Dirty Money on the Wires:
The Business Models of Cyber Criminals

-

Virus Bulletin Conference 2006
Guillaume Lovet

Abstract

Scammers, Phishers, Bot Herders, Spammers, Online Extortioners, Identity thieves... The names may seem obscure, but their intent is not: they are all out to steal our money. It is no secret that today, cyber crime is draining massive amounts of money every year, all around the globe. And while old school hackers would rent their services to conduct a limited number of high-profile industrial spying operations, today's cyber criminals combine social engineering, viruses, trojans and spyware to target average, everyday users.

There are several questions that we must try and understand in order to fight these cyber criminals: who are the culprits and do they fit any standard profile? What is their business model and how easy is it to set up? Through which channels is the cyber crime money flowing and who is getting this money, eventually? Is the "real" organized criminals -the so called mob- implicated at certain levels in the model?

This paper will attempt to shed some light on these questions. Answers will be developed, correlated and backed up by concrete data, numbers, and figures.

The expected proliferation of increasingly used mobile smart phones will open the door for a broad range of new cyber crime possibilities and business models, which this paper will also examine. The goal is to raise public awareness and industry anticipation of this potentially severe issue.

Definition

Cybercrime is a term used broadly to describe criminal activity in which computers or networks are involved, regardless the level of such an involvement (source, target, means...). This paper focuses more specifically on cyber criminals involved in schemes that rely tremendously on the internet: carding, phishing, herding, spyware planting, industrial spying, and online extortion.

Introduction

Gauging the economic impact of cybercrime is by no mean an easy task, for reported offenses are merely the tip of the iceberg. Indeed, the general consensus suggests that only a third of the victims report to the police. However, various estimations give a good idea of how gargantuan is the cybercrime business today:

For instance, a report carried out by the FBI revealed that cyber-crime caused $67 billion in damages in the US alone, last year. Britain's National Hi-Tech Crime Unit (NHTCU), at the same time, estimates the nation's cost of computer crime in 2005 at 2.45 billion pounds ($4.6 billion) a year. And then again, there is this famous quote by Valerie McNiven, who advises the U.S. Treasury on cybercrime: "Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion," [1]

Additionally, credit card fraud alone is generally thought to cost some 400 million dollars every year - and virus attacks some 12 billion. Profits lost by firms whose patents and trademarks are stolen reportedly amount to 250 billion dollars every year, or nearly 5% of world trade.

All those figures are prone to give a little vertigo to most of us, and undeniably call for a more detailed breakdown: What is cyber crime, who does it profit to, how and where ?

I. Cybercrime zoology

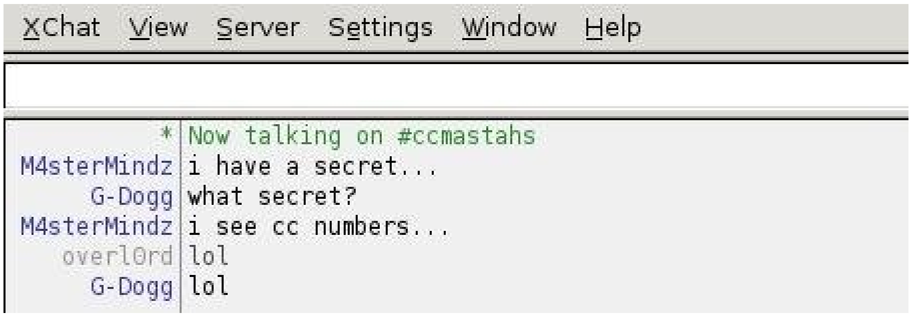
As a matter of fact, cybercrime is an umbrella term for various malicious online activities prone to generate financial profit, generally at the expense of a target organization or person. Albeit non-exhaustive, the following list of categories help classify such activities:

1.1. Spamming

Spamming, is, unfortunately, a global pestilence every user is - very unwillingly - familiar with today. Therefore, a mere definition (featured in Wikipedia's article about spamming, see [2]) should suffice: Spamming is commonly defined as the sending of unsolicited bulk e-mail - that is, email that was not asked for (unsolicited) and received by multiple recipients (bulk).
Since this topic has been widely addressed in various papers already, business models relative to spamming will not be examined here.

1.2. Carding

Credit card frauds over the Internet are often called "Carding" in the cyber criminals jargon. This activity has been flourishing on IRC chat rooms for years, following the skyrocketing curve of online shopping. Indeed, stolen Credit Card information originates, by large, from compromised online shops keeping databases of their customers credentials. A "full cc" usually refers not only to the credit card number, but also to all the related information, such as the card verification value number (aka the CVV, i.e. the 3 non-embossed digits usually appearing on the back of the card), cardholder name, address, and sometimes Social Security number and driving license number. In some cases, the PIN code is also part of the package. Since online shops do not equire customers to enter their PIN code, it is a strong sign that this CC was acquired via a Phishing scam (see below).
Every day, millions of "fresh cc" are traded by cyber criminals (calling themselves "carders") over the internet.



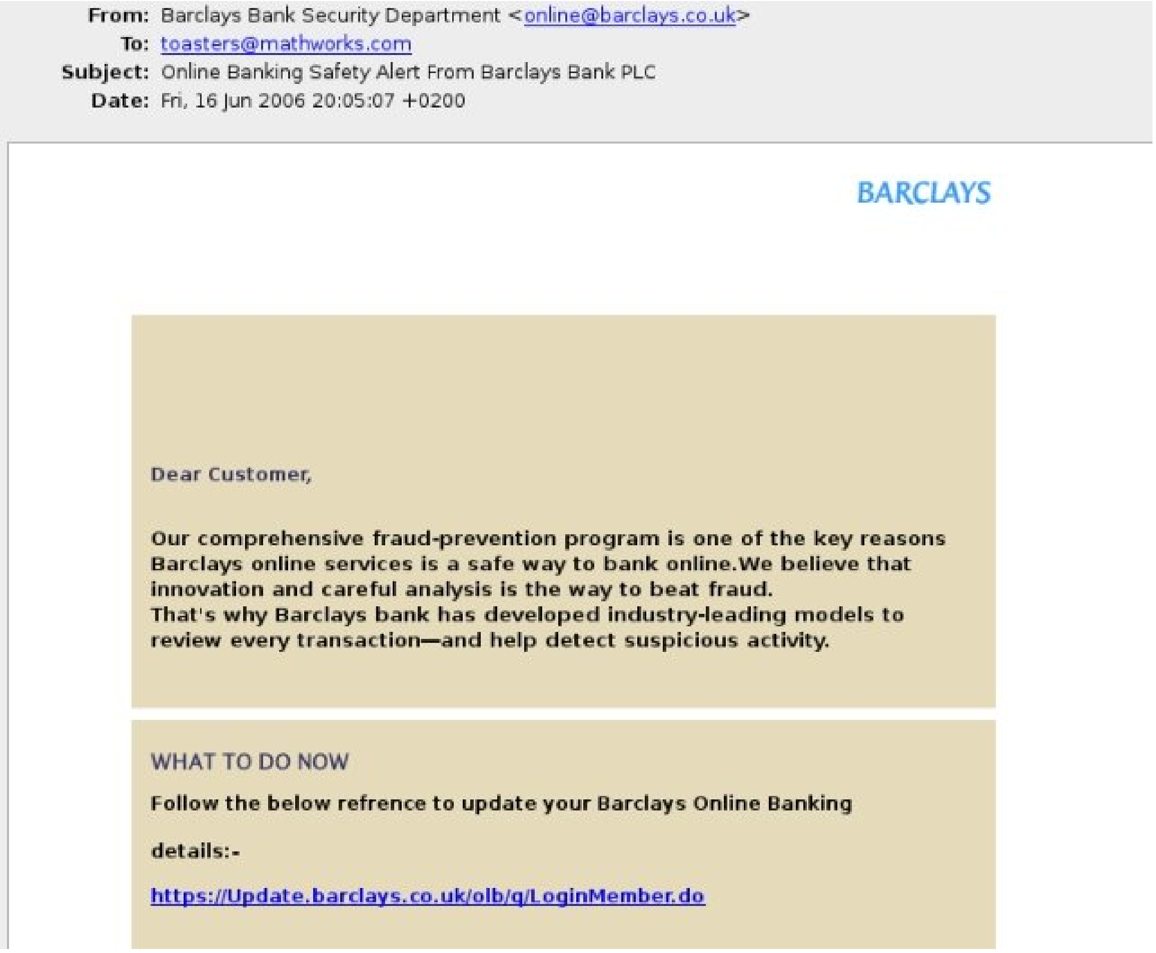
```
          * Now talking on #ccmastahs
M4sterMindz i have a secret...
     G-Dogg what secret?
M4sterMindz i see cc numbers...
    overl0rd lol
     G-Dogg lol
```

Figure 1: carders channel

1.3. Phishing

Phishing is characterized by attempts to fraudulently acquire sensitive information, such as passwords and online banking login credentials of targeted individuals. According to Wikipedia, this is generally done by masquerading as a trustworthy person or business in an apparently official electronic communication. Typically, an e-mail.

