TEAM CYMRU

the underground economy: priceless

Rob Thomas is a long-time network security professional and founder of Team Cymru. He has written many papers on information security and spoken at numerous conferences worldwide on the topic of Internet security.

robt@cymru.com

Jerry Martin is an advocate of the complete information assurance process: risk assessment, policy development, solution deployment, and user education. He has worked in several information security positions, including at the U.S. Air Force.

jerry@cymru.com

THE CYBER UNDERGROUND ECONOMY is just as seedy and illegal as its physical counterpart. The primary objective of those who operate there is *money*. The National Cyber Security Alliance published some data a while ago that concisely describes the problem:

1. Fully 61% of U.S. computers are infected with spyware.
2. Americans say they lost more than US$336 million last year to online fraud.

These figures are largely based on self-reporting, which is often suspect. Given the enormous quantity of data witnessed on numerous Internet Relay Chat (IRC) channels, both numbers may be underreported. Given these staggering numbers, one might well ask what is being done to address this criminal activity. Lamentably, the answer is, "Not much." The popular school of thought is that finding and prosecuting these perpetrators of financial fraud and outright theft is too costly, too resource-intensive, and just too hard. This article will expose the infrastructure the miscreants have established; the open arrogance the buyers, sellers, traders, and cashiers exhibit; the activities and alliances in which the underground denizens are involved; the method by which they receive their ill-gotten goods; the blatant manner in which they advertise; and the personal data that is harvested every single hour of every day of the year. Numerous snippets of captured IRC chatter will illustrate the points raised, although the nicknames and the information harvested are obfuscated.

The miscreants can make a handsome living through these activities. Even those without great skills can barter their way into large quantities of money they would never earn in the physical world. It is important to note that these miscreants are located all over the globe, and thus they may be earning well above the average income for their areas.

Infrastructure

Entire IRC networks—*networks*, not just single servers—are dedicated to the underground economy. There are 35 to 40 particularly active servers, all of which are easy to find. Furthermore, IRC isn't the only Internet vehicle they use. Other conduits include, but are not limited to, HTTP, Instant Messaging, and Peer-to-Peer (P2P).

Increasingly, many of the miscreants utilize encryption in these services, such as VPNs or SSL. The following table illustrates the number of cards compromised in three months for a single server!

Month	*Amex*	*Visa*	*MasterCard*	*Discover*
2005/10	70	28942	11820	1064
2005/11	51	31932	13218	1214
2005/12	89	26492	10662	1079

The miscreants in the underground economy are typically self-policing. Each IRC network will normally have a channel, such as #help or #rippers, dedicated to the reporting of those who are known to conduct fraudulent deals. The operators of these networks will ban the nicknames of those who have a proven history of fraud. This is a form of self-regulation that ensures the sellers and buyers have a "pleasant" experience and attempts to elicit repeat visits. The miscreants keep meticulous records of those who have defrauded them, and they are quick to share those records with everyone. As with all criminal societies, there is a fair amount of fraudulent dealings and "ripping" (bad business deals).

The tale goes something like this: Miscreant <A> advertises a need for roots, which are compromised UNIX systems on which someone has obtained root access. <B> disappears for a while to have a private conversation with <A>, which is the norm for those finalizing deals. <B> then pastes that conversation into the open trading channel as a warning to other miscreants:

<B> i rember when u tried to sell me a root scanner
<B> lol were u going to try scam me
<B> yeah
<B> coz u told me last weekk u had a private root scanner
<A> i need it
<B> you were going to try scam me
<B> A is a scammer so beware
<B> 1 day he trys selling me a root scanner next day he needs roots
<B> so beware

Rest assured that a great many miscreants will now avoid conducting business with <A>. In contrast, some miscreants are well vetted, with certain underground economy networks and forums bestowing verification on those miscreant merchants who are considered reliable.

