How Cyber Criminals Works

Cyber crime has become a profession and the demographic of your typical cyber criminal is changing rapidly, from bedroom-bound geek to the type of organized gangster more traditionally associated with drug-trafficking, extortion and money laundering.

It has become possible for people with comparatively low technical skills to steal thousands of pounds a day without leaving their homes. In fact, to make more money than can be made selling heroin (and with far less risk), the only time the criminal need leave his PC is to collect his cash. Sometimes they don't even need to do that.

In all industries, efficient business models depend upon horizontal separation of production processes, professional services, sales channels etc. (each requiring specialized skills and resources), as well as a good deal of trade at prices set by the market forces of supply and demand. Cyber crime is no different: it boasts a buoyant international market for skills, tools and finished product. It even has its own currency.

The rise of cyber crime is inextricably linked to the ubiquity of credit card transactions and online bank accounts. Get hold of this financial data and not only can you steal silently, but also – through a process of virus-driven automation – with ruthlessly efficient and hypothetically infinite frequency.

The question of how to obtain credit card/bank account data can be answered by a selection of methods each involving their own relative combinations of risk, expense and skill.

The most straightforward is to buy the ‘finished product’. In this case we’ll use the example of an online bank account. The product takes the form of information necessary to gain authorized control over a bank account with a six-figure balance. The cost to obtain this information is $400 (cyber criminals always deal in dollars). It seems like a small figure, but for the work involved and the risk incurred it’s very easy money for the criminal who can provide it. Also remember that this is an international trade; many cyber-criminals of this ilk are from poor countries in Eastern Europe, South America or South-East Asia.

The probable marketplace for this transaction will be a hidden IRC (Internet Relay Chat) chatroom. The $400 fee will most likely be exchanged in some form of virtual currency such as e-gold.

Not all cyber-criminals operate at the coalface, and certainly don’t work exclusively of one another; different protagonists in the crime community perform a range of important, specialized functions. These broadly encompass:

Coders – comparative veterans of the hacking community. With a few years' experience at the art and a list of established contacts, ‘coders’ produce ready-to-use tools (i.e. Trojans, mailers, custom bots) or services (such as making a binary code undetectable to AV engines) to the cyber crime labour force – the ‘kids’. Coders can make a few hundred dollars for every criminal activity they engage in.

Kids – so-called because of their tender age: most are under 18. They buy, trade and resell the elementary building blocks of effective cyber-scams such as spam lists, php mailers, proxies, credit card numbers, hacked hosts, scam pages etc. ‘Kids’ will make less than $100 a month, largely because of the frequency of being ‘ripped off’ by one another.

Drops – the individuals who convert the ‘virtual money’ obtained in cyber crime into real cash. Usually located in countries with lax e-crime laws (Bolivia, Indonesia and Malaysia are currently very popular), they represent ‘safe’ addresses for goods purchased with stolen financial