

Cybercrime Exposed

Cybercrime-as-a-Service

By Raj Samani, Vice President and CTO, EMEA, McAfee
François Paget, Senior Threat Research Engineer, McAfee® Labs

Table of Contents

Foreword	3
Executive Summary	4
Cybercrime-as-a-Service	4
Research-as-a-Service	5
Vulnerabilities for sale: a commercial marketplace	5
Exploit brokers	5
Spam services	6
Crimeware-as-a-Service	7
Professional services	7
Malware services	8
Exploits	8
Cybercrime Infrastructure-as-a-Service	11
Botnets	11
Hosting services	12
Spam services	13
Hacking-as-a-Service	14
Password cracking services	14
Denial-of-service	15
Credit card information	16
Conclusion	17
About the Authors	17
About McAfee Labs	18

Foreword

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. A marketplace offering cybercrime tools and services provides would-be criminals with an arsenal that can either be used as a component of a cyberattack or a handy way of outsourcing the process entirely.

This underground marketplace is enabling an army of cybercriminals—and the cost is being borne by all citizens. According to recent research,¹ 17% of European citizens have been victims of identity theft, costing an average of £1,076. Indeed, the ease with which such tools are available enables cybercriminals to target not only citizens, but also businesses and governments at a rapidly growing rate.

Numerous examples of the services-based nature of cybercrime have already caused significant damage. We're not only witnessing an increase in volume of such incidents, but also seeing that the individuals partaking in these misdeeds are far removed from the public perception of the computer hacker.

The growth in the "as-a-service" nature of cybercrime fuels this exponential growth, and this flexible business model allows cybercriminals to execute attacks at considerably less expense than ever before. Examples include the ability to rent services for a relatively small sum—services that offer financial return or that claim to be able to bring down entire sites or systems.

This paper provides insight into the cybercrime marketplace and presents pricing schemes for the services offered. Clearly, these prices will differ based on the sources. One point, however, must be clear: much like law enforcement partners around the world, EC3 European Cybercrime is relentless in the pursuit of criminal groups or networks who steal your money, your information, or your identity and of those who engage in online abuse of children.

Troels Oerting

Head of EC3 European Cybercrime Centre

Executive Summary

There's no doubt that cybercrime is on the increase. That is the message from multiple sources across both the public and private sectors. Indeed, the Federal Bureau of Investigation (FBI) reported a decline in physical crimes such as bank robberies in 2012,² as opposed to cybercrime, which has increased at an alarming rate. 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.

However, one possible contributing factor to this increase is the ease with which cybercrime tools are available. Moreover, the cybercrime market now affords potential criminals with a multitude of services which means that deep technical expertise is not a prerequisite. Much like cloud computing, 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 *as-a-service* acronym "aaS" and a marketplace offering multiple variants of hosted services.

Although this approach may seem innovative, the *as-a-service* model itself is nothing new. The underground economy established by nefarious cybercriminals has used a services-based model for considerably longer than businesses have enjoyed the benefits of cloud computing. 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 (for example, coding an exploit), with a broad variety of products and services available either to buy or rent.

This paper analyzes the growth of the "as-a-service" nature of cybercrime. In particular, it focuses on the evolving manner in which the various actors advertise their services and on the multitude of services now available along with their associated costs. What has become evident is that the marketplace contains many stakeholders, ranging from formal, legitimate organizations selling vulnerabilities to parties that meet their strict eligibility criteria to underground websites that allow individuals to offer illegal services. The focus on cybercrime at a global level by law enforcement has led to "as-a-service" models for illegal activities going even deeper underground.

Such underground platforms are implementing stronger mechanisms to ensure that participants are who they purport to be (or at the very least are not law enforcement officials). Ironically, while the platforms that facilitate the services marketplace for illegal activities are going deeper underground, the trade in zero-day vulnerabilities is more transparent than ever before.