Because these miscreants encounter a wide variety of fraud, they capitalize on the existing criminal support structure, which includes places to obscure their ill-gotten profits. "OS" and "os" mean "offshore bank" in this case:

<A> whats a good os bank?
<B> you can use webmoney
<B> if you can deal with their fees
<B> its not a OS bank
<B> but they wont ever freeze your account
<A> .ee right?
<B> no
<B> thats an exchanger
<B> `www.wmtransfer.com`
<B> is the official webmoney site

Buyers, Sellers, and Traders

Even the miscreants who spend most of their days herding bots have requirements, mostly in support of their profit-making activities with those bots. In one bit of chatter, a miscreant is specifically seeking an IRC daemon to prevent interlopers from running the intelligence-gathering commands. Such IRC daemons do exist, as do the IRC daemons that produce bogus responses. The needs and those who meet them do have exchange rates, though these can fluctuate wildly. Some miscreants willingly list their prices, such as <A> in the following:

> <A> Sell Cvv US(1$ each),Uk(2$ each)Cvv with SSN & DL(10$ each)and ePassporte Account with 560$ in acc(50$),Hacked Host(7$),Tut Scam CC Full in VP-ASP Shop(10$).shopadmin with 4100 order(200$), Tool Calculate Drive Licsence Number(10$).... I'm sleeping. MSG me and I will reply U as soon as I can !

Compromised hosts sold by <A> cost US$7, which is quite a lot, considering that the average bot costs US$0.04 (four cents). Note as well that <A> is actually asleep; his scripted advertisements continue unabated, providing a steady marketing opportunity.

Dealing in the underground economy is not without risks, however, and the merchants realize this fact. This is why they provide friendly advice designed to maintain the safety of those who visit their servers. <A> is a bot that emits this message at regular intervals:

> <A> Precautions 1. Use Fake Ip or Use a VPN While On This Server. 2. Do Not Use Your Real ID in picking any type of money 3. Dont give your real information to anyone unless you know him/her. 4. keep your self safe on [UNDERGROUND ECONOMY IRC NETWORK]. ThankS!!

One can readily see the plethora of advertisements by the miscreant merchants and the miscreant consumers regarding compromised financial accounts, drops (compromised financial accounts used to launder funds), and cashiers (those who can clean them out):

> <A> i have wells and boa logins and i need to good drop man .....ripper f#@! off
> <B> <=== .Have All Bank Infos. US/Canada/ Uk ...Legit Cashiers Only Msg/me
> <C> HELLO room... I am Ashley from the State... I got drops for US banks and i need a very trust worthy and understanding man to do deal with ... the share its 60/40...Msg me for deal

The miscreant spammers are some of the most highly paid individuals in the underground. It's easy to see why—spam works, and yields high profits. In one particular instance, the spam involved online (illegal) diplomas. At US$1000 per diploma, it's obvious why these sponsors can afford to pay the miscreant spammers. The miscreant spammers can then afford to pay the proxy creators, malware creators, etc.

Activities and Alliances

The miscreants have all sorts of capabilities and all sorts of needs. They aren't so unimaginative as to limit their opportunities. When they have needs, they offer remuneration or even partnership. One miscreant advertises his need for a spam mailer to fill Hotmail inboxes. He is willing to pay through e-gold, or will even share the proceeds from his phishing (the miscreants call it "scam") site. They'll happily pay for that which no one

will trade. Selling source code for malware (rarely 0days) is another avenue to profit. It is critical to note that these aren't the malware authors. There are miscreants who spend quality time obtaining source code and reselling it. Some of them, a very few, will also modify it for a fee.

Those who provide services in the underground economy are looking for long-term customers. It pays to keep the customers happy and to nurture those illicit business relationships. Oh, and don't believe those reports from security vendors who say all hacking happens in South Korea, or Brazil, or China. There are miscreants everywhere (e.g., <A> i need any hacker from 'country x').

The large number of online merchants that are regularly hacked is both sad and impressive:

> <A> selling admin database password of hacked online store with hundreds of cvv2 and check draft payment (it's Bank accounts # and Routing#) inside. I receive the payment 1st (WU/E-Gold). Also trade cvv2 for [WEB SITE] account.

