bank robberies in 2011, but that number dropped to 3,870, marking a

23 percent decrease. Compare this to cybercrime: a recent Pricewaterhouse Coopers (PwC) study of cybercrime in the United States stated that "the U.S. Secret Service has reported a marked increase in the quality, quantity, and complexity of cybercrimes targeting both private industry and critical infrastructure."[8] In terms of monetary value, the global cost of cybercrime is estimated to be $445 billion per year.[9] Clearly, the risk associated with physical crimes, such as bank robberies, contributes to such a shift; cybercriminals enjoy the luxury of carrying out their crimes from a physical location of their choosing.

The Center for Strategic and International Studies (CSIS) report's "Net Losses: Calculating the Cost of Cybercrime" suggested that "the combination of high value, low risk, and low 'work factor' (the amount of effort it takes to break into a network) makes cybercrime a winning proposition."[10] The latter part of this statement refers to the ease with which cybercrime tools are made available. Moreover, the cybercrime market now affords potential criminals with a multitude of services. The result is that deep technical expertise is not a prerequisite to engage in cybercrime. In "Cybercrime Exposed," the head of the European Cybercrime Centre notes that "today's cybercriminals do not necessarily require considerable technical expertise to get the job done, nor, in certain cases, do they even need to own a computer. All they need is a credit card."[11]

The services-based nature of cybercrime allows greater efficiency and flexibility when conducting business. The ability to provide technology solutions as a service to businesses has allowed organizations to focus on their core competencies. An unintended consequence of this evolution has been the rise of the aaS model and a marketplace offering multiple variants of hosted services. Although this approach may seem innovative, the aaS model itself is nothing new. The underground economy established by cybercriminals has been using a services-based model for some time. Although the term "Crimeware-as-a-Service" may be relatively new, the services-based nature of cybercrime has been in effect considerably longer than its descriptive acronym. Moreover, the services-based approach extends well beyond hiring individuals to undertake specific tasks (e.g., coding an exploit). With a broad variety of products and services available either to buy or rent, such an economy has evolved with more products coming online. Having addressed the overall services orientation of the cybercrime industry, it is now fitting to delve into the specific services available.

Research-as-a-Service

The available services within this category include the identification of a previously unknown vulnerability within a targeted system, otherwise known as "zero-day vulnerability." Despite the threat of legal action by affected software vendors in certain countries, the sale of vulnerabilities has recently become a growth area for researchers and brokers alike. Today, security researchers are presented with a number of options when they identify previously unknown zero-day vulnerabilities. Each option is accompanied by differing outcomes in publicity and monetary compensation. Today's marketplace provides those looking to acquire zero-day vulnerabilities with many options. At first

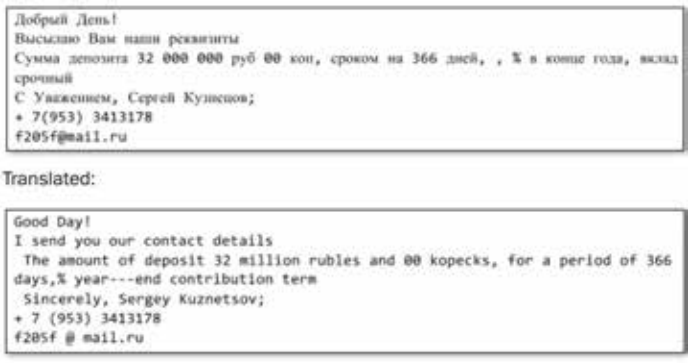
glance, this may appear to be detrimental to underground marketplaces. For example, one particular vendor defines its eligibility requirements as being limited to only public sector organizations, in particular, law enforcement. Furthermore, restrictions are placed on the geographic location of the agency; its customers can only be in predefined countries. However, though many organizations selling zero-day vulnerabilities actually limit their sale to specific buyers, the underground market continues to thrive.

It is worth noting that the acquisition of zero-day vulnerabilities is a somewhat gray area, since sellers will not disclose their customer lists; however, recent breaches of companies that sell such services revealed that their customers included many government agencies.[12] Important among these actors are "exploit brokers." Although the acquisition of vulnerabilities can be conducted through a commercial entity, there is an opportunity to connect with a brokering service, which can be defined as a single individual who acts as a middleman to facilitate the sale to a third-party. By acting as middleman for the sale of zero-day vulnerabilities, exploit brokers are able to charge a commission by facilitating the sale of said vulnerabilities. For example, in one scenario the sale of an Apple iOS exploit for $250,000 allowed the broker to pocket 15 percent in commission.[13] Customers of such vulnerabilities are not necessarily committing a crime in acquiring such products, and as the example above has demonstrated, their acquisition is limited to certain organizations.

Spam Services

In the majority of successful cyber-attacks, the initial infection vector will use a spear-phishing message to someone within the target organization. What this usually means is that somebody within the targeted organization will receive an email invoking some form of action (e.g., clicking onto a link), which in turn results in malware being installed onto their computer. This was demonstrated in Operation *Carbanak*; in this case "all observed cases used spear phishing emails with Microsoft Word 97 – 2003 (.doc) files attached or CPL files."[14] An example of the phishing email that was sent to employees within the targeted organization is illustrated in Figure 13.1.