Cybercrime-as-a-Service

There is a multitude of services available to the would-be cybercriminal. Most of these services are clearly administrated by cybercriminals. There are, however, a number of services that remain legal. Overall, we can class services as part of black or gray markets. The classification "gray" is used when the activities or real customers are difficult to determine. To simplify the marketplace, we propose four categories:

1. *Research-as-a-Service*—Unlike other categories, Research-as-a-Service does not have to originate from illegal sources; there is room for a gray market. There are commercial companies that provide the sale of zero-day vulnerabilities to organizations that meet their eligibility criteria. And, there are individuals who act as middlemen, selling such intellectual property to willing buyers who may or may not have the same strict eligibility requirements.
2. *Crimeware-as-a-Service*—This 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 (droppers, downloaders, keyloggers, bots, and more). This also includes tools used to conceal malware from security protection mechanisms (cryptors, polymorphic builders, joiners, crackers, and the like), as well as spammer/robot tools like XRumer. In addition, this category includes the availability of hardware that may be used for financial fraud (for example, 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 include the availability of platforms to host malicious content, such as bullet-proof hosting.
4. *Hacking-as-a-Service*—Acquiring the individual components of an attack remains one 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.

Many services within the cybercrime ecosystem broadly fit within the preceding categories. This paper does not intend to provide an exhaustive overview of every available service, but rather incorporates some key services as an illustration of the ecosystem and of the “as-a-service” nature of cybercrime today.

Research-as-a-Service

The available services within this category include the identification of a previously unknown vulnerability within the targeted system, otherwise known as a 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 unidentified zero-day vulnerabilities. Each represents differing outcomes in publicity and monetary compensation.

Vulnerabilities for sale: a commercial marketplace

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. However, since many organizations selling zero-day vulnerabilities actually limit their sale to specific buyers, the underground market continues to thrive. 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.

Exploit brokers

Although the acquisition of vulnerabilities can be conducted via 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. A recent article in *Forbes*³ provides details of one such individual known as the Grugq. By acting as a middleman for the sale of exploits to government agencies, the broker was able to facilitate the sale of an Apple iOS exploit for \$250,000 and pocket 15% in commission. Table 1 provides the prices that were quoted for zero-day exploits.

Table 1. Prices for zero-day vulnerabilities.

Adobe Reader	\$5,000–\$30,000
Mac OS X	\$20,000–\$50,000
Android	\$30,000–\$60,000
Flash or Java Browser Plug-ins	\$40,000–\$100,000
Microsoft Word	\$50,000–\$100,000
Windows	\$60,000–\$120,000
Firefox or Safari	\$60,000–\$150,000
Chrome or Internet Explorer	\$80,000–\$200,000
iOS	\$100,000–\$250,000

This is just one example, and the middleman in this case represents one individual. As this particular industry is not illegal, there is no shortage of available middlemen advertising their services on very public forums such as Twitter, among others. One Twitter offer we saw read: “Hi...we have 5 Odays that will enter in the auction process.”

The market for these types of services today is very different from the market of six years ago. The 2007 paper, *The Legitimate Vulnerability Market; Inside the Secretive World of 0-day Exploit Sales*,⁴ states, “The current market for the legitimate sale of zero-day exploits is not openly accessible.” However, it is worth noting that although more options may exist, some of the previous challenges from 2007 are still present. As Table 1 indicates, the prices for vulnerabilities vary significantly. Indeed, the level of transparency regarding potential remuneration remains unavailable publicly, which makes decisions about the most profitable route to selling any zero-day vulnerabilities significantly more difficult.

Spam services

A successful spam campaign relies on a number of factors, many of which we cover later. However, one element belongs in the Research-as-a-Service category, namely 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. This is depicted in Figure 1; in this instance, a list of email addresses is available for individuals in France. Aside from the customization of the message in a particular language, the unsolicited email may require more granularity. For example, if there is something particularly relevant in a US state, there are services that supply email addresses belonging to individuals from a specific state, as depicted in Figure 2. In this illustration, the would-be spammer has the opportunity to acquire 10 million email addresses of individuals based in Florida.



Figure 1. French email addresses for sale.



Figure 2. Florida residents email addresses for sale.

Of course, these two examples are merely the tip of the iceberg. They are indicative of the market and the level of granularity. Services are available that offer buyers the ability to purchase varying volumes to support their unsolicited email campaigns. 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 particular gender. In such instances, the underground marketplace supports the acquisition of such lists, as depicted in Figure 3. As this illustrates, it is possible to identify a specific profession as well as geography, such as US 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 3. Anyone call for a doctor?

Later, we will look at other services that support campaigns to propagate unsolicited email. This includes the infrastructure required to distribute the mail, as well as the back-end systems used to host malicious content.