Carding servers is easy, thanks to the proliferation of hosting sites that provide online purchase and configuration capabilities. The good news for the miscreants is that they no longer rely on boxes on their cable or DSL links. They now have professional, redundant hosting for their IRC servers, botnet servers, etc. Even exclusive, rare credit cards will be stolen. One can just imagine the purchasing power <A> has with this card:

> <A> I got an american express black card the other day
> <A> weird huh?
> <B> ... black card?
> <B> i thought it wa blue
> <A> go look it up
> <A> its called the centurion
> <B> first link has "black is beautiful" in the thingy
> <B> and it's talking about the card

It is also a reality that miscreants actually buy physical goods in the underground economy:

> <A> Sell cc's full info with PIN (debit, credit), COB's Laptops (alienware area51 = 500$, Dell inspiron 6100=400$, Scam pages (ebay, aol, paypal, egold, escrow, earthlink), track2gen (.exE) support 857 bins, 2000 bins (update bins), root. Payment (wu or e-gold).

The miscreants are avid proponents of online banking, particularly other people's online bank accounts. This has been and remains quite the popular activity, with accounts compromised daily. These accounts may be traded several times prior to any activity passing through them. Buying and selling compromised bank accounts continues unabated. Email inboxes, with their lack of security, provide yet another compromise vector for personal information:

> <A> has everything on 1 person from there emails,to paypal to ebay, online banking .travelcity , expedia , you name it i probably have it full info cc high limit /msg me

One miscreant inquires about the worth of 40K compromised financial accounts. It isn't worth much to him because he cannot cash it out. For this task, he requires a cashier and a drop (a place or account through which to route the money to him). For this reason, he will be paid pennies on the dollar for his collection of compromised financial accounts, which is just fine:

<A> how much would a lets say 40k
<B> with all informations 40k ??
<B> Fulls
<A> user name and pass
<A> 200-300 an account ?
<B> variable between 250 $ =====> 500 $
<A> ill retire in a month

This is the greatest failure of new technology—a rush to market, without consideration of the risks and a cost/benefit analysis. This is at the heart of the security problem. Certainly, that is not to say that industries should not capitalize on technological advances but, rather, that they should consider risk and threat mitigation strategies prior to bringing any product to market.

Obtaining a fake ID to cash out an illegal funds movement is an easy task in the underground. Many of the miscreants sell or buy such IDs, or teach others how to create them. There is quite the cottage industry providing supplies for this endeavor. All of the ID chatter is for U.S. IDs of various sorts, including college IDs, state IDs, and drivers' licenses.

Cashiers

Extracting cash from the underground economy is the goal of many, if not most, participating miscreants. They find all sorts of ways to accomplish this goal, though these aren't new techniques; physical world criminals have been doing this for years. So what's different? Online crime is often easier and has a lot less inherent risk. The biggest challenges to the miscreants aren't IDS, firewalls, 0day creation, or any other technological hurdle. The biggest challenge is where to cash the checks. Those who actively participate in the underground economy have another problem—how to move the significant quantity of illegally obtained funds. There are a variety of solutions they discuss, such as offshore trusts to protect their financial assets against lawsuits. Lawsuits, prying eyes, and seizure are all mitigated through the use of offshore banking. Several offshore banks will wittingly accept such accounts.

The miscreants advertise for cashiers for both logical and physical (e.g., go collect the money at a Western Union site) account cleanups. Cashing out these accounts often must be accomplished from within the country where the account resides. Enter the bank broker, the miscreant who will cash out the account. Demand is high for these miscreants, and they never ask questions. When a cashier attempts to clean out a bank account (50% always goes to the cashier) on behalf of another miscreant, that cashier must have some semblance of legitimacy with the bank. Increasingly, the miscreants are finding that a male voice attempting to clean out an account obviously belonging to a female isn't accepted by the banks. Thus is born a new skill set: gender-based cashiers. There are plenty of female miscreants, willing to clean out accounts both virtually and physically. When the market makes a demand, the demand-based underground economy responds:

<A> i need who can confirmer westernunion female visa
<B> speaking of wu, who can do females?