Figure 13.1. *Carbanak* Phishing Email (with Translation)



Source: Kaspersky

Whether the target for the attack is a consumer or an employee within a large enterprise, the modus operandi for many cybercriminals is to leverage some form of social engineering to coerce the user into an action facilitating malware infection.

However, with the prevalence of social engineering in many publicly disclosed cyber-attacks, there exists either an inherent weakness in the acumen of victims to distinguish malicious communications, or cybercriminals are using more complex methods to bypass the "human firewall." The answer, of course, likely lies somewhere in between these two statements, but regardless of the root cause, it does demonstrate that the first line of defense is evidently failing. More importantly, the default position—to simply blame users as the cause for breaches—is not entirely fair. Indeed, while there will be examples where clearly unsafe practices are being employed, as this chapter will demonstrate, the techniques used by attackers are intended to bypass the consciousness of their targets and attempt to manipulate victims through leveraging subconscious levers of influence.

For the purpose of this chapter, I define "social engineering" as a deliberate application of deceitful techniques designed to manipulate someone into divulging information or performing actions that may result in the release of that information.[15] During a social engineering interaction, the target is not consciously aware their actions are wrong or ill-advised. The social engineer exploits the natural instincts, not the criminality of the target. This is done using a variety of methods to trick the user into divulging useful information or performing an action, such as clicking a link. Social engineering exploits subconscious behavior of the target, unlike conscious techniques such as bribery, threat of violence, and so on, which do not fall within the scope of social engineering.

Any successful spam campaign relies on a number of factors, many of which are discussed below. One fundamental element belongs in the Research-as-a-Service category: the identification of targets. Having to manually gather together an email list can be a time-consuming exercise—fortunately, the would-be spammer has the luxury of simply purchasing a list of email addresses. Aside from the customization of the message in a particular language, the unsolicited email may require more granularity. For example, there is also the opportunity to acquire email addresses from a specific geography, with the level of granularity even to state or city level.

Such examples are merely the tip of the iceberg. Indeed, since the publication of "Cybercrime Exposed," we have identified an enormous marketplace offering email addresses at considerably low prices within commercial environments. In fact, on commercial auction sites, 50,000 email addresses that are available on a per-town basis sell for as little as $10. These are advertised as marketing databases; however, they give no indication of whether consent has been confirmed (as per Data Protection requirements). Attempting to understand the scale and volume of sales for unauthorized personal information is difficult; however, one indication was revealed in the "What Price Privacy" report by the United Kingdom Information Commissioner which states, "We know of one private investigation firm receiving some £50,000 a month from just one finance company for tracing new addresses at £35 a time, and £55 for a new employer and new address. The

same firm was also undertaking checks for other companies, which gives some idea of the scale of operations."[16]

While granularity based on geographic location is common, the would-be spammer has the opportunity to be even more specific about the potential targets. For example, a campaign may target specific users of a service, a particular bank, or an internet service provider. Or a campaign may target specific professions, or even a specific gender. In such instances, the underground marketplace supports the acquisition of such lists, as depicted in Figure 13.2. As this illustrates, it is possible to identify a specific profession as well as a certain geography, such as U.S. doctors. Another consideration should be the manner in which the service is offered. The presentation of the service is similar to those offered by legitimate companies selling legal products; some even offer commercial payment mechanisms.

Figure 13.2. Selling Email Addresses by Profession

Source: McAfee Labs

Identifying a list of targets is the first step, developing a convincing message and the requisite malware will follow. However, as we will see in the following sections, these are all accessible and available for sale.

Crimeware-as-a-Service

In the past, the distinction between the accessibility of crimeware and Research-as-a-Service options was that the former was only accessible in underground forums while the latter was accessible on the Surface Web. Focusing our attention on the availability of tools necessary to infect victims, we find a multitude of products available for either sale or rent. Below are many of the Crimeware-as-a-Service tools available today.

Professional Services

Simply purchasing details of where vulnerabilities may exist within a specific application or computer operating system is only the first step. There will then exist a requirement to

develop specific code to exploit this vulnerability, which can be outsourced. An example of this was seen as early as 2005, with the Zotob worm. In this example, a programmer was paid to develop the malware; indeed, after the arrest of two individuals, according to the assistant director of the FBI Cyber Division, "the Moroccan was responsible for writing the code, he had a financial relationship with the Turkish man."[17] Other professional services include translations. In the Research-as-a-Service category, we saw how it was possible to acquire email addresses for a specific country; if the attacker is a native speaker, then crafting an email to entice victims is relatively simple. However, the cybercrime market has evolved such that not knowing a language is no longer a hindrance in targeting particular populations. Services provide translations to support non-native speakers in their efforts to communicate with potential victims. What is even more remarkable is that much like the modern social media tools we use today, there is an indicator as to the reputation of the individual behind the profile offering such services.