Crimeware-as-a-Service

While the trade in zero-day vulnerabilities may exist within public forums, the underground market offers these and considerably more services. If we focus our attention on the available tools, we find a multitude of cybercrime tools available for either sale or rent. Below are many of the Crimeware-as-a-Service tools available today.

Professional services

Developing code to take advantage of a specific vulnerability requires a degree of technical expertise—at the very least, software programming skills. However, much like the outsourcing market for commercial software, we can find services that offer such code for nefarious purposes. The outsourcing of this particular element of the attack has been around for some time, with some specific examples of malware being outsourced to a third party. 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, which was estimated to have cost affected companies \$97,000 to clean up.⁵

Other professional services available 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.

Not knowing a language is no hindrance, however. Services provide translations to support non-native speakers in their efforts to communicate with potential victims.

Figure 4 shows a forum that offers translation services to would-be buyers. In this example, a communication method is defined, but also included is a reputational indicator. Much like the modern social media tools we use today, there is an indicator as to the reputation of the individual behind the profile.

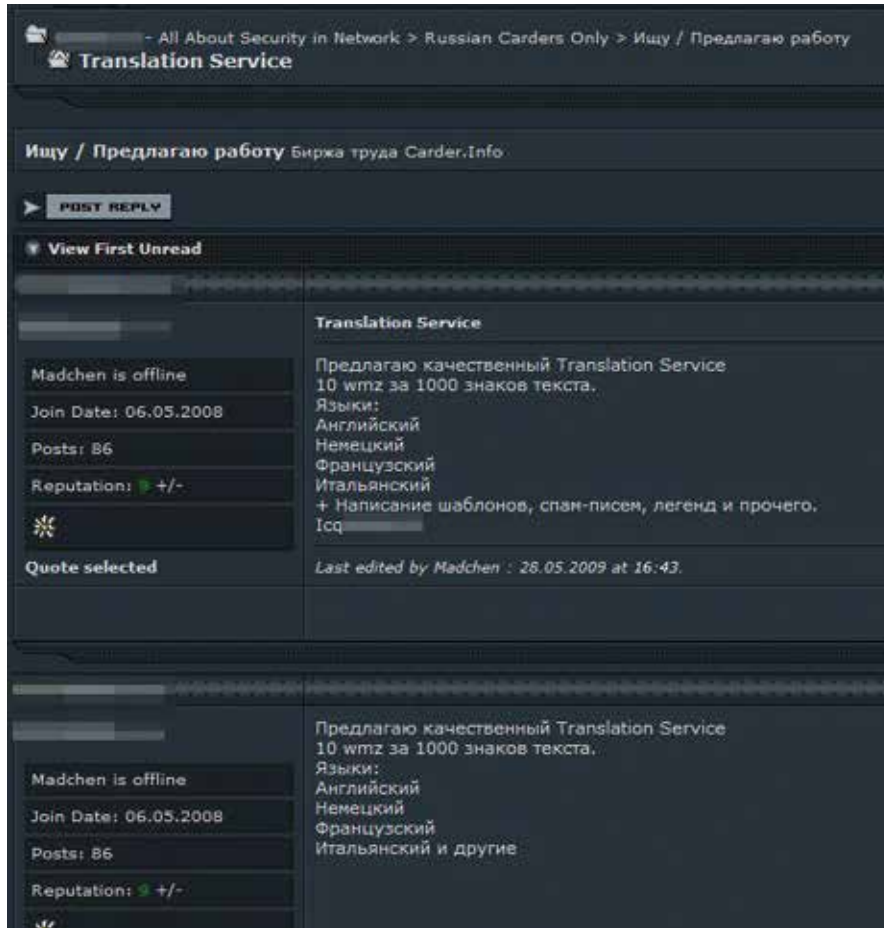


Figure 4. Translation services for hire.

Malware services

Numerous malware variants are available for sale. 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 (such as providing credit card details). Such software is available for sale within the underground market.

Exploits

As we mentioned earlier, 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 toolkit, for example, charges by the day, recently advertised for \$150 per day.

Figure 5 shows the sale of such exploits. This illustration includes the details of the targeted system, a brief description, and its price. Also of interest are prices, which closely align with the potential impact of the exploit. Those classified as high impact are approximately three times as expensive as those classified as low/moderate.