The miscreants who serve as cashiers in the underground economy are ready and waiting to fill the orders. They are happy to generate cash transfers, often through services such as Western Union. The mule or the intended recipient then picks up the cash at a Western Union office. This is both easy and convenient, the benchmarks of success in the increasingly online world. Although slightly obfuscated, this example is quite real:

<A> Western Union Money Transfer? Pick Up Notification.
<A> Dear X X,
<A> Thank you for using the Western Union Money Transfer
<A> Your money transfer has been picked up by the receiver.
Following is a summary of your transaction.
<A> XXXXXXX508
<A> Date of Order:
<A> 09/15/2005
<A> Amount Sent:
<A> $900.00
<A> Receiver Name:
<A> X X
<A> Status:
<A> Picked Up
<A> write me if u want me to cashout creditcard for you throgh westernunion

It's easy to move money online, because of the large number of cashiers. These criminals widely and loudly advertise their skills, prices, and specialties. They are competing for the business of other miscreants and are certain to add that touch of quality customer service:

<B> I have Bank drops for Quick Cashout in(Hsbc,Wells, Lloyds, Citibank,Boa, Barclays,Woolwich,rbc) Contact me now for Fast Cash out..Deal is 50% each
<D> Hello,I'm a professional MTCn confirmer if you have any order pending you can IM me,i have done so many transaction for different people and also i made different kind of transfer into account such as BAO, WELS,HSBC any body with full infos for this account who wanna transfer should IM me now and also i have BIN,EBAY SCAM PAGES,PHP bulk mailer if anyone is interested IM me all rippers keep off.NOTE I VERIFY FIRST.....

It's an odd use of the term "professional," but, in fact, these *are* skilled, reliable professionals. They know their business, are risk-averse, and are rarely caught. (What is the MTCN? That is the Money Transfer Control Number.)

Drops

One of the hottest commodities in the underground economy is the drop. A drop can have one of two definitions. The first definition of a drop is a location to which goods or cash can be sent. The person who owns the drop will then resend the items or hold them for pickup. There is a charge for this service, of course, ranging from a 70/30 (30% to the drop owner) split to a 50/50 split. Drops include homes and businesses, and often the drop owner is clueless about the contents of the dropped package. In this case, the drop owner is paid a flat fee by the shipper or the broker. The second definition of a drop is a bank account through which money can be moved. This is a convenient way to cash out bank accounts, online financial accounts such as PayPal, and credit cards. The drop owner almost always receives 50% of the take, although competition in this space is reducing that percentage. The location of the drop is critical, as some companies won't ship overseas. Some miscreants want a drop close to home and physical access. The demand is never-ending, with the greatest demand placed on U.S.-based drops, although some are undesirable. Where there is demand, there shall be supply. The underground economy abhors a vacuum.

There are miscreants who need drops in certain countries or who are able to cash out bank accounts in another country. Sometimes the same miscreant will conduct "business" in several nations. This miscreant is looking for drops (shipping addresses to which fraudulently obtained or outright stolen goods can be delivered) in a number of nations. The list of nations in which <A> will do business is both interesting and impressive:

> <A> I NEED DROPS FOR PHONES AND PDA's in Singapore Australia Austria Belgium Brunei Darussalam Canada China Denmark Finland France Germany Greece Hong Kong Indonesia India Ireland Israel Italy Japan Korea (South) Luxembourg Macau Malaysia Netherlands New Zealand Norway Portugal Saudi Arabia Spain Sweden Switzerland Taiwan Thailand United Arab Emirates United Kingdom United States

Criminals know no boundaries, and online crime is an international business. The miscreants understand ROI, and they also understand that an alliance only needs to last as long as it takes to accomplish the goals. The miscreants continue to build large networks of like-minded criminals. It will take a global network to thwart them. The denizens of the underground economy aren't unlike anyone else. They would like to retire at some point. Unlike honest, hard-working people, however, the miscreants have a paucity of ethics and perhaps a faster path to retirement.