Malware Services

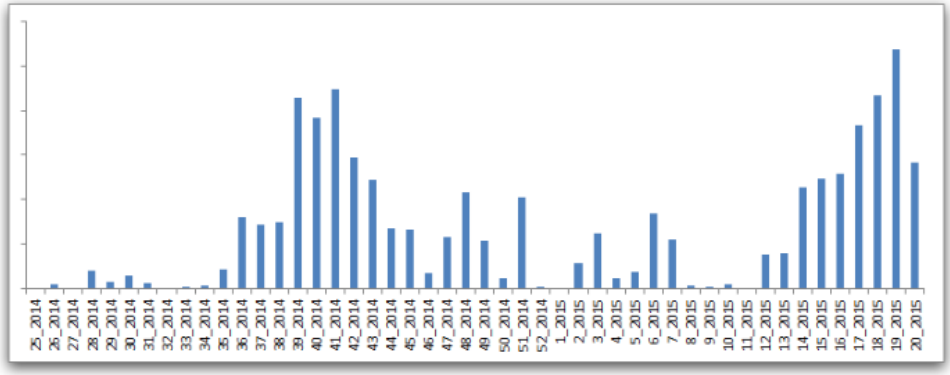
Developing a convincing phishing email is the first step, but as we have seen in the *Carbanak* example, developing malware that can infect the computer of an employee within the targeted organization is also critical. For the development of such nefarious code, there is a burgeoning marketplace available that negates the need for technical knowledge on the part of the cybercriminal. This takes the form of numerous malware variants available for sale, or even available for rental. Purchasers can acquire developed code to conduct their attacks. For example, attackers who want to acquire information can buy a Trojan Horse, a malicious program concealed within a legitimate file. Other examples include:

- *Rootkit Services.* Surreptitious code that conceals itself within the compromised system and performs actions as programmed.
- *Ransomware Services.* Software that restricts the user from conducting further activity until a specific action is taken (such as providing credit card details). An example of this ransomware aaS phenomenon under the name of "Tox" was uncovered in recent research conducted by McAfee Labs.[18] This program provides visitors a free service to develop a ransomware campaign and target any number of users. Once the visitor has registered, the only required action is to enter the amount of money that will be charged to unfortunate victims (the ransom amount), a particular cause, and of course, the obligatory captcha (the graphic that is used in the registration process, usually asking the person to type in certain characters). Once this information is provided, the newly registered user has to enter a Bitcoin address, and all profit (less a 20-percent service fee) is transferred to them. Tox is not an isolated case; many of the most prevalent ransomware campaigns are based on this aaS model which may, in part, explain the reason for such a growth in this digital threat—ease of use, and of course, profits. Consider that "between February and April 2015, the perpetrators extorted

$76,522 from 163 victims," using the TelsaCrypt variant of ransomware.[19]

- *Exploits.* There are many options to purchase exploits that take advantage of vulnerabilities. Their prices vary based upon the target system and whether the vulnerability has been previously identified. There is also the opportunity to rent as opposed to buying. The CritX tool kit, for example, charges by the day, and recently advertised for $150 per day. While acquiring individual exploits is an option, a more commonly adopted method has been the use of exploit kits (EKs). These kits are used "in a process known as a drive-by download, which invisibly directs a user's browser to a malicious website that hosts an exploit kit. The exploit kit then proceeds to exploit security holes, known as vulnerabilities, in order to infect the user with malware. The entire process can occur completely invisibly, requiring no user action."[20] To get a sense of the growth of exploit kits, Figure 13.3 illustrates the number of detections on a weekly basis by security firm Sophos, of the most popular kit (as of the time of writing) known as Angler.

Figure 13.3. Growth of Angler EK



Source: Sophos

Such investment on the part of the cybercriminal will motivate the acquisition of services to evade possible detection (note that Tox has these included by default). To avoid possible detection, there exists many services that can assist in obfuscation; this includes the cryptor packs that can encrypt particular files, as well as counter-antivirus (AV) services. The latter are services that allow would-be attackers to run their exploits against the most popular AV products to ensure that they are not identified as malware. While the manual process of installing every possible AV program and running the exploit can be costly, it will certainly be incredibly time-consuming. Counter-AV services are an extremely cost-efficient method in ensuring that the attack is not easily detected, and one such service allows the cybercriminal to run newly acquired exploits against the most popular AV software packages for less than $0.15 per check.

Cybercrime Infrastructure-as-a-Service

Identifying a list of suitable targets, and developing the necessary tools to facilitate an infection may be perceived as all of the necessary steps required to conduct a successful cyber-attack. However, the question of delivering the attack remains. For a would-be cybercriminal, the option to leverage the aaS model remains available. As expected, the marketplace offers a number of infrastructure services to support a cybercrime operation. These range from the availability of services to conduct DoS attacks (attacks that aim to impact the availability of victim services by overwhelming them with excessive volume), to hosting malicious content.