0 [CVE-2012-3558] Opera Web Browser 11.64 Address Field Spoofing Unspecified vulnerability in Opera allows remote attackers to spoof URL into the location bar. Credit to Jordi Chancel Low/Moderate  200\$
0 [CVE-2012-1924] Opera 11.61 High Remote Code Execution When the download dialog is displayed, it should always be visible to the user, to ensure that the user realizes it is there. If the dialog is displayed in a small enough window, the user may not realize it is being displayed, and if the right keyboard sequence is carefully followed, they can end up running a downloaded executable. Additional social engineering steps are needed to ensure that the user presses the correct key sequence, without being able to show any relevant visual feedback, as the page cannot see that the keys are being pressed High  600\$
0 [CVE-2012-1925] Opera 11.61 Remote download and execution vulnerability Dialogs such as the download dialog are usually displayed on top of page content, to ensure that the user knows that the dialog is requesting attention. In some cases, this policy was not implemented correctly in Opera, allowing certain page content to overlay the dialog. In these cases, clicking the page content causes the dialog to be clicked instead. While an attacker may not have much control over the appearance of the overlapping content, they may be able to use it to trick the user into performing harmful actions, such as running a downloaded executable High  600\$
0 [CVE-2012-1928] Opera 11.61 Address Bar Spoofing The address field should always show the address of the page that is being displayed. In certain cases, if a target site responds slowly, reloading an attacking page and redirecting to the target page can cause the address field to show the target site's address, while the attacking site is still being displayed. Low/Moderate  200\$

Figure 5. Exploits for sale—the higher the impact, the higher the price.

There are also exploit packs that offer encryption services used to conceal an attack and avoid detection. This may include encrypting particular files, which may be used in conjunction with other techniques using encryption to further disguise the malicious code. An example of such exploit packs, with the crypter capability as an additional feature, is depicted in Figure 6.



Figure 6. Exploit packs come with add-ons.

Another available service is checking files against security software. Cybercriminals want to ensure that all of their hard work is not blocked at the first hurdle by antivirus software. Services such as those in Figure 7 illustrate that rather than going through the arduous process of buying, installing, updating, and testing their malware against antivirus software, attackers have an alternative, more efficient option. In this instance, the service providers test the malware against 35 antivirus vendors' solutions. In addition, they provide a service that tests the sending domain against a known list of domain blacklists. Such lists are used by companies and service providers to block email from domains that are known to send content against their policies, such as spam.

We mentioned earlier the low cost of cloud computing when compared with internal services, and an association with cybercrime. The prices quoted in the bottom right of Figure 7 undoubtedly validate that assertion. At a cost of \$30 per month, and only \$0.15 per check, the outsourced service proves not only cost effective but also efficient in terms of time spent. The implications of such a service are very clear: the bad guys have the opportunity to ensure that their malware is better and more likely to succeed, which will have significant ramifications for all Internet users.



Figure 7. The low cost of cybercrime services.

Within this category a number of products and services are available for sale, and, more recently, for rent. Potential buyers can engage in as much or as little activity (such as programming or researching) as they like, with the only constraints being how deep their pockets are, their technical competence, and available time. In some instances, certain services in this category are not illegal, with commercial companies offering their expertise on public forums.

Cybercrime Infrastructure-as-a-Service

A number of infrastructure services are available to support a cybercrime operation. These range from the availability of services to conduct DoS attacks to hosting malicious content.

Botnets

A robot network, or botnet, is a network of infected computers under the remote control of an online cybercriminal. The botnet can be used for a number of services, such as sending spam, launching DoS, and distributing malware.

Figure 8 illustrates the cost of renting a botnet and the flexible options available. In effect, multiple services are available to suit any budget.

10- th version.

Packages:

â€¢ Minimum: DDoS Bot, no free updates, no modules = \$450
â€¢ Standart: DDoS Bot, 1 month free updates, password grabber module = \$499
â€¢ Bronze: DDoS Bot, 3 months free updates, password grabber module, 1 free rebuild = \$570
â€¢ Silver: DDoS Bot, 6 months free updates, password grabber module, 3 free rebuilds = \$650
â€¢ Gold: DDoS Bot, lifetime free updates, password grabber + "hosts" editor modules, 5 free rebuilds, 8% discount on other products. = \$699
â€¢ Platinum: DDoS Bot, lifetime free updates, password grabber, unlimited free rebuilds, 20% discount on other products. = \$825
â€¢ Brilliant: DDoS Bot, lifetime free updates, unlimited free rebuilds, all modules for free, 25% discount on other products. = \$999

Other:

â€¢ ReBuild (URLs changing) â€" \$35.
â€¢ Sources - ~3500-5000\$, discuss individually
â€¢ New features - discuss individually.
â€¢ Web-Panel reinstalling (1st time is free) - \$50

Figure 8. Botnet services.