A typical phishing e-mail would be:



From: Barclays Bank Security Department <online@barclays.co.uk>
To: toasters@mathworks.com
Subject: Online Banking Safety Alert From Barclays Bank PLC
Date: Fri, 16 Jun 2006 20:05:07 +0200

BARCLAYS

Dear Customer,

Our comprehensive fraud-prevention program is one of the key reasons Barclays online services is a safe way to bank online.We believe that innovation and careful analysis is the way to beat fraud.
That's why Barclays bank has developed industry-leading models to review every transaction—and help detect suspicious activity.

WHAT TO DO NOW

Follow the below refrence to update your Barclays Online Banking

details:-

https://Update.barclays.co.uk/olb/q/LoginMember.do

Figure 2: phishing letter

Upon clicking on the advertised hyperlink, the targeted users are directed to a fake banking site mimicking the bank login page.

The stolen credentials are usually directly sent to the "phisher"'s email address, rather than stored on the server (which is usually a hacked host, toward which a DNS redirection with a legit-looking domain name has been added)

1.4. Herding (short for botnet herding)

Botnets have received tremendous media attention along the past year, and were often presented (including by the author himself, in his AVAR 2005 paper [3]) as the Epicenter of cyber criminal activity today. Again, for our matters of interest, a short outlook will suffice:

"Botnet is a jargon term for a collection of software robots, or bots, which run autonomously. [...] The word is generally used to refer to a collection of compromised machines running programs (usually referred to as worms, Trojan horses, or backdoors) under a common command and control infrastructure. A botnet's originator can control the group remotely, [...] usually for nefarious purposes. [...] Often the command and control takes place via an IRC server or a specific channel on a public IRC network." [4]

For in-depth (technical and non-technical) details, please refer to the very good papers by Martin Overton [5] and The Honeynet Project & Research Alliance [6].

Among other activities, botnets are extensively used in Online Extortion schemes and Spyware planting operations. Both of which will be developed in the Business Models section below.

1.5. Industrial Spying

Of course, industrial spying is not new. As a matter of fact, it is as old as industries themselves - while the use of the internet to achieve it is, again, probably as old as the internet itself. Traditionally, this has been the reserved hunting field of a few hundreds of highly skilled hackers, contracted (often for several hundreds of thousands of dollars, depending on the "assignment") by high-profile companies or certain governments via the means of escrow organizations. However, with the growing public availability of Trojans and Spyware material, even low-skilled individuals are now inclined to generate high volume profit out of industrial spying. This is often referred to as "Targeted Attacks" (which includes "Spear phishing") in the press. This aspect of Industrial Spying is the one to be addressed in the Business Models section of this paper.

II. Cyber criminals profiles

Cyber criminals are rarely involved at all levels in such activities. Similarly to "real-life" organized crime, the cyber criminal schemes rely on different categories, or "layers" of culprits. As a matter of course, some individuals do not clearly fit in one single category, but the classification below does give a good idea of what the basic pieces in the cyber crime jigsaw are.

2.1. Coders

The "skilled" guys, aged between 20 and 25 years old, generally holding an experience of 5+ years in the hacking community - though not necessary on the front scene. Young self-made programmers, or professional coders looking for side incomes, generally from a country where $300 a month will make a difference which is significant enough to take a little risk.
To simplify, they sell ready-to-use tools (Trojans, mailers, custom bots), or services (making a binary undetectable to AV engines), to the cyber crime labour force (the "kids", below), charging fees that are generally in the hundreds of USD. By staying at the supply only level, the risks they take are very limited; they systematically attempt to back themselves up with "I am not responsible for the use of this educational tool. Do not use to spam / hack / trojanize".
Scam artists, who craft and sell Phishing scam letters and scam pages, though not necessary technically gifted, can reasonably be classified into this category.

2.2. Kids

The genuine labour force of the cyber crime scene. Aged between 15 and 20, they massively hang around IRC carding channels, where most of them try to make small profit on buying (or trading), then re-selling the elementary bricks needed to set up effective scams: spam lists, php mailers, proxies, cc, hacked hosts, scam pages, etc... They show no hesitation to rip their "customers" off, and their small traffic merely generate 2 digits monthly incomes - when they do not end up ripped off themselves. However, there is no denying that $20 a month is worth the time spent online, when you are a teenager living in, say, Ukraine.

A few percentage of them - typically the most clever and experienced ones - actually "do something": building botnets, setting up phishing scams, harvesting CC by the mean of simple web page exploits targeting vulnerable online shops, and so on. As a matter of course, kids from the first sub-category (described above) constantly try to find someone from the "doers" sub-category to become their Mentor. Since they have few to offer, and granted for a potential mentor, forming another "doer" would only bring a competitor on the market, only the most socially gifted actually succeed in that quest.

2.3. Mob

Bringing in-depth inputs about the real mafia while staying within the strict boundaries of the law raises complex issues for an isolated researcher. Additionally, bigger investigation means, field presence and years-long infiltration commitments would certainly be needed. The author leaves it to the competent authorities, yet, it is no denying that crime syndicates involved in traditional "activities" are one of the cyber crime back ends; this will be addressed in the phishing business model below.

2.4. Drops

Generally significantly older than kids, "drops" play an essential role on the cyber crime scene. It's one of the main point where "virtual" money (stolen online bank logins, paypal accounts, eCurrency accounts...) is converted to real cash. They offer cyber criminals the opportunity to transfer stolen funds to their own, legal bank account. Once it has been done, they keep a percentage (usually 50%) of the transferred funds, and wire back the other 50% to the

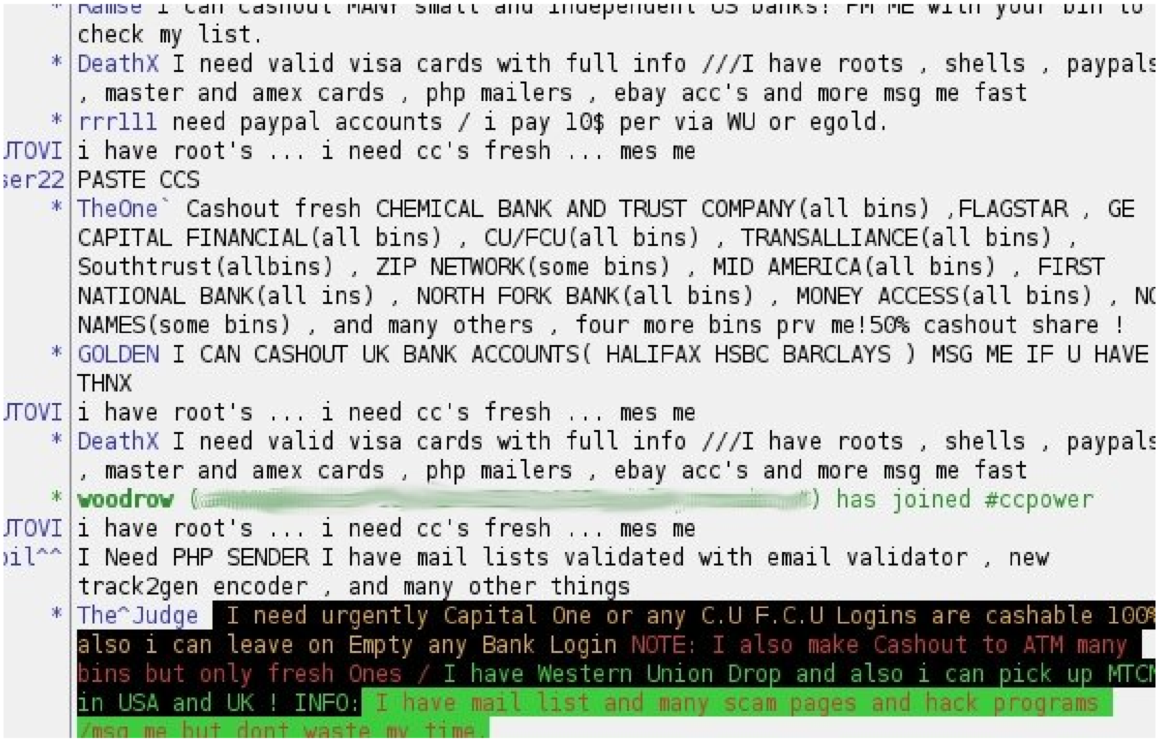
cyber criminal in cash (there are several international services for that: Moneygram, Western Union, etc...). Or at least they claim to do so... Rips off, again, are common in such transactions, since the cyber criminal originating the transfer has no real real guarantee that the "drop" will wire the cash back.
Thus, as it is always the case in similar social configurations, Webs of Trust are being naturally created. Cyber criminals want to establish a relation of trust with their "drop", and tend to systematically use the same one, once it has been proven to be a "legit one", and possibly share the "drop" with "friends".

The main requirement for being a "drop", besides having a bank account, is to reside in a country that does not have laws about digital acts (or loose policies about them), by this way effectively ignoring the notion of cyber crime. Popular countries that fall in that category are Indonesia, Malaysia and Bolivia.

In the USA themselves the Anti-Phishing Act has been introduced in 2005 only.