Botnets

A robot network, or botnet, is a network of infected computers under the remote control of an online criminal. The botnet can be used for a number of services, such as sending spam, launching DoS, and distributing malware. As one would expect, the cybercrime marketplace offers the would-be cybercriminal a multitude of options in terms of leveraging the botnet for the facilitation of an attack. Indeed, the rental options of a botnet show a relatively cost-effective mechanism. These prices will of course vary, but according to Havocscope:

> The price to rent 1,000 infected computers in the United States costs $180. If the hosts are located in the United Kingdom, the price is $240. France and Russia both costs [sic] $200, Canada costs $270, and 1,000 infected computers located around the world costs $35. There is a daily limit of 20,000 hosts.[21]

What we tend to find is that the variants, or rather, configurable options, will impact the price paid. As the above quote demonstrates, geographic location makes a difference; however, alternate options include regular updates (so that the code will regularly change and reduce the likelihood of detection and clean-up amongst the infected computers) and the modules that are provided. These modules refer to the function of the botnet; for example, if you want your botnet to steal passwords from infected computers, then this module may be added.

Hosting Services

A "bulletproof" hosting provider is a company that knowingly provides web or domain hosting (or other related services) to cybercriminals, intending to ignore complaints by turning a blind eye to the malevolent use of their services. Such services provide a multitude of options for the buyer. In one particular example, an individual known as "Matad0r" provided three levels of service, ranging from $50 per month to as much as $400 per month. The variable pricing is based on the specification of the system provided; a more powerful system with more options corresponds to a higher price. This demonstrates that, much like the commercial environment, a myriad of hosting services is available—the only constraint is the amount of money one is willing to pay, and, in some cases, the ethics of the hosting provider. The term "ethics" refers to what the hosting provider is willing

to host on the systems they offer to market. Some sellers will be specific about what they are not willing to host, for example, information related to terrorist activities or related to child pornography. There are, of course, sellers of such services that have no concern about hosting such data.

The importance of hosting services should not be underestimated. In the ongoing game of cat and mouse, those behind cyber-attacks will go to extraordinary lengths to ensure that the systems hosting their malicious content are not blocked by security controls. Indeed, this was realized in 2013, in an attack that was described as the biggest cyber-attack of its kind in history.[22] The attack impacted the nonprofit organization Spamhaus, whose team of volunteers maintains blocklists of systems it believes are used for malicious purposes. After blocking servers owned by a Dutch provider known as "Cyberbunker," Spamhaus experienced a significant Distributed Denial-of-Service (DDoS) attack intended to prevent legitimate traffic. Such was the ferocity of the attack, that the chief executive for Spamhaus commented, "they haven't been able to knock us down. Our engineers are doing an immense job in keeping it up. This sort of attack would take down pretty much anything else."

Delivering Unsolicited Mail

Numerous services are available for the would-be spammer. These include services that support the sending of unsolicited mail, alternatively known as a "mail relay." Certain services are capable of managing particularly large volumes; research identified one service capable of sending 30 million emails in a one-month period. What was remarkable was that the service offered a live chat option with a customer service agent, as well as payment options many of us are accustomed to in the legitimate world.

Of course, simply having an infrastructure is not enough to support an unsolicited email campaign. There is also a need for the email addresses themselves, as well as a back end set of systems to continue the deception. The latter could be hosted through bulletproof hosting services, and the former was addressed under the Research-as-a-Service category.

Hacking-as-a-Service

If the budget allows, a budding cybercriminal can skip the process of conducting research, building appropriate tools, and developing an infrastructure, to launch a cyber-attack by choosing a service that will outsource the entire process.

Password Cracking Services

There is a multitude of services available within the Hacking-as-a-Service category. The following examples illustrate how little technical knowledge is required for buyers to try their hand at cybercrime. This includes the availability of services that allow the prospective buyer to retrieve an email password of their intended victim. To illustrate the point made earlier about cybercriminals not requiring any technical expertise, the would-be buyer would only need the email address and name of the target. After that, all that remains is to pay for the service.

Denial-of-Service (DoS)

The press has been awash with stories of hacktivists bringing down large companies with sophisticated hacking techniques. The reality is very different. Although many attacks may be sophisticated, many of them are simply DoS or DDoS attacks. These DoS services aim to send a huge volume of traffic to the victim to overwhelm and disrupt normal business operations. Building a cyber-army capable of generating enough traffic does, at the very least, require an investment in time that the would-be cybercriminal may not have. Fortunately for them (and unfortunately for the rest of us), the aaS cybercrime market is there to help. The price list for a "Cheap Professional DDoS Service" will vary; however, the level of technical knowledge required to recruit such services is very low. It only requires the buyer to inform the service of which site they wish to launch a DDoS attack against, decide how much they are willing to pay, and then initiate the service. What is remarkable however is the cost; one such example is a DDoS attack lasting an hour that only costs $2.

One of the biggest challenges law enforcement faces in combating cybercrime is its global nature, and the above example highlights this. Take for example an attack by one business on its neighbor, where a traditional crime would be carried out in the same physical jurisdiction (e.g., smashing the windows of a neighboring business). In a digital DoS attack, a third-party service may be used. Such a service could be hosted by a provider outside of the geographic jurisdiction of the victim. Introduction of this added level of complexity makes any investigation considerably more difficult.