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 are illustrated in Figure 9. Other individuals may provide considerably more options and with different pricing structures. This is illustrated with the services provided by an individual known as Matad0r, who provides 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 mean a higher price. This demonstrates that, much like the commercial environment, a myriad of hosting services are available—the only constraint is the amount of money one is willing to pay, and, in some cases, the ethics of the hosting provider.

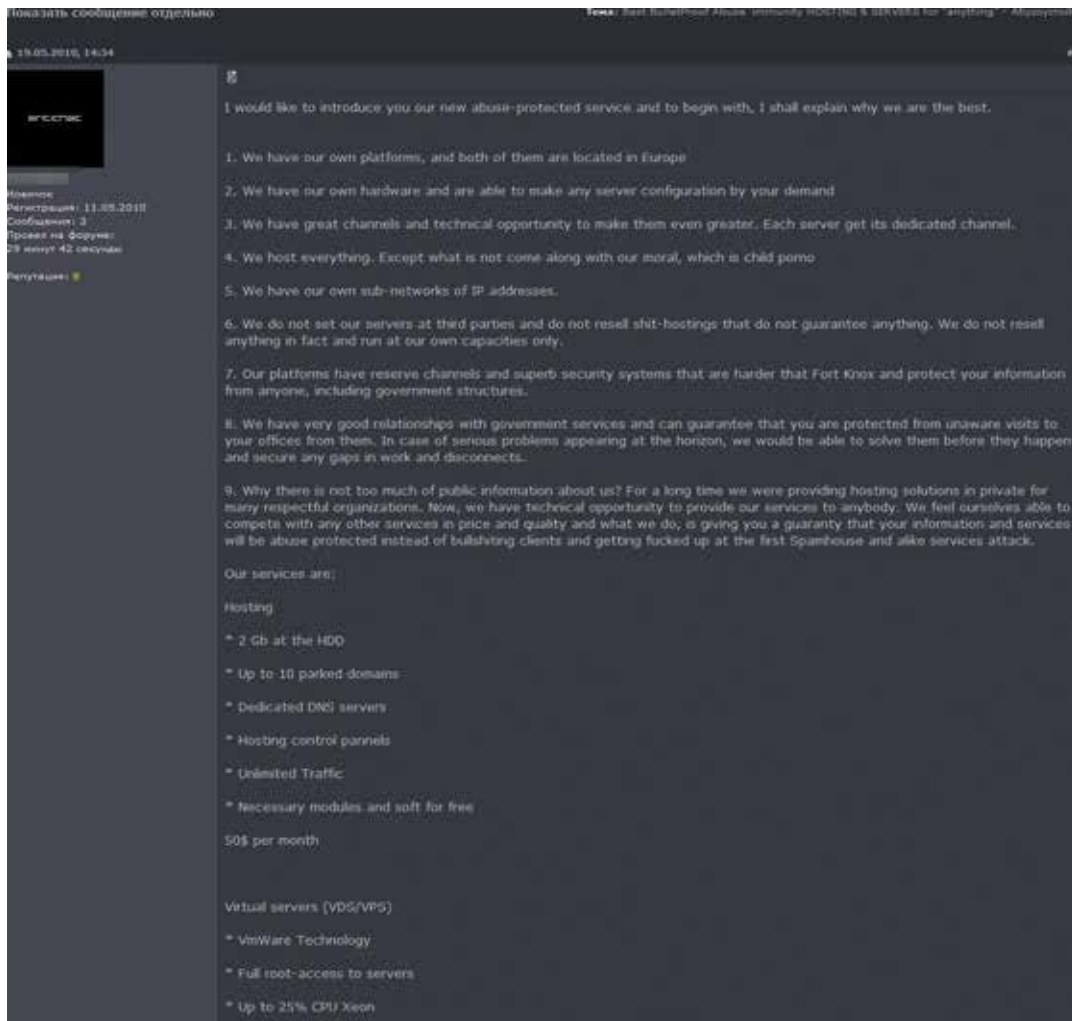


Figure 9. Secure hosting.