III. Business models, or how this little world cooperate

3.1. The marketplace



```
   * Ramse I can cashout MANY small and independent US banks! PM ME with your bin to
     check my list.
   * DeathX I need valid visa cards with full info ///I have roots , shells , paypals
     , master and amex cards , php mailers , ebay acc's and more msg me fast
   * rrr111 need paypal accounts / i pay 10$ per via WU or egold.
JTOVI i have root's ... i need cc's fresh ... mes me
ser22 PASTE CCS
   * TheOne` Cashout fresh CHEMICAL BANK AND TRUST COMPANY(all bins) ,FLAGSTAR , GE
     CAPITAL FINANCIAL(all bins) , CU/FCU(all bins) , TRANSALLIANCE(all bins) ,
     Southtrust(allbins) , ZIP NETWORK(some bins) , MID AMERICA(all bins) , FIRST
     NATIONAL BANK(all ins) , NORTH FORK BANK(all bins) , MONEY ACCESS(all bins) , NO
     NAMES(some bins) , and many others , four more bins prv me!50% cashout share !
   * GOLDEN I CAN CASHOUT UK BANK ACCOUNTS( HALIFAX HSBC BARCLAYS ) MSG ME IF U HAVE
     THNX
JTOVI i have root's ... i need cc's fresh ... mes me
   * DeathX I need valid visa cards with full info ///I have roots , shells , paypals
     , master and amex cards , php mailers , ebay acc's and more msg me fast
   * woodrow ([redacted]) has joined #ccpower
JTOVI i have root's ... i need cc's fresh ... mes me
oil^^ I Need PHP SENDER I have mail lists validated with email validator , new
     track2gen encoder , and many other things
   * The^Judge  I need urgently Capital One or any C.U F.C.U Logins are cashable 100%
     also i can leave on Empty any Bank Login NOTE: I also make Cashout to ATM many
     bins but only fresh Ones / I have Western Union Drop and also i can pick up MTCN
     in USA and UK ! INFO: I have mail list and many scam pages and hack programs
     /msg me but dont waste my time.
```

Figure 3: the marketplace

All these "elements" of the puzzle find each other on the main cyber crime marketplace, that is to say IRC.

IRC stands for Internet Relay Chat, and, according to Wikipedia [7], "is a form of instant communication over the Internet. It is mainly designed for group (Many-to-many) communication in discussion forums called channels, but also allows one-to-one communication. [...] An IRC server can connect to other IRC servers to expand the IRC network. Users access IRC networks by connecting a client to a server".

Popular IRC client software are mIRC (Windows) and X-Chat (Linux).

IRC has been part of the Global Village since 1988. Users profiles and origins are highly mixed, although IRC has traditionally been associated with hacking groups. It is best defined as a parallel society, with codes, rules, idols, masters and stories.

Many cyber criminal related channels are publicly accessible, though high-profile ones are typically on "invite only" mode.

An important point to note is that unlike on most IM systems, the IP addresses of IRC users are public to every other users. Since most of them, especially in the cyber crime scene, want to remain anonymous, proxies are heavily resorted to. Socks proxies, shell redirection, or even simple TCP redirection can be used, but a lot of users opt for proxies dedicated to the IRC protocol, with advanced functionality. Such proxies are informally known as "bouncers", the most popular one being PsyBNC.

Due to the generally loose control of all the nodes (i.e., the servers) that form an IRC network "legit-ness", confidentiality on IRC is highly debatable. Notably, tools logging every single message sent to any channel over an IRC network do exist. Bearing that in mind, IRC is still a great place for cyber criminals to initiate contacts and transactions, that are then being pursued over private IM networks; most kids will happily do business on Yahoo Messenger or ICQ, while coders usually prefer protocols with native support of encryption (e.g. Jabber clients such as Psi).

Numerous web forums are also used as carding marketplaces (CCpowerForums.com is a popular one), although the persistence of messages is a barrier to most serious cyber criminals, who generally opt for IRC instead.

3.2. The currency

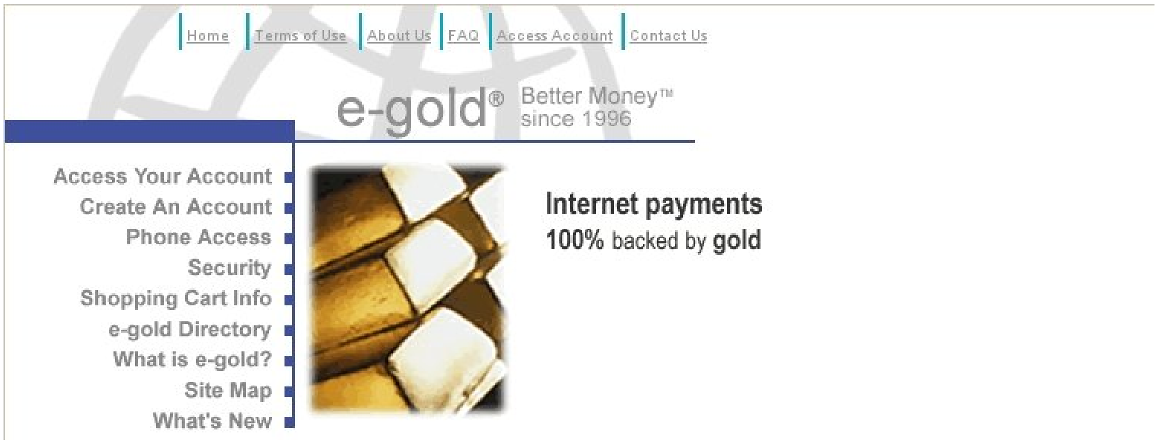


Figure 4: www.e-gold.com

e-gold is a digital gold currency operated by Gold & Silver Reserve Inc. under e-gold Ltd., and is a system which allows the instant transfer of gold ownership between users [8]. Typically, large accounts are owned by so called "Gold Bugs", i.e. people who have a pessimistic view of the fiat currencies (money whose purchasing power derives from a declaratory fiat of the government issuing it: USD, GB Pound, Euro, Yen) stability and prefer to invest in gold; however, the ease of use associated with e-gold transactions has made it a rather universal means of payment.

Discussing the inner workings, advantages or flaws of the e-gold system is not the main goal of this paper, yet, the specific features that make it a currency of choice to cyber criminals have to be underlined:

- **Anonymity**: Creating an e-gold account takes less than a minute, and only requires a couple of mouse clicks. No valid e-mail is requested, and although users are required to enter a name, this name is not checked by any means. IP addresses are logged, yet the simple use of a proxy make this measure essentially useless as a user tracking means. Conclusion: e-gold accounts are anonymous.

- **Irreversibility**: Unlike popular online payment systems such as Paypal, all transactions (called "spends") over e-gold are irreversible. The company enforces this policy, even in case of user mistakes.

- **Independence**: e-gold Ltd. was originally registered in Nevis (West Indies) in 1999, but was removed from the register in 2003, due to non-payment of "fees". It therefore appears to be an unregistered entity, not clearly bound to any country's authority. That feature, however, has to be mitigated by Chairman and founder Dr. Douglas Jackson's recent statement in a public letter: "e-gold operates legally and does not condone persons attempting to use e-gold for criminal activity. e-gold has a long history of cooperation with law enforcement agencies in the US and worldwide, providing data and investigative assistance in response to lawful requests.[...] Our staff has participated in

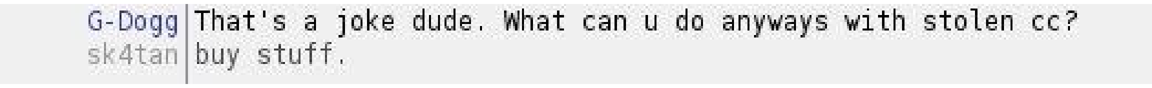
> hundreds of investigations supporting the FBI, FTC, IRS, DEA, SEC, USPS, and others." [9]

Although e-gold is probably the most emblematic of all, other e-currencies are of course widely used in cyber criminal deals. Beyond those, very popular means of payment are wired money transfers; such services are offered by companies such as Western Union or MoneyGram, to cite the most popular ones. The scheme is simple: Individual A deposits some cash in one of the wired money transfer company's office, along with the coordinates of individual B. Individual B can then show up at any of the company's office in the world, and with the transaction number (sent directly to him by A) and an ID, is delivered the cash (needless to say, minus a transaction fee).

Again, this is by very nature, irreversible, it crosses borders almost instantly, and it's fairly anonymous. Indeed, although in theory an ID is asked to the recipient for cash delivery, in practice offices in some countries operate a "light" ID checking - or even no checking at all. Such countries are, for instance, Brazil, Russia, Ukraine and most of Africa. This may sound as a shockingly loose policy at first, however, bearing in mind the fact that in some countries IDs are not mandatory (and most people can't afford them), it follows a certain logic.

Both e-gold and wired money transfer agencies are not tied to cyber criminality per se; they are used for totally legal deals, as well as for criminal deals that have no link with internet-related scams. For instance, both have frequently been under the presumption of essentially being money laundering instruments, due to the nature of the features they offer.

3.3. Carding business model



```
  G-Dogg | That's a joke dude. What can u do anyways with stolen cc?
   sk4tan | buy stuff.
```

Figure 5: the bare truth

As mentioned earlier, thousands of credit card full information - sometimes including the owner social security number - are stolen everyday. On most networks, a "CC full" costs between $2 and $5, payable by e-gold. There is, of course, no guarantee that such CC are valid... As a matter of fact, most carders I have talked to estimate that about 80% of all CC traded on IRC are not valid. Thus, again, webs of trust involving buyers and sellers play an important role.