Hidden Data Economy

The previous examples are of technical services. Yet, also available is an economy in which multiple forms of data are made accessible for sale. Published in late 2015, the new white paper by McAfee (co-authored by myself) uncovers an industry in which for a small fee almost every conceivable stolen record is available.[23]

This underground marketplace has evolved to include almost every conceivable cybercrime product for sale or rent. We correctly predicted that the rise of this aaS model would act as a key driver in the growth of cybercrime. The "McAfee Labs Threats Report: May 2015" provides evidence of this with the rise of the ransomware CTB-Locker.[24] The authors of CTB-Locker established an affiliate program as part of their business strategy: affiliates use their botnets to send spam to potential victims, and for every successful infection in which the victim pays the ransom, the affiliate gets a percentage of the money.

The growth of the aaS economy across all components of an attack (research, cybercrime tools, and infrastructure) continues to grow and none more so than Hacking-as-a-Service, and in particular the component in which stolen data is made available. It is important to highlight why apathy among victims of a data breach, and ultimately those data subjects whose information is being sold, may be costly. A sad side effect of reading about data breaches is the concept of "data breach fatigue," which is another way of saying apathy. The recent article "I Feel Nothing: The Home Depot Hack and Data Breach

Fatigue" provides a wonderful example of such apathy. The author writes, "Because banks are responsible for making us whole if our credit cards are misused, and we are simply issued new cards (an annoying hassle, but not life altering), I join you in reacting to news of these hacks with a shrug."[25] "We are in the trough of disillusionment," says Gartner analyst Avivah Litan.[26] Although such a view may be understandable due to the steady stream of breach notifications and stories detailing the theft of millions of records, it is important to recognize that this is data about us. Our information is being openly sold, and the individual repercussions may not be felt for some time.

Financial Data

Selling stolen financial data is a relatively broad topic, with a multitude of data types for sale and marketplaces that vary between the visible web via a standard browser and the Dark Web through other access methods.

Data breaches involving the theft of financial data, particularly payment card information, continue to dominate headlines. Particularly impacting retailers, the theft of such information invariably results in this data appearing on the visible web. Payment card information made available in those marketplaces will vary in price based on a multitude of options. A snapshot of these options is shown in the following table.

Table 13.1. Estimated Per-Card Prices for Stolen Payment Card Data (Visa, MasterCard, Amex, Discover)

Payment Card Number with CVV2	United States	United Kingdom	Canada	Australia	European Union
Random	$5–$8	$20–$25	$20–$25	$21–$25	$25–$30
With Bank ID Number	$15	$25	$25	$25	$30
With Date of Birth	$15	$30	$30	$30	$35
With Fullzinfo	$30	$35	$40	$40	$45

The preceding categories relate to the information available along with the payment card number:

- "CVV" is the industry acronym for "card verification value." CVV1 is a unique three-digit value encoded on the magnetic stripe of the card, and CVV2 is the three-digit value printed on the back of the card.
- "Random" means that the number is automatically generated (via software).
- "Fullzinfo" means the seller supplies all of the details about the card and its owner, such as full name, billing address, payment card number, expiration date, PIN number, social security number, mother's maiden name, date of birth, and CVV2.

Occasionally, additional information is available for sale. Payment card data that includes "with COB" refers to those cards with associated login and password information. Using these credentials, the buyer can change the shipping or billing address or add a new address. Some sellers fail to deliver the data after purchase. After all, whom will the buyer complain to in the event that the stolen information is not delivered?

Payment Card Data with Additional Information

Buyers have many options, including the geographic source of the card and the card's available balance. Both of these options impact the price of a card, as we see in the following table:

Table 13.2. Dump Track Prices per Card

Dump Track with High Balance	Price
Track 1&2: PinATM United States	$110
Track 1&2: PinATM United Kingdom	$160
Track 1&2: PinATM Canada	$180
Track 1&2: PinATM Australia	$170
Track 1&2: PinATM European Union	$190

The term "dump" refers to information electronically copied from the magnetic strip on the back of credit and debit cards. There are two tracks of data (Track 1 and Track 2) on each card's magnetic stripe. Track 1 is alphanumeric and contains the customer's name and account number. Track 2 is numeric and contains the account number, expiration date, the CVV1 code, and discretionary institution data. List prices are variable, based on supply, balance, and validity.

The sale of payment card data is common, and is well documented in a recent series of McAfee blogs.[27] However, such payment cards are not the usual type of financial data targeted and subsequently sold on the open market. Much like cards, PayPal accounts are also sold on the open market, with their prices determined by additional factors. Such factors are, however, considerably more limited than those of payment cards, with the balance the only defining factor influencing prices, as we see in the following table:

Table 13.3. PayPal Accounts for Sale here

PayPal Account Balance	Estimated Price per Account
$400–$1,000	$20–$50
$1,000–$2,500	$50–$120
$2,500–$5,000	$120–$200
$5,000–$8,000	$200–$300

The prices in this table are estimates, though we have seen many examples of services for sale that fall outside of these price ranges. Everything is available. This includes bank-to-bank transfers offered for sale, and the availability of banking login credentials.