Spam services

Numerous services are available for the would-be spammer. These include the availability of services that support the sending of unsolicited mail, alternatively known as a mail relay. Figure 10 shows a service capable of sending 30,000,000 emails. What is particularly relevant is how the proposition is presented. The service offers a live chat option with a customer service agent, as well as payment options many of us are accustomed to in the legitimate world. The “as-a-service” nature of the proposition is further emphasized by the fact that the would-be cybercriminal is provided the relay for just one month (with an upper limit of 30,000,000 emails).

The screenshot shows a website interface for a spam service. On the left, there is a sidebar with a 'Log in' button, a 'LIVE CHAT' section with a woman's profile picture and the text 'Offline now. Leave a message. Send Here', and a 'CATEGORIES' list including various email lists (2012 Business, Country, Domain, General Global, Men's, Targeted, Woman), 'Discounted Price', 'Email Marketing Campaigns', 'Mass Email Software', and 'Smtf Relay Server'. The main content area has a breadcrumb trail: 'Home > Smtf Relay Server > Smtf Relay Server for 30 000 000 emails'. Below this is the title 'SMTP RELAY SERVER FOR 30 000 000 EMAILS'. A diagram illustrates the email relay process: 'Sender's SMTP Server' connects to 'Recipient's SMTP Server', which in turn connects to 'Recipient's Backup SMTP Server #1' and 'Recipient's Backup SMTP Server #2'. The connection is labeled 'SMTP'. To the right of the diagram, a text box states 'Smtf Relay Server for 30 000 000 emails for the one month'. Below this, a price section shows 'PRICE LOWERED!' with the current price '\$13,340.25 tax incl.' and the original price '\$14,822.50 tax incl.' (price reduced by 10 %). A quantity selector is set to '1', and the availability is '999 items in stock'. There are buttons for 'Add to cart' and 'Add to my wishlist'. At the bottom right, there is a 'PayPal' logo with the text 'Click here to pay'. At the bottom center, there is a small diagram showing a network of servers and connections.

Figure 10. This spam service offers support, just like many legitimate online offers.

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 is covered 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 cyberattack by choosing a service that will outsource the entire process.

Password cracking services

There are a multitude of services available within the Hacking-as-a-Service category. The following examples illustrate how little technical knowledge is required for buyers try their hand at cybercrime. Figure 11 illustrates a service that makes it easy for a buyer to retrieve an email password—with no technical expertise. In this example, all that is required is the email address and name of the target. After that, all that remains to be done is enter the password and pay for the service.

The screenshot shows a website interface for 'Email Password Cracking made easy..!!'. The navigation bar at the top includes links for 'Home', 'Cracking', 'Order', 'Faqs', and 'Contact'. The main content area is titled 'Request an E-mail Password :-' and contains the following text: 'Fill in the below form to the best of your knowledge. Make sure that the email addresses are entered correctly. Once submitted, check your email for a confirmation mail. Add our email address(es) in your address-book, to prevent our emails and the proofs landing in bulk folder. Once you verify the order by clicking on the confirmation link sent to you, we will process your order.'

The form includes the following fields and options:

- Your Name**: Text input field.
- Your Email Address**: Text input field.
- Confirm your Email Address**: Text input field.
- Your Country**: Text input field.
- Urgency**: Three radio buttons labeled 'Most Urgent', 'Urgent', and 'Just do it whenever you can'.
- Victim Name**: Text input field.
- Victim Email Address**: Text input field.
- Confirm Victim Email Address**: Text input field.
- Victim Country**: Text input field.
- Victim Language**: Text input field.
- Optional Information :-**: A section containing several text input fields:
 - How you know us**
 - Your Yahoo! Chat ID**
 - Your MSN Chat ID**
 - Preferred Mode of Payment**
 - Bonus offered (if any)**
- Any Instructions ?**: A large text area with a vertical scrollbar.
- Submit your Order**: A prominent button at the bottom of the form.

Figure 11. Need an email password? It's as simple as providing address, name, and payment.

What is really surprising is that the service providers remind their buyers about the junk (bulk) email folder. Such a simple reminder illustrates how the level of technical expertise required for this new breed of cybercriminal is incredibly low.