I noticed that buyers rarely purchase one single CC; rather, CC are bought by bunches of 10 to 100+. The deal then resembles a drug deal: the seller provides a "sample" (one CC) to his buyer, who verifies it. If the sample appears to be valid, the buyer then buys the whole bunch. The "safest" way to verify of a CC consists in debiting its associated account by a few pennies, although some online checking services with a highly variable accuracy do exist.

CC buyers seem to use them for either one of these two reasons:

3.3.1. "Buy stuff" online

A site where cyber crooks can "buy stuff" online with a stolen credit card info is called in the jargon a "cardable" site. Cardable sites are online shops which do not require billing and delivery addresses to match, hence allowing goods to be purchased with a stolen card and shipped to a "drop".

While the average carder will find and bribe such a drop for punctual operations (to buy a laptop, a t-shirt, etc...), some criminal organizations go as far as turning this into a full-time business. They recruit drops via phony job offers sounding like the letter presented in appendix (this one is for a paypal drop however, not for a package drop).

Cyber criminals buy goods online, get them delivered to drops, drops forward packages to cyber criminals, and goods are sold on eBay.

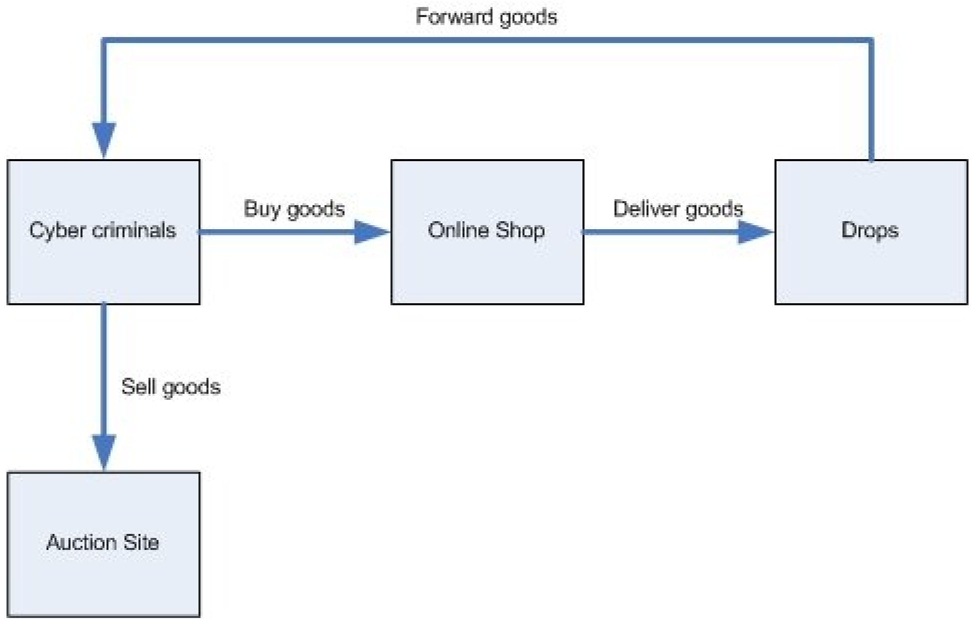


Figure 6: using drops

Such a business model monthly profitability can be estimated thanks to the following example of costs / profits break down, which considers a monthly roll-over of 40 packages:

Costs

- Buying 40 valid CC info: **$200** [Need to buy 100 cc at $2 each from a trusted seller to have about 40 of them usable]
- Bribing 10 drops to forward one package per week: **$800** [at the rate of $20 per package]
- Drops to cyber criminal packages delivery costs: **$800**
- Profits
- Selling the goods on eBay: **$16,000** [Averaging value of $400 per package, some being more (eg: laptops), some being less (eg: clothes)]

Total Cost, monthly: **$1,800**
Total Profit, monthly: **$16,000**
Net Gains, monthly: **$14,200**
Productivity index (Profits/Costs): **8.9**

As a matter of course, this is just an example. Profits can be maximized by resorting to a more aggressive roll-over pace. In that case, however, chances to stay "under the radar" of international justice are being exponentially reduced. As for nearly all cyber criminals business models, there is a typical trade-off between profit and chances to get caught.

3.3.2. "Buy stuff" in real stores (aka "instore carding")

This strategy has been around since the early 90s - when online shopping was still non-existing - and as such, can be fairly deemed "Old School". Back then, carders would trade what they would call "dumps". In the carding jargon, a dump is a digital copy of the information contained in the magnetic tracks of credit cards, and is generally collected by the infamous ATM Skimmers - those electronic devices crooks append to ATMs.

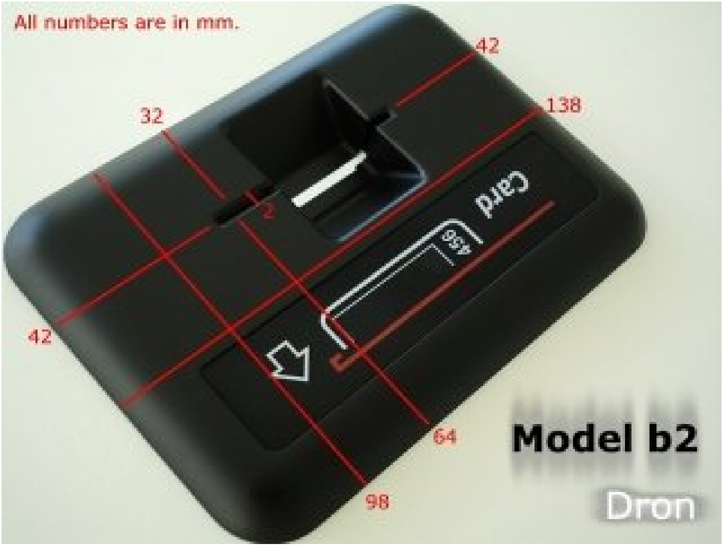


Figure 7: Skimmer

Collected dumps were then sold and encoded back onto fake credit cards (called "plastics") with a device called a Magnetic Stripe (or Card) Writer. Purchases in shops - only limited to the cloned card balance limit - could then be done with such fake cards. In case the PIN has been collected as well (by a fake keypad on the ATM, a camera, shoulder snooping...), cash could be retrieved as well.

Today, skimmed dumps are still actively being traded over the internet. However, with a simple CC info stolen from an online shop database, it is possible to generate a dump, thus in turn to encode a "plastic" with it. Generated dumps are well known to be less reliable than skimmed dumps, but they are also a lot cheaper: less than $10 vs around $80 for a basic Visa Classic skimmed dump.

Figure 8: Plastics	*Figure 9: Magnetic stripe writer*

This leads us to consider the following business model:

Costs

- 20 valid cc info: **$200**
- 20 pastic cards: $60 x 20 = **$1200**
- Magnetic stripe writer: **$400**

Profits

- Considering that 40% of crafted cards will be refused, and estimating an average balance limit of $1000 per crafted cards (Visa classic cards have a balance limit of $500 to $3,500): **$12,000**

Total Cost: **$1,800**
Total Profit: **$12,000**
Gain: **$10,200**
Productivity index (Profits/Costs): **6.67**

3.4. Spyware/Adware planting business model

Among the numerous hands botnet herders have in their game, one of the most juicy one is perhaps to use their armies of Zombies (i.e. infected "slave" machines) to massively install Spyware.

To draw a refined analysis of this business model, it is worth taking a moment to look closer at Adware companies own business model - the two being tightly linked together.
The key role of Spyware/Adware companies - officially calling themselves "behavioral marketing" company - is to provide a central point of meeting for three essential audiences: advertisers, partners (also often called "affiliates"), and users. The business model breaks down to two steps:

1. Advertisers pay the Spyware/Adware company to have their adds displayed to the users (pop-ups, embedded windows, etc...)
2. The Spyware/Adware company pays its partners/affiliates for each install of the Spyware/Adware program they perform onto an end-user computer.

The latter is generally done via bundling the Adware/Spyware program with a "free" software. Morally, there is nothing wrong with such a concept. Users may choose to install free software with the drawback of having advertisements displayed from time to time rather than ad-free expansive software (much like when one is watching TV shows on freely available channels).
However, the "partner" component can very well be the rotten part of the fruit. It is public knowledge in the botnet community that the main source of revenue for Botnet herders today comes from adware/spyware installations they initiate on their herd of compromised computers, which yields "partner" payment from Adware companies. As a matter of course, most adware companies clearly state on their websites how ethical and honest partners must be in order to take part in their partner programs. For instance, BetterInternet has the following guideline page for partners: http://www.bestoffersnetworks.com/partners/guidelines.php
However, a quick examination of Spyware/Adware programs installation statistic figures reveal that the honesty behind such statements is highly questionable. Take, for instance, the Adware program deemed Adware/BetterInternet by Fortinet. The activity report of February, 2006, shows the following figure:

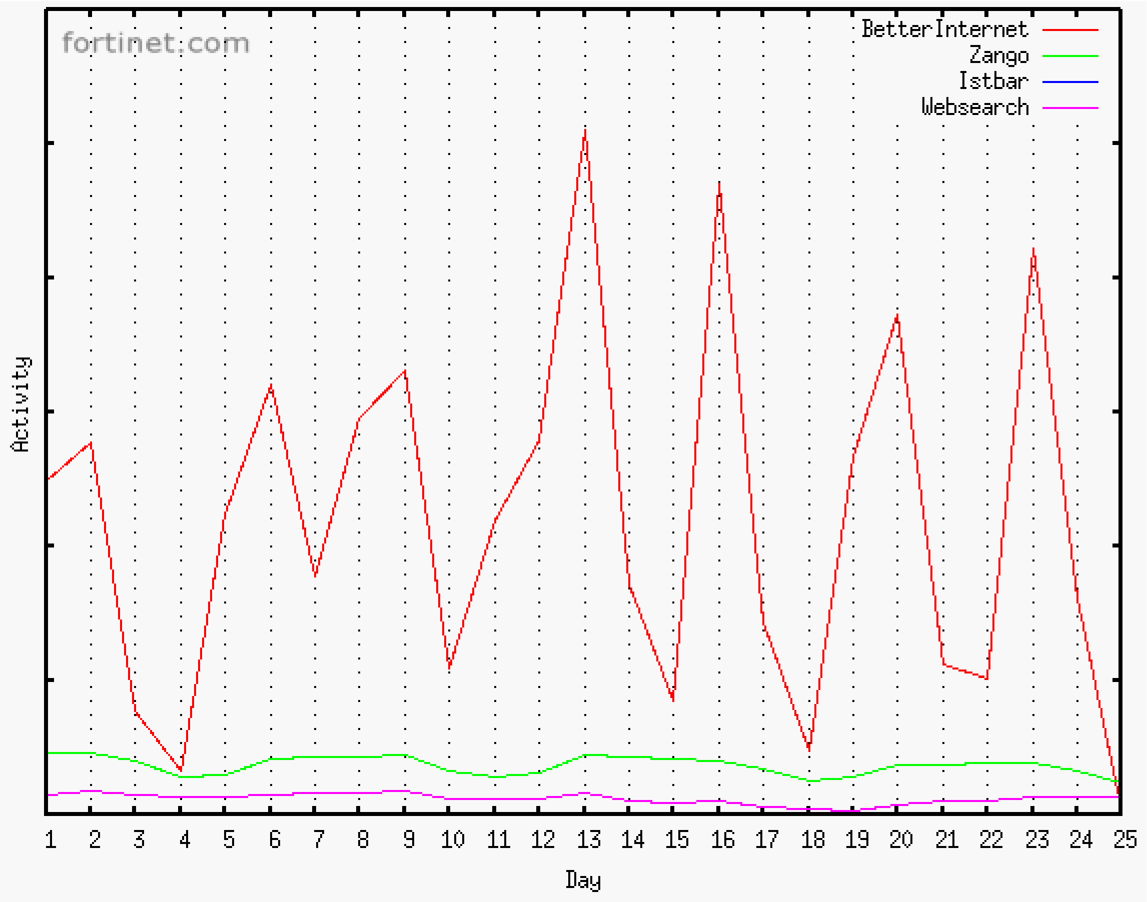


Figure 10: BetterInternet statistics

There is a striking pattern in the figure: Tremendously sharp peaks of the Adware component installation volume appear on every Monday and Thursday of the month. This was also the case in January. Such a consistency and regularity of activity peaks, both in "height" and frequency indicates that some botnet owner somewhere initiated a massive installation procedure of the Adware component each Monday and Thursday along the month. In between those days, the adware component is most likely wiped off the infected computer, so that next install generates the same impact again.

The question is: Are Adware companies with a partner program really abused by botnet herders? Or do they passively allow this activity because in the end the only victims are really users, while everyone else in the loop profits from the situation?

While answering this question is left as an exercise to the reader, an Adware planting business model is devised below:

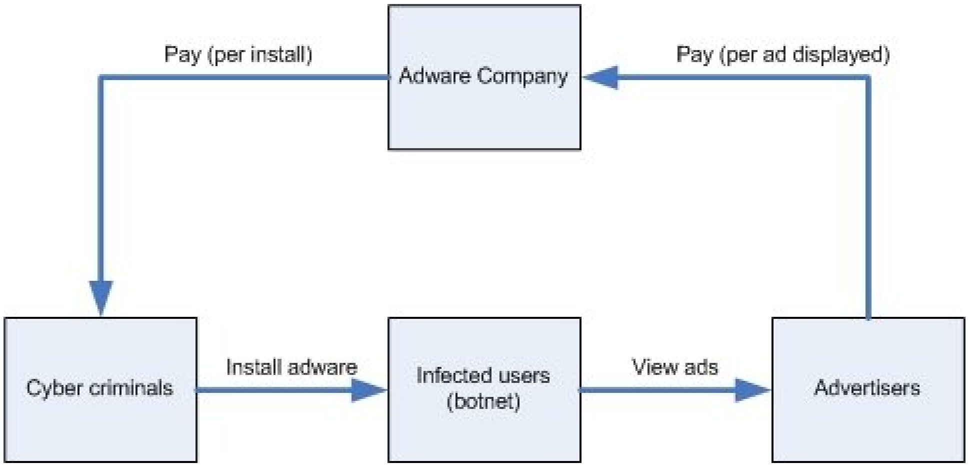


Figure 11: using botnets for Spyware planting

The costs involved mainly sum up to building a botnet:

- Root access to a Linux machine to host the Command & Control channel (usually, an IRC server): **$15**
- Stolen CC to register the domain name of the Command & Control channel: **$2**
- Bot source: **$2**
- Packing it into an executable file undetected by main AV vendors for a day or two: **$100**
- Fresh spam list (i.e. list of active e-mail addresses): **$8**
- A fistful of php-mailers to spam out 100K e-mails for 6 hours: **$30**

Assuming that the Adware company pays $0.40 per install, that the botnet is made of 5000 Zombie machines, and that two installation operations on all Zombies are performed per week, this gives the following result, for the first month of exploitation:

Total Cost: **$157** (once)
Total Profit: 0.4 x 5000 x 8 = **$16,000** (monthly)
Gain: **$15,843** (first month)
Productivity index (Profits/Costs): **102** (first month)

Two points are worth noting here:

1. Botnet herding implies having certain skills: being able to install an IRC server, to tweak and compile a bot... This may not sound impressive to an experienced user, yet to the eyes of regular "kids", botnet herders are indeed a superior caste.

2. This business model insures a monthly income, with few maintenance costs. Essentially, maintenance costs get down to keeping the botnet up and running with a constant size. Since Zombies are sometimes disinfected or re-installed, this implies repeating the three last steps above (packing, finding a spam list, spamming) from times to times.

3.5. Online extortion business model

This business model could be referred to as cyber-racket, for it closely resembles "real world" racket on many aspects. A typical scenario is the following:
A company doing online business, say, selling music records online, receives a threatening e-mail. In this letter, the company is asked to immediately wire $10,000 to a specified drop, otherwise its website would be heavily crippled during the next week. The company disregards this threat, and within a few days starts to experience worrying down-times of its servers, thus

losing considerable amounts of money. Then comes a second e-mail, asking this time for $40,000 to be wired. If the ransom is not paid, the down-time will increase. In the other case, one year of generous protection is offered. The company "does its math", and pays. Finally, the ransom appears as "security consulting costs" on the company's financial records.

Although most victim companies do not want to communicate on this, such a scenario probably occurs more frequently than what we are being told. Indeed, while in a survey lead by Carnegie Mellon University researchers [10], only 17% of small and mid-size businesses reported being targeted, it is generally estimated that two thirds of online extortion attempts are not reported.

The key to the success of online extortion business models is the following: As long as the extorted funds are clearly less important than what is being lost during the down-time, and what it takes to afford a complete, effective protection solution, there is no reason why such a model would not function.

For instance, in the famous BetCris.com case [11], the targeted company (a gambling site located in Costa Rica) reckoned to lose as much as $100,000 per day of down-time. This is tremendously more than the initial $20,000 cyber criminals required to cease their attack. Before evoking the costs of a protection solution, it is now useful to have a quick overlook of the technical aspects of an online extortion attack. The key points are the following:

- Cyber criminals use a technique known as a "Distributed Denial of Service" (DDoS) attack to cripple the victim website. Such attacks are typically launched from a botnet. The principle is simple and tremendously effective: Via the botnet's Control & Command channel, each single Zombie machine (the infected "slaves" forming the botnet) is instructed to flood the target, generally with what seems to be legit traffic (simple example: requesting a web page on the target server). Provided there are enough Zombies participating in the attack, the resulting aggregated traffic consumes all the resources of the targeted network - beginning with its bandwidth.

- The "regular" kind of botnet features from 5,000 to 10,000 zombies and can therefore generate a DDoS attack "eating" up to 1 Gbps of the target's bandwidth. This is enough to take down the vast majority of unprotected businesses, but would not fill the pipe of a solid, prepared data center to a lethal extent. However, there have been botnets featuring up to one million Zombies dismantled in the past, and some smaller botnets are obviously connected (i.e., they belong to the same herders, hence they can correlate their forces in a single DDoS attack).

- Due to the nature of DDoS attacks, protection is a complex and demanding challenge. Although off-the-shelf products do exist, at a certain point, the only way you can prevent your bandwidth from being exhausted is to increase the size of your network pipe, so that all the traffic generated by the Zombies can be absorbed. Some companies offer high-bandwidth data centers, which, combined with various anti-DDoS tricks can efficiently absorb the traffic generated by a mid-sized DDoS attacks, the legit traffic being then distilled to the customers servers - hence transparently maintaining up-time during the attack. This strategy is known as "scrubbing" and the service costs around $50,000 per year for a mid-sized business.