There will always be suspicions about the validity of the products for sale, as many individuals have paid for stolen financial data, only to not receive what they expected. One seller refers to this dishonor among thieves within their opening pitch:

> ARE YOU FED UP OF BEING SCAMMED, AND RIPPED?
> ARE YOU TIRED OF SCAMMERS WASTING YOUR TIME,
> ONLY TO STEAL YOUR HARD-EARNED MONEY?

This particular seller, though not offering free credit cards that a buyer could use as a test, does offer a replacement policy for any cards that do not provide the advertised balance. Other methods of ensuring a seller's honesty include the use of social validation, with positive feedback from other buyers. Forums are full of helpful advice from buyers that have successfully negotiated purchases as well as which sellers to avoid.

> Hey man, don't know if you know this, but [redacted] pulled a exit scam on evo?
> as far as i know, he pulled an exit scam, then he came back saying his friends had screwed him over, asked people to pay like 4BTC to join his official priviate reselling club. he then just disspeared again.
> in fact theres a guy called Underwebfullz (or somthing like that) whos doing the same thing on alpahbay, so people think its him

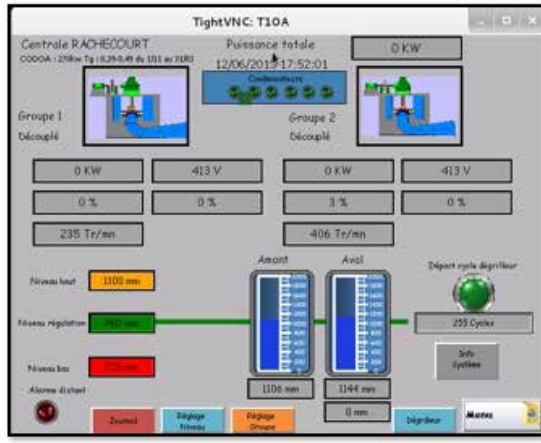
Sellers who employ sophisticated sales and marketing efforts are leveraging YouTube to advertise their wares to potential customers. The videos often attempt to provide some degree of visual confirmation for prospective buyers that they can be trusted, although such approaches can backfire through comments associated with the videos.

Login Access

Other types of data for sale include access into systems within organizations' trusted networks. The types of entry vary, from very simple direct access (e.g., login credentials) to those that require a degree of technical competence to carry out (e.g., vulnerabilities). One seller, for example, was selling access to bank and airline systems located in Europe, Asia, and the United States for a fee.

As with the sale of financial data, sellers strive to offer a degree of proof to prospective buyers that their offers are valid. Recent research by cybercrime expert Idan Aharoni suggests that the types of systems criminals sell access to now include critical infrastructure systems. In his article "SCADA Systems Offered for Sale in the Underground Economy," Aharoni included one example in which a seller provided a screenshot that appears to be a French hydroelectric generator as evidence that the seller had access to it, as depicted in Figure 13.4.[28]

Figure 13.4. For Sale: Access to a Critical Infrastructure System



As with previous examples, a buyer can question whether the access offered is indeed valid. It would not be particularly difficult to produce a screenshot and imply this represents access; yet, this message does represent a very worrying trend, as Aharoni points out.

Access to Online Services

Many people subscribe to digital services, including music, videos, loyalty programs, and others. Because such accounts are relatively inexpensive, one might assume that information from them would not offer a sufficient return. Nonetheless, such accounts are widely available across multiple marketplaces which would suggest a demand amongst prospective customers.

When a stolen online account becomes compromised, the legitimate owner can be impacted in a variety of ways. The account can be held or closed due to malicious activity by the buyer—sometimes causing weeks of support calls. A victim could also suffer financial losses from the purchase of items with stored credit card information, or lose access to free perks such as loyalty points collected during the lifetime of the account. Worse, there are circumstances in which the impact is quite disturbing. The use of a stolen Uber account can bypass many safety checks to protect patrons of the service. An owner of the Uber account can suffer reputation, information, and monetary damage, and a customer of the service could face great personal risk. It is unclear exactly how many valid accounts have been sold, but prices as low as $5 offer anyone the opportunity to masquerade as a

driver.

The sad reality is that access to just about every conceivable online service is available. We found one Hulu account selling for $0.55. With single accounts to digital services selling for less than a dollar, criminals must move a lot of Netflix or Hulu accounts to make their efforts worthwhile. Many other streaming entertainment media services are commonly sold. Both HBO NOW and HBO GO accounts can be found for less than $10, as well as the TV-streaming service Xfinity. Clearly, video streaming services are in high demand. Even live sports streaming services, such as MLB.tv, can be found for $15. We also found other online accounts being sold, including lifetime subscriptions to premium pornography accounts, as well as free referral links to the Dark Web market, Agora.

Even free online accounts attract criminals. For example, a hotel loyalty account with 100,000 points can sell for $20. Customers legitimately open these accounts at no cost, and yet there is a market for them, resulting in the loss of accumulated perks that sometimes take years to accrue. One motivation for purchasing stolen online account access is to hide the buyer's reputation, either due to bad business practices or outright fraud. A buyer wishing to acquire a new eBay business identity can pay plenty, but an established account with good history can be valuable. For less stringent needs, eBay accounts are available in packs of 100 for a range of account types.