Denial-of-service

Much of 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 attacks (or distributed denial-of-service [DDoS] attacks). These DoS services aim to send a huge volume of traffic to the victim and prevent them from conducting normal business operations.

Building a cyberarmy 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 “as-a-service” cybercrime market is there to help. Figure 12 shows the price list for a “Cheap Professional DDOS Service.” This service simply requires attackers 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.

The image is a screenshot of a website for a service called "CHEAP PROFESSIONAL DDOS SERVICE". The website has a dark background with blue and yellow text. It includes sections for service description, pricing, payment methods, contact information, and an about section.

CHEAP PROFESSIONAL DDOS SERVICE

Cheap Professional DDOS Service
Trusted
Strong/Fast Service
Takes down Large Website/Forum/Game Servers etc.
No time limit

PRICE

1 - 4 hours / 2\$ per hour
5 - 24 hours / 4\$ per hour
24 - 72 hours / 5\$ per hour
1 month / 1000\$ fix price

PAYMENT ACCEPTED

Paypal (Verified users only)
Liberty Reserve
Western Union
MoneyBookers

CONTACT

Yahoo Messenger :
Msn :
Skype :

ABOUT

We are here to provide you a cheap professional ddos service.
We can hit most large websites/forums game servers.
We will test the website/server before accepting your money.
Due to the nature of the business we dont offer refunds.

Figure 12. This service offers to launch a DoS attack for a very low price.

What may surprise many of us is the low cost of the service. This may demystify the sophisticated portrayal of today's hacker. For only \$2 per hour, an attack can be launched against the systems of the buyer's choosing. What is particularly interesting is the comment about not providing any refunds. Outside of cybercrime, is there any other criminal activity in which the company that knowingly facilitates the crime feels the need to remind their customers that there are no refunds?

Credit card information

Many services offer credit card information. In many cases, they offer considerable flexibility and varying price models based upon the information sold. An example of prices are depicted in Table 2.

Table 2. Prices for stolen credit card numbers.

Dumps	Estimate of Prices (without PIN, with PIN, PIN and good balance)									
	US			EU			CA, AU		Asia	
Visa Classic	\$15	\$80		\$40	\$150		\$25	\$150	\$50	\$150
Master Card Standard	\$90			\$140			\$150		\$140	
Visa Gold/Premier	\$25	\$100	\$200	\$45	\$160	\$250	\$30	\$160	\$55	\$150
Visa Platinum	\$30	\$110		\$50	\$170		\$35	\$170	\$60	\$170
Business/Corporate	\$40	\$130		\$60	\$170		\$45	\$175	\$70	\$170
Purchasing/Signature	\$50	\$120		\$70			\$55		\$80	
Infinite				\$130	\$190		\$60	\$200	\$190	
Master Card World	\$140									
AMEX	\$40			\$60			\$45		\$70	
AMEX Gold	\$70			\$90			\$75		\$100	
AMEX Platinum	\$50									

The "Dumps" in Table 2 refer to the information that is copied from the magnetic stripe on the back of credit and debit cards. The information includes two tracks of data on the magnetic stripe. Track 1 is alphanumeric and contains the name of the customer and the account number. Track 2 is numeric and contains the account number, expiration date, the secure code (CVV), and discretionary institution data. A third track is rarely used. This is graphically represented in Figure 13.

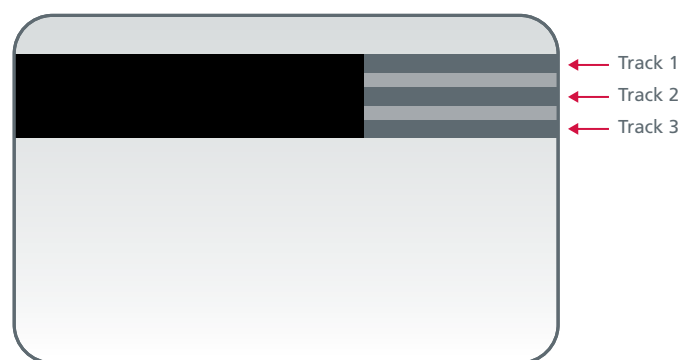


Figure 13. Credit card track data.

Credit card information is valuable to would-be criminals, but there are also considerably more types of financial information that support attacks. For example, also available are the login credentials for online banking. An example of the pricing structure for this type of information is depicted in Table 3.