Advertising

> <A> JOIN #[CHANNEL] THE BEST HACKER CHANNEL!!! JOIN US ..!!! U CAN BECOME HACKER AND RICH...!!!!

Doesn't that just about sum it up? Things have changed; these aren't the miscreants who will hack something, get arrested, and land a six-figure job at a security consultancy (though they might sell their sploits to one). Now they'll be paid to hack things, or write tools to hack things, or just sell things they've hacked, and not get arrested, and still make great money.

When a miscreant is dealing in compromised financial accounts, the miscreant must advertise to attract business. This proves to any potential consumers that the miscreant has the goods and can deliver. <A> begins by sharing some data from one of his collections of compromised accounts:

> <A> Account Summary
> <A> For optimal viewing of the Wells Fargo Web site, we recommend that you enable CSS
> <A> Cash Accounts
> <A> Account Account Number Available Balance
> <A> CHECKING 367-3157xxx $425.38
> <A> Total $425.38
> <A> Credit Accounts
> <A> Account Account Number Outstanding
> <A> Balance Available
> <A> Credit
> <A> VISA (View Spending Report) xxxx-xxxx-xxxx-9556 -$80.82 $5,900.00
> <A> Total -$80.82 $5,900.00
> <A> To end your session, be sure to Sign Off

It isn't strictly about extracting cash, however. The miscreants use the cash to obtain other goods, or they sell goods for cash. This gives us some sense of the relative value of certain goods. The bulk sales offer is troubling, as it

indicates the result of a larger compromise:

> <D> Selling CVV.$USD 3 EACH.IF BUY IN BULKS(100) 2 USD EACH

The underground shopping mall is open, as always, and happy to provide for every need. Be it through cash or barter, everything is for sale. Many of the traded items can yield hard currency:

> <B> got ebay/paypal/yahoo/hotmail/citibank/aol scams + psyBNC + hotmail mailbox closing exploit + how to crack anything + can create scam of any site in very little time + Track2gen.exe. Got millions of proxies all over the world + 3million ebay/paypal/egold mail list + track2gen(.php)(.exe) + dark-mailer pro v1.9(300$) + gamadye mailer registered(140$) + wolrds fastest mail bomber to get them msg me

Data Stolen

How much money do the miscreants make in the underground economy? More to the point, how much money do they steal? Here's a snapshot from one underground economy trading channel over a 24-hour period. These are the total account values for financial accounts to which these criminals have obtained access. These are just the *samples*; these miscreants claim to have many more accounts to sell, and they offer up the samples as advertising. All amounts are in U.S. dollars, and some of these account totals are impressive, while others are quite small. The true account owner probably doesn't consider them unimportant, however:

> <A> Total: $310.64—A is from Country A
> <B> Total $930,391.94—B is from Country B
> <C> Total $216,934.93
> <C> Grand Total $1,803.59—C is from Country C
> <D> Total: $49.00—D is from the Country D
> <E> Total $258,602.27—E is from Country E
> <F> Total $60.07—F is from the Country D
> <G> Grand Total $1,987.97—G is from Country F
> <H> Total $48,096.65—H is from Country A
> <I> Total $33,332.76—I is from Country B

So, with one channel, one 24-hour period, and just a few samples, at least US$1,599,335.80 has gone to fund multinational criminals.