Bearing that figure in mind, as well as the fact online businesses world-wide drain billions of dollars each year and offers a wide, growing range of potential targets (online music shops, gaming sites, betting sites, gambling sites, online services... Everything that can lose money when being offline), it is reasonable to think online extortionists have many bright days ahead.

Assuming a cyber criminal willing to stay relatively "low" under the radar, the following example may be devised:

Total Cost: building 5 to 10 middle-sized botnets: **$1,500**
Total Profit: **$50,000** yearly, assuming 5 successfully racketed companies, with a ransom rate of $10,000 per company.
Gain: **$48,500** (yearly)
Productivity index (Profits/Costs): **32.3** (yearly)

3.6. Phishing business model

Perhaps the cyber-criminal activity getting the most press-coverage, Phishing makes vertiginous amounts of money flow on the dirty wires, at the expense of naive - or simply non-experimented - users. Here is a snippet of a conversation I had with a Phisher on IRC:

<G-Dogg> Man, ppl are really st00pid to fall for such scams
<high5> nah their not
<high5> look
<high5> if u never heard of this u would do the SAME thing
<G-Dogg> maybe
<high5> im here since 98, and believe me. Even professors reply to scampages
<high5> i broke into one of the biggest .edu domain
<high5> with password from a scampage
<high5> can u believe that?

This highlights, if needed, that the reason why phishing is being successful does not lay in user's stupidity, but rather in user's poor education to security concerns. Thus, contrary to what some have suggested, we do not need "patches for human stupidity", but user education programs.
Let us close this parenthesis, however, and focus on dissecting the Phishing business model, with the help of the following example.

3.6.1. Phishing phase

Costs covering the actual Phishing operation (excluding the cashing out part):

- Phishing Kit: Scam letter + scam page: **$5**
- Fresh spam list: **$8**
- A fistful of php-mailers to spam out 100K emails for 6 hours: **$30**
- Hacked site for hosting scam page for a couple of days: **$10**
- Valid cc to register domain name: **$10**

Total costs for the phishing operation: **$63**

It is worth noting that very basic skill only is required to set this up. The rate of success depends on many different factors, among which we can cite:

- The "quality" of the mailing list - that is to say the rate of active individual accounts it contains.
- How focused is the attack. For example, a scam targeting a brazilian bank sent to .br addresses would have a higher success rate than a "shot in the dark".
- How educated is the targeted population. See above, people are tremendously more likely to be fooled if they have never heard of Phishing. That is why, all along 2005 and 2006 we have seen phishing regularly expanding to new countries. Users of such un-phished yet countries are fresh meat to the phisher's eyes.
- The quality of the mailers. To spread their poison, phishers generally buy what they call "phpmailers direct to inbox". A phpmailer is a simple php interface to the mail server of the (hacked) server it runs on, and is the simplest way to send spam. A monkey could do it (no offense to monkeys):

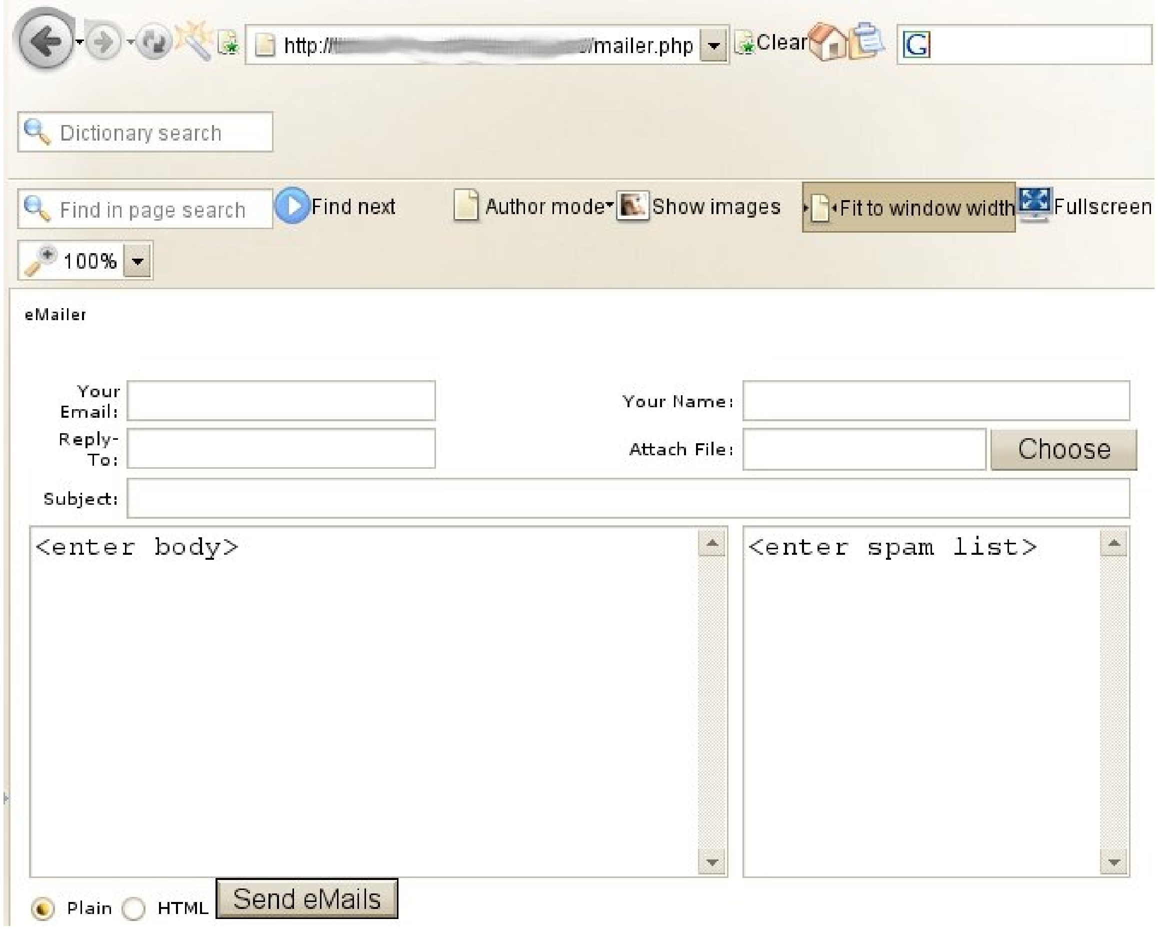
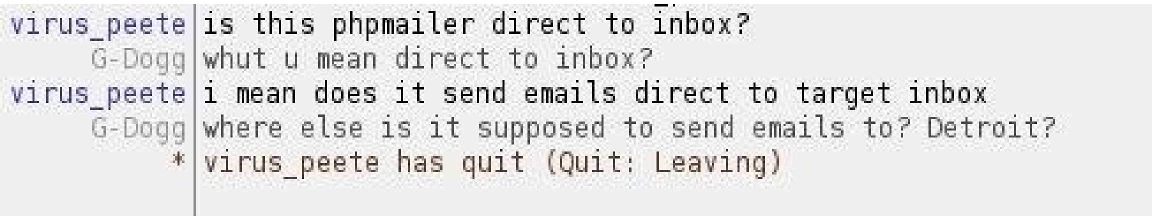


Figure 12: Php Mailer

The "direct to inbox" concept, on the other hand is more difficult to grab and gave raise to amusing situations during our investigations:

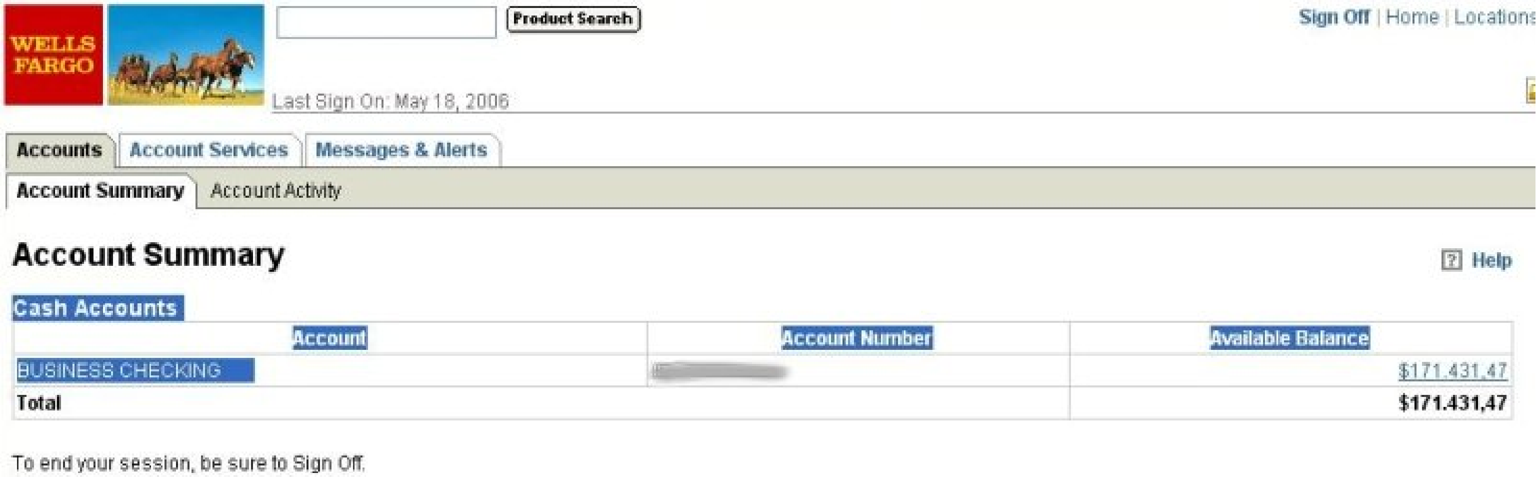


```
virus_peete | is this phpmailer direct to inbox?
     G-Dogg | whut u mean direct to inbox?
virus_peete | i mean does it send emails direct to target inbox
     G-Dogg | where else is it supposed to send emails to? Detroit?
          * | virus_peete has quit (Quit: Leaving)
```