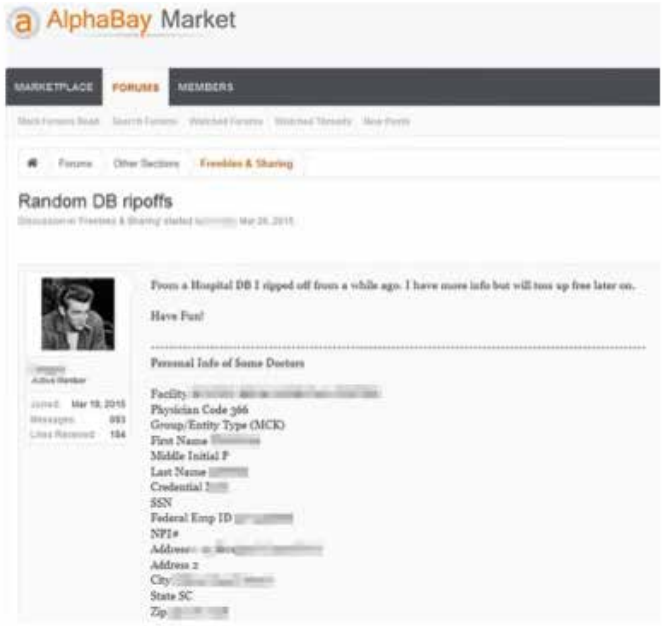
Figure 13.5. eBay Accounts for Sale

Identities

Beyond the sale of these accounts, identity theft is burgeoning aspect of cybercrime. The sale of a victim's identity is the most frightening category because it is so personal. Intel Security recently collaborated with law enforcement agencies in Europe to take down the Beebone botnet.[29] This botnet was able to download malware—including ZBot banking password stealers, Necurs and ZeroAccess rootkits, Cutwail spambots, fake AV, and ransomware—onto the systems of unsuspecting users. We are dismayed at the lack of remedial action taken by users, and in particular those based outside of the United States and Europe. A vast section of society fails to appropriately protect their data—often with significant ramifications. In one case, a particular seller was found offering the complete digital identity of an individual based in the UK; this allowed the prospective buyer to take control of this individual's digital life—social media, email, and more.

Closely related to the marketplace for stolen identities is the marketplace for stolen medical information. Such data is not as easy to buy as payment card data, but sellers of medical information are online. Security journalist Brian Krebs discussed this in his article, "A Day in the Life of a Stolen Healthcare Record," in which a "fraudster leaked a large text file [that] contained the name, address, social security number, and other sensitive information on dozens of physicians across the country."[30]

Figure 13.6. Medical Data for Sale



Conclusion

It would appear that almost not one day goes by without another story of another organization that has fallen victim to another data breach. The only question that is often asked, aside of course from speculation regarding attribution, is the number of records that have been compromised. Indeed, as this chapter has demonstrated, it is not only about payment cards, what with marketplaces selling all forms of data and with ready and willing buyers.

This chapter has intentionally avoided the discussion of attribution for the simple reason that determining the true source of attack within the digital realm is unsuitably technical for this book. As we have seen earlier, there are multiple products, tools, and services available for sale. These are sold to all manner of buyers, from those within the criminal realm—and as we have seen from exposures from zero-day sellers—to those in government institutions. What this demonstrates is that the rather dominant view of hacktivists, criminals, and nation-states is simplistic and naïve. Individuals with specific technical expertise are available for hire. They are available for hire to anybody with the

necessary funds, and through criminal investigations we have seen this outsourcing model used more frequently for everything from the attack itself to even laundering the funds gained from the attack.

This is not a new form of crime; rather, it is an evolution of traditional crime. It seems somewhat trite to end this chapter with this sentence, partly because it is not entirely true. Wars are waged online by nation-states at significantly lower cost than traditional weapons, and more importantly, with plausible deniability. No longer is there a need to send physical assets into hostile territory when it is possible to make a digital attack appear to come from another place in seconds, disrupting an entire nation. Make no mistake—cybercrime is no longer about the lone teenager looking to show off his technical prowess (although this still exists); it is a big business and it is here to stay.

More ominously, all that is available in the Cybercrime-as-a-Service marketplace is available to any malicious actor regardless of their motivations. As we learn more regarding the 2015 Ukrainian power outage, we see that malicious actors are beginning to exploit the connected nature of critical infrastructure. Equally, money gained through cyber-related crimes can be used to advance the goals of such malicious actors against their targeted states. It should be a priority of every state to at least keep up with, if not outpace, the evolving wave of cybercrime.

Notes

[1] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (Santa Clara, CA: McAfee, June 2014).

[2] Limor Kessem, "Carbanak: How Would You Have Stopped a $1 Billion APT Attack?" *Security Intelligence,* February 23, 2015, available at <https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/>.

[3] Paul Peachey, "Mafia cybercrime booming and with it a whole service industry, says study," *Independent,* September 29, 2014, available at <http://www.independent.co.uk/news/uk/crime/mafia-cybercrime-booming-and-with-it-a-whole-service-industry-says-study-9763447.html>.