When your credit card details are stolen, *all* of the details are stolen. When a miscreant offers up a "full" or "full info" for sale or trade, that miscreant will have the goods. Here is an example from <A>, an overseas miscreant. The victim's details have been slightly obfuscated. There is no such thing as a "secret question" when it comes to the miscreants:

> <A> Name: Jason XXX
> <A> Address 1: XXX S University Blvd.
> <A> City: XXX
> <A> State: OK
> <A> Zip: XXXXX
> <A> Country: usa
> <A> Home Phone: (XXX) XXX-X991 Ext:
> <A> Date Of Birth: 12/8/19XX
> <A> Social Security Number: XXXX32199
> <A> Mothers Maiden Name: Reaves
> <A> Drivers License Number: XXXX24766
> <A> Drivers License State: OK
> <A> Secret Question: What is your pet's name?
> <A> Secret Question Answer: Joad

<A> Name On Card: Jason XXX
<A> Credit Card Number: 4492XXXXXXXX8831
<A> Credit Card Brand: Visa
<A> Credit Card Type: Credit
<A> EXP Date: 4/2006
<A> Credit Card PIN Number:
<A> Card ID Number: X46
<A> Card Bank Name: OU Federal Credit Union
<A> Card 1800 Number: 1800XXXXX9
<A> eBay User ID: XXX
<A> eBay Password: XXXXXX
<A> eBay Password: XXXXXX
<A> **********
<A> **********

Unfortunately, the little snippets don't provide a sense of the frequency of such advertising or the inferred frequency of the transactions between buyer and seller. In one six-minute period of underground economy chatter from one underground economy network and channel, *eight* distinct miscreants sought to launder stolen money. This is fairly typical, with advertisements coming in ebbs and flows, drops and transfers occurring, and boldly advertising cashiers doing deals. Such activities are all readily accessible to anyone and everyone, with numerous participants happy to route money out of individuals' accounts to anywhere at all.

The use of keylogging and data-extraction bots, which is just about every bot now installed, has enabled the miscreants to have ready access to bank accounts and other financial accounts:

<A> selling Bank Of America online access with $10,000 and other with $900 balance. Payment : Western Union
<B> who can cashout Bank Of America/Washington Mutual without pin but with online access msg me and lets make a great deal !
<C> can cashout verified paypals in 2 days. $2000 every couple of days. 75/25. Msg me for deal
<D> Payee: Centennial Bank

One miscreant even provided a screen shot of a compromised Wells Fargo account, with a net total of US$21,431.18 in cash.

Conclusion

The underground economy is fertile ground for the pursuit (and, we hope) prosecution of the miscreants. Most of the underground economy servers are public, advertised widely, and easy to find (standard IRC ports, very descriptive DNS RRs, etc.). There is absolutely no presumption of privacy in the underground economy; the channels aren't hidden, the channels have no keys, and the servers have no passwords. The clients in these channels are widely divergent. Think about what has just been shared:

1. There is no need for specialized IRC clients.
2. There is no need to rapidly track ever-changing DNS RRs and IPs.
3. There is no need to pull apart every new permutation of malware.
4. There is no need to hide, period.

This is a cosmopolitan mix; there is evidence of physical crime as well as online crime, and admissions of guilt, and all are readily available. Although the data in this article is obfuscated, these stanzas of gross fraud come with the name, address, phone number, SSN, and mother's maiden

name of the victim. That seems ready-made for a complaint and one might imagine that a prosecutor, judge, and jury would understand those blatant advertisements. These same individuals have, in the past, been successfully educated about DDoS, hacking, and warez. Even in child-exploitation cases, the jury learned about the methods by which such horrors were shared online. There are approximately 38 active underground economy IRC servers at present, and most of these are located in the United States.

If more than one year can be expended tracking a pair of bot-herders, then surely logging and tracking the miscreants who are online, advertising their crimes, is worth the resource expenditure. If the goal is putting a dent in online crime, then focus on the biggest perpetrators instead of the insignificant players. It is imperative to hit the miscreants where it hurts—in the conduits for their ill-gotten gains.

It is well past time to use the miscreants' greatest asset, the underground economy, against them. It seems that many people still remain largely unaware of the underground economy. They remain unaware that the underground economy drives most of the Internet-based malfeasance everyone (largely silently) endures. In the end, almost everything comes down to money. Certainly, the stated reasons for an action might be religious or nationalist, but those actions are funded by only one thing—*money*. The underground is a reflection of the real world, and to ignore it is to ignore the real world.