Figure 13: Communication breakdown

Actually, by "direct to inbox", kids mean that emails sent from that phpmailer are going to end up in the INBOX folder of targeted users, not in the BULK (for @yahoo.com addresses) or SPAM (for @gmail.com addresses) folder. Even though the targeted mailing list does not necessarily contains such addresses, it seems to be common belief that "if it works with @yahoo.com, it works with all". Interestingly, they seem to consider that the "directness" solely depends on the mailer host (i.e. is it on the spam blacklists, does it craft correct headers and SMTP envelopes, does it comply to the Sender Policy Framework [12], etc...) and not on the scam letter contents.

Once they tweaked those factors, most phishers I spoke to reported they were getting around 20 accounts per operation involving sending 100,000 phishing e-mails. Balances are, of course highly variable and unpredictable, but it is not rare to hear or see phishers bragging about "$100K+" balances (i.e. balances of over $100,000).



Last Sign On: May 18, 2006

Account Summary

Cash Accounts

Account	Account Number	Available Balance
BUSINESS CHECKING	[redacted]	$171.431,47
Total		$171.431,47

To end your session, be sure to Sign Off.

Figure 14: phished account

However, as high as the stolen accounts balances can be, this is not cash. This is virtual money. This is a number on a web-based banking interface. Hence the next question: How to turn this virtual money into cash? (no philosophical stone involved)

3.6.2. Cashing phase

There are three main strategies a successful phisher can use to make some cash out of his stolen online banking logins:

a) Selling the stolen login credentials

This is where most phishers are heading to, because the traceability of banking transactions and the high volume of money involved imply higher risks and further complications than simple carding does. The account appearing on Figure 13 above was negotiated on the basis of $400, payable by e-gold immediately. In general, accounts holding a $100K+ balance are being negotiated from $100 to $500 e-gold.

For the sake of the example, we can assume that out of the 20 accounts he got from the phishing operation described in phase 1 above, a typical phisher can make from $200 to $2,000 by selling them. Considering the phishing operation costs ($63), this leads to the following model:

Total Cost: **$63**
Total Profit: **$200 - $2,000**
Gain: **$137 - $1,937**
Productivity index (Profits/Costs): **3.17 - 31.7**

As one can see, the productivity may not always be high, but it still generates more money than the traffic "entry level" kids are into, and it is undeniably less risky than playing around with drops to cash the money out.

b) Cashing the money via drops

This solution is undeniably juicer, however it implies finding a reliable drop (see the "drops" section in the "Profiles" part), which is nothing but an easy task; especially when "reliable" means the drop would not "give you out" in case he gets nailed... Indeed, for drops to wire money back to phishers, in theory they need their name and address. In practice, a cautious phisher may use several layers of drops before the money (or what remains of) reaches him.

It is also possible to ask for payment in e-gold, but drops seem to be reluctant to do so.

Assuming typical drops charging 50%, a "rip-off rate" of 0.5 (i.e. one drop out of two is a ripper) and a total stolen balance varying from $10,000 to $100,000, this yields the model:

Total Cost: **$63**
Total Profit: **$2,500 - $25,000**
Productivity index (Profits/Costs): **40 - 400**

c) Cashing the money via off-shore accounts

This is perhaps the most advanced strategy; it involves two layers of anonymity:

i. Stolen credentials are used to buy e-gold, preferably split between several accounts to keep the visibility of each transaction low.
ii. e-gold is used to load debit cards (Typically Cirrus or Maestro) issued by off-shore companies, which only require a valid address to send the cards to. This address can be the one of a post box, or of a drop.

Cash is then withdrawn in ATMs with the debit cards, until the daily balance limit of the cards is exhausted. Assuming a total balance for stolen accounts of $100,000:

Costs:

- Phishing operation: **$63**
- e-gold transaction fees: 4% of $100,000 = **$4,000**
- Ordering 100 debit cards: $20 x 100 = **$2,000**
- Monthly fees for all the debit cards: $3 x 100 = **$300**
- Card loading fees: 3.5% of $100,000 = **$3,500**

Total Cost: **$9,863**
Total Profit: **$100,000**
Gain: **$90,137**
Productivity index (Profits/Costs): **10**

3.6.3. A word on the mafia

Phishing channels on IRC are just that: marketplaces where some people sell stolen online banking login credentials, and other people buy them. The later may be isolated individuals willing to implement either strategy b) or c) above without having to go through the hassle of setting up a phishing operation. Or it can be criminal organizations, using their own, local, controlled thus safe drops to cash the money. Assuming a buying price of $500 for an account holding a balance of $200,000, this yields an outstanding productivity index of 400.

Let us do a quick comparison with the hard drugs business: where poppy is cultivated, in the famous Golden Triangle, 10 kilograms of opium cost around $1,000. With such an amount, a good chemist obtain around 850 grams of pure heroin. On the end market, each individual dose of 0.085 grams is sold for about $100. This yields a global productivity of $1,000,000/$1,000 = 1000.

This productivity, however, does not take into account numerous side costs related to chemical transformations, transporting and stocking products. Considering this productivity is, at least, cut by two due to the aforementioned costs, it roughly gets down to the productivity devised above (400).

In conclusion, the phishing business, yielding a very high productivity while being much less risky and effortless than the drugs business has all it takes to draw tremendous interest from traditional criminal organizations.

3.7. Industrial spying business model

It was evoked earlier on that companies subject to online extortion tend to keep their mouth shut about it. Unsurprisingly, this also applies very well to companies victim of focused attacks aiming at stealing corporate data, intellectual property, or whatever else that may yield a competitive advantage for a rival company.
A few cases are surfacing, however, among which is the famous Israeli Trojan story [13], where a software engineer based in London created a Trojan Horse program specifically designed to ex-filtrate critical data gathered from machines infected by his program. He had made a business out of selling his Trojan Horse program to companies based in Israel, which would use it for industrial spying purpose by planting it into competitors networks. The means used to inoculate the Trojan Horse were varied and sometimes quite inventive, ranging from simple e-mail traps to the mailing of promotional CDs infected with the evil program!

In parallel we witnessed the apparition of email worms automating similar data ex-filtration features. For example, the mass mailing worm deemed W32/MyFip@mm [14] main characteristic is to scan the hard drive of infected machines for all files with the following extensions:

.PDF
.DOC
.DWG
.SCH
.PCB
.DWT
.DWF
.MAX
.MDB

Such files are uploaded to an FTP server owned by the cyber crooks. This is clearly aimed at stealing as much intellectual property as possible wherever it can be, then selling it to the players which are ready to pay for it.

This leads us to consider two distinct business models for cybercrime applied to industrial spying:

3.7.1. Selling Trojan-ware

This is typically what "coders" (see the profiles above) do. There is no production cost involved per se, safe for the time spent coding the customized Trojans ordered by "customers". A full-blown, undetectable customized Trojan with rootkit features can cost up to $800, plus monthly fees of around $20 to get regular updates; such updates are only meant to keep the malware undetected to main Antivirus vendors scanners.
The sole "make my trojan undetectable" service is also proposed, at a lower price ($80 to $150). The technique consists in iterating a process of packing and tweaking the binary, until it goes undetected to online cross-scanning services.

It is worth mentioning that if a geek version of "Who wants to be a millionaire" is ever organized one day, we may see that kind of question:

With which disclaimer do the coders involved in Trojan-ware business systematically try to back themselves up?

a) We do not take responsibility for our customers action
b) We do not condone the use of our software for malicious purpose
c) This is for educational use only
d) All of the above

3.7.2. Selling stolen Intellectual Property

This model typically functions on a contracted basis. Although worms like MyFip have been around for over a year, cyber criminals openly advertising stolen I.P. from company X have not been spotted during this investigation - most likely because contractors do not hang around these trading channels, which are a complete different world than the one of high-profile hackers. This may change however, sooner or later, considering that contracting a hacker implies costs that are in the thousands (and can reach several hundreds of thousands of dollars, depending on the job) while a kid who trojanized a company via the simple use of a network worm will happily sell everything he could steal to the first buyer for as little as $500.

3.8. The new deal: Mobile Phones abuse, or the Return of Dialers

In the old analogic modem days, existed a category of malware deemed "Dialer". Dialers would use the victim's modem to call premium numbers, hence making some reasonable money at the expense of unfortunate users. But back then, botnets were not as popular as today and the vast majority of viruses and worms were not money-motivated. Then, when the era of botnets really begun in 2004, the analogic modems had been replaced by DSL or Cable modems, with no real telephony features.

Today, the upcoming reign of smartphones is making the dangerous encounter Dialers / Botnets possible. Indeed, smartphones are really personal computers with telephony functions. This opens for many juicy possibilities, ranging from premium calls abuse to roaming network abuse.

On the technical side, MMS worms such as Commwarrior [15] proved their capability to spread in the wild. In a study lead by Fortinet in 2005, results showed that as much as 5% of all MMS on mobile operators networks were infected by a Commwarrior variant. This figure is likely to grow, at the same pace as the percentage of smartphones among mobile phones is growing. As a matter of fact, sooner or later, all mobile phones will be smartphones, thereby opening the door to fast mobile worms outbreaks, much like desktop computer worms outbreaks. And of course, it is just a matter of months before someone embeds a bot into a Commwarrior variant, hence turning infected phones into Zombies.

The cyber criminal business models based on mobile phones abuse would then be likely to function on a buyer / seller scheme, where the seller does the dirty job, then offers his services to the buyer who makes the biggest profit out of it. A possible scenario is the following:

A botnet herder controls a botnet featuring 5,000 zombies, all running on infected mobile phones. As he is advertising his botnet on IRC, the owner of an off-shore company that sells ring tones for mobile phones contacts him. The owner offers **$500** e-gold to have each bot download 10 ringtones from his company. Assuming ring tones cost $2 each (paid via calling / texting a premium number), this almost instantly generates a raw income of 5,000 x 5 x 10 = **$100,000** for the ring tones vendor, that is to say a net benefit of $99,500 (corresponding to a productivity index of **200**).

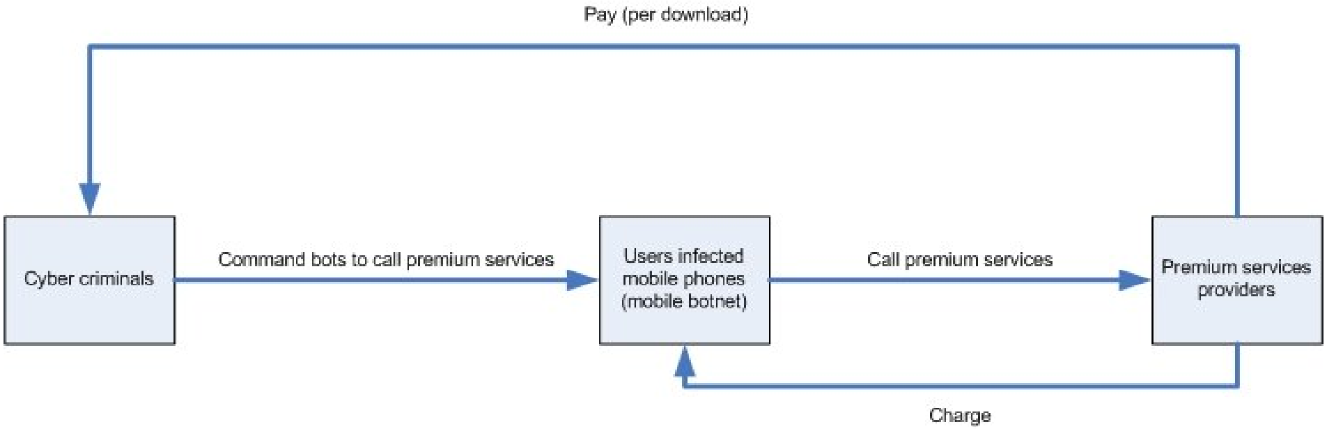

Pay (per download)
Cyber criminals
Command bots to call premium services
Users infected mobile phones (mobile botnet)
Call premium services
Premium services providers
Charge

Figure 15: Using mobile botnets for premium calls abuse

Not only does the operation yield impressive benefits, it also involves very little risk. The victim customers may complain when seeing their bill at the end of the month, either to their mobile operator or to their phone vendor. Chances are that both would decline responsibility, with no further investigation. In the best case, should it be proved that the mobile phone was infected by a bot, it still does not imply the customer did not make the calls by himself.

Additionally, the impact of customers complaints would be greatly softened by the fact they would be reported to different operators, possibly in different countries.

Does this scenario sound worrying? Picture this: the same ring tone vendor contracts a coder to create a mobile worm that:

1. Downloads ten ringtones, one from the contractor's company, and nine from randomly chosen competitors
2. Sends itself to all the contacts of the infected phone
3. Self-destructs

Stealth, moving, hard to trace at a financial level... In a nutshell, a nightmare to cope with for abused customers, mobile operators and law enforcement people. Given the potential behind all that, cyber crooks may even start registering online goods merchant companies for the sole purpose of implementing this kind of cyber criminal business model.

As complex as the issues raised by such scenarios can be, though, we have to try to anticipate them - because given the amounts of money involved, they are more than likely to happen.

Conclusion

We have seen throughout our investigations how profitable the various business models of cyber criminals can be, with productivity indexes sometimes reaching or surpassing those of drugs business, while involving tremendously lower physical risks. This is all the more worrying that most of these schemes are reasonably easy to set up, and require little skill; indeed, needless to be a computer wizard to use a php-mailer.

Now, the models and scenarios we shed light upon raise many questions and challenges in terms of prevention, protection and law enforcement. As a matter of course, in-depth analysis of such challenges could be the subject of a whole paper; undeniably, the main track to explore is also the main point of failure when it comes down to combating cybercrime: the lack of international digital laws and cross-border law enforcement coordination. Indeed, in many of the business models we studied, "drops" play a crucial role, and they generally do so in the front scene without even taking particular precautions, yet hardly feel threatened.

Further, tracking cyber criminals seems technically possible, but raises some ethical issues. For instance, hacking into the open proxies cyber criminals use to set up their scams would almost always reveal their real IP address. Even easier: feeding the cyber crooks community with proxies and servers secretly owned by the authorities would permit compiling many charges and IP addresses. However, doing so equals to, at least temporarily, helping them in setting up their scams - which is highly debatable from an ethical point of view.

At users level, we evoked how phishing letters could fool anybody who is particularly unaware of cyber scams. One track to explore, in the user education branch, would be for banks to impose a mini "scam training" (possibly online) to their customers before enabling online banking for their account.

As a matter of fact, in a cyber world, insecure by design (but who could foresee the internet growing to that extent back in the 80s?) and evolving at an unrestrained pace, cyber crime fighters must explore all the possible tracks, and above all, be more inventive and creative than the culprits themselves. Otherwise, cyber criminals may endlessly keep an edge.

References

[1] Reuters press agency, 2005

[2] http://en.wikipedia.org/wiki/Spamming

[3] "Zombie or not to be: Trough the meshes of Botnets" (http://www.aavar.org/avar2005/speech/023.ppt)

[4] http://en.wikipedia.org/wiki/Botnet

[5] http://arachnid.homeip.net/papers/VB2005-Bots_and_Botnets-1.0.2.pdf

[6] http://www.honeynet.org/papers/bots/

[7] http://en.wikipedia.org/wiki/Internet_Relay_Chat

[8] http://en.wikipedia.org/wiki/E-gold

[9] http://www.e-gold.com/letterdetail.html

[10] http://www.heinz.cmu.edu/whatsnew/images/CMU_Cyber_Extortion_Study.pdf

[11] http://www.csoonline.com/read/050105/extortion.html

[12] http://www.openspf.org/

[13] http://www.msnbc.msn.com/id/8064757/

[14] http://www.fortinet.com/VirusEncyclopedia/search/encyclopediaSearch.do?method=viewVirusDetailsInfo&fid=38590

[15] http://www.fortinet.com/VirusEncyclopedia/search/encyclopediaSearch.do?method=viewVirusDetailsInfo&fid=30623

Appendix

Typical drop recruitment letter:

--
Good afternoon ladies and gentlemen.

Our company is glad to offer you Work the Internet of the manager in our company.
Working with our company, you can earn from 1000 euros up to 2400 euros day.

For what to get a job in our company you should have the bank account or Pay Pal account.

Our company offers you legal and highly paid work

Principle of work:

On your bank account or on yours Pay Pal account will act money of our clients

You should take money, and send 90 % of money on system of remittances Western Union or e-gold.
Our company will pay to you cost of transportation and charges on sending of money in Western Union.

You can, earn, yours of 10 % not spending money for the commissions.

Plus of work with our company:
You can earn up to 7000 euros a week (further the salary will raise)
You can sign the contract with our company for the first 3 years of work.
To work to you it will be necessary no more than 3 hours per day (From Monday till Friday)
An opportunity of increase on career ladders up to the main manager and the Chief of department (with increase of your wages)
Working with our company, you can receive free-of-charge holiday by family yearly for the sum not exceeding 2500 euros.
Our company does not demand from you an operational experience and higher education .

Our company will give up to you in reception of work only on the given conditions:
If you have problems with authorities
If you still do not have 18 years.

For reception of work of the manager in our company you will need to fill in the form of registration on a site of our company: (http://wwwanypayfinance.net)

After you fill in the registration form, our operator will contact you through phone or your e-mail during 24 hours from the moment of filling the form.

Hurry up.
The amoun t of workplaces in our company is limited.
--