[4] Ibid.

[5] An exploit is a software that takes advantage of a vulnerability or flaw.

[6] Raj Samani and Francois Paget, *Cybercrime Exposed: Cybercrime-as-a Service*, McAfee White Paper 2013 (Santa Clara, CA: McAfee, 2013), available at <http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf>.

[7] "Robberies decrease as cyber crime increases, FBI says," *WMBF News,* February 5, 2013, available at <http://www.wmbfnews.com/story/20972727/robberies-decrease-as-cyber-crime-increases-fbi-says>.

[8] PricewaterhouseCoopers LLP, *US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey* (New York, NY: PwC LLP, 2014), available at <http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf>.

[9] Chris Strohm, "Cybercrime Remains Growth Industry With $445 Billion Lost," *Bloomberg Business,* June 9, 2014, available at <http://www.bloomberg.com/news/articles/2014-06-09/cybercrime-remains-growth-industry-with-445-billion-lost>.

[10] Center for Strategic and International Studies, *Net Losses.*

[11] Samani and Paget, *Cybercrime Exposed.*

[12] Joshua Kopstein, "Here Are All the Sketchy Government Agencies Buying Hacking Team's Spy Tech," *Motherboard,* July 6, 2015, available at <http://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech>.

[13] Andy Greenberg, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits," *Forbes,* March 23, 2012, available at <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#bbc53f060335>.

[14] "The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide," *Kaspersky,* February 16, 2015, available at <http://www.kaspersky.com/about/news/virus/2015/

Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide>; Kaspersky, *Carbanak APT: The Great Bank Robbery* (Moscow: Kaspersky Lab HQ, February 2015), available at <https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf>.

[15] Raj Samani and Charles McFarland, *Hacking the Human Operating System* (Santa Clara, CA: McAfee, 2013), available at <http://www.mcafee.com/us/resources/reports/rp-hacking-human-os-summary.pdf>.

[16] Information Commissioner's Office, *What price privacy? The unlawful trade in confidential personal information* (Norwich: The Stationery Office, 2006), available at <https://ico.org.uk/media/about-the-ico/documents/1042393/what-price-privacy.pdf>.

[17] Robert Lemos, "Zotob suspects arrested in Turkey and Morocco," *The Channel,* August 30, 2005, available at <http://www.channelregister.co.uk/2005/08/30/zotob_suspects_arrested/>.

[18] McAfee Labs, "Meet 'Tox': Ransomware for the Rest of Us," *McAfee Blogs,* May 23, 2015, available at <https://blogs.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us/>.

[19] John Leyden, "Hi! You've reached TeslaCrypt ransomware customer support. How may we fleece you?" *The Register,* May 20, 2015, available at <http://www.theregister.co.uk/2015/05/20/teslacrypt_ransomware_scam_dissected/>.

[20] Downloads, "A closer look at the Angler exploit kit," *Sophos,* July 21, 2015, available at <https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/>.

[21] "How Much it Costs to Rent a Botnet to DDoS," *Havocscope*, 2014, available at <http://www.havocscope.com/how-to-ddos-by-renting-botnet/>.

[22] Dave Lee, "Global internet slows after 'biggest attack in history,'" *BBC News,* March 27, 2013, available at <http://www.bbc.com/news/technology-21954636>.

[23] Charles McFarland, Francois Paget, and Raj Samani, *The Hidden Data Economy: The Marketplace for Stolen Digital Information*, McAfee White Paper 2015 (Santa Clara, CA: McAfee, 2015), available at <http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf>.

[24] McAfee, *McAfee Labs Threats Report 2015* (Santa Clara, CA: McAfee, 2015), available at <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf>.

[25] Elise Hu, "I Feel Nothing: The Home Depot Hack And Data Breach Fatigue," *NPR,* September 3, 2014, available at <http://www.npr.org/sections/alltechconsidered/2014/09/03/345539074/i-feel-nothing-the-home-depot-hack-and-data-breach-fatigue>.

[26] Ibid.

[27] Raj Samani, "New Year's Sales; Big Discounts on Stolen Data," *McAfee Blogs,* January 29, 2014, available at <https://blogs.mcafee.com/mcafee-labs/new-years-sales-big-discounts-stolen-data/>.

[28] Idan Aharoni, "SCADA Systems Offered for Sale in the Underground Economy," *Infosec Island,* June 22, 2015, available at <http://www.infosecisland.com/blogview/24608-SCADA-Systems-Offered-for-Sale-in-the-Underground-Economy.html>.

[29] McAfee, *Catch Me If You Can: Antics of a Polymorphic Botnet* (Santa Clara, CA: McAfee, 2015), available at <http://www.mcafee.com/us/resources/reports/rp-catch-me-if-you-can.pdf>.

[30] "A Day in the Life of a Stolen Healthcare Record," *Krebson Security,* April 28, 2015, accessed at <http://krebsonsecurity.com/2015/04/a-day-in-the-life-of-a-stolen-healthcare-record/>.