Table 3. Stolen bank login information commands a higher price than credit card numbers.

Type of Login	Prices
US bank with fullz info	2% of balance
EU bank with fullz	4–6% of balance
PayPal, Moneybookers, Netteier verified	6–20% of balance
Western Union transfer	10% from amount

Conclusion

This white paper offers a view into the reality and size of the cybercrime market. Entire books have been dedicated to providing insights into how hackers have profited from individual services within these broad categories, and there are many other services that have not been included in this paper.

Any paper that purports to be an exhaustive summary of services available on the underground market is likely to be out of date even before the author clicks “save.” This report offers readers a snapshot of the cybercrime market and how its services-based nature supports new entrants who do not require technical expertise. All that the modern cybercriminal needs to provide Cybercrime as-a-Service is a means with a payment method. We are witnessing the emergence of a whole new breed of cybercriminal. As a result, the volume of cyberattacks is likely to increase, and current trends and data suggest that this is exactly what we are seeing today.

About the Authors

Raj Samani

Raj Samani is an active member of the information security industry through his involvement with numerous initiatives to improve the awareness and application of security in business and society. He is currently serving as the vice-president and chief technology officer for McAfee, EMEA, having previously worked as chief information security officer for a large public sector organization in the UK. He was recently inducted into the Infosecurity Europe Hall of Fame (2012).

Samani has worked across numerous public sector organizations in many cybersecurity and research-orientated working groups across Europe, including the Midata Interoperability Board, as well as representing DIGITALEUROPE on the Smart Grids Reference Group, which was established by the European Commission in support of the Smart Grid Mandate. He is the author of the recently released Syngress book, *Applied Cyber Security and the Smart Grid*.

In addition, Samani is currently the Cloud Security Alliance’s strategic advisor for EMEA, having previously served as the vice president for communications in the ISSA UK Chapter, where he presided over the award of Chapter Communications Programme of the Year 2008 and 2009. He is also on the advisory council for the Infosecurity Europe show, *Infosecurity Magazine*, an expert on both searchsecurity.co.uk and the Infosec portal, and regular columnist for *Computer Weekly*. He has had numerous security papers published and appeared on television (ITV and More4) commenting on computer security issues. He has also provided assistance in the 2006 RSA Wireless Security Survey and part of the consultation committee for the RIPA Bill (Part 3).

You can follow Raj Samani on Twitter at http://twitter.com/Raj_Samani.

François Paget

François Paget is one of the founding members of the McAfee Avert group (now McAfee Labs). He has worked there since 1993. In Europe, over a 12-year period, he was in charge of analyzing new threats, identifying them, and making modules available for detecting and eliminating them. His main responsibility was researching new generic and heuristic detection methods for 32-bit Microsoft Windows environments. Today, Paget conducts a variety of forecast studies and performs technological monitoring for his company and some of their clients. He focuses particularly on the various aspects of organized cybercrime and the malicious use of Internet for geopolitical purposes. Paget is active in various partnership actions with French and international authorities involved in fighting cybercrime.

In 1991, he was the leader of the “Virus Group” within CLUSIF (Club de la Sécurité de l’Information Français [French Information Security Club]). As the Secretary-General of this association, Paget is currently involved with their “Threats” team as well as the annual cybercrime overview.

He is a regular conference speaker at various French and international events in this field. In 2006, Paget published a reference work through DUNOD, addressing the current set of malware problems. He is also a contributor for several collective works related to information system security.

<http://blogs.mcafee.com/author/Francois-Paget>

About McAfee Labs

McAfee Labs is the global research team of McAfee. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based service McAfee Global Threat Intelligence™. The McAfee Labs team of 500 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public. <http://www.mcafee.com/labs>

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world’s largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivalled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. <http://www.mcafee.com>



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

¹ <http://www.telegraph.co.uk/finance/personalfinance/consumertips/9579167/UK-worst-in-Europe-for-identity-fraud.html>

² <http://www.wmbfnews.com/story/20972727/robberies-decrease-as-cyber-crime-increases-fbi-says>

³ <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>

⁴ <http://weis2007.econinfosec.org/papers/29.pdf>

⁵ <http://www.crn.com/news/security/172900859/summers-zotob-attack-cost-companies-100k-each-in-cleanup.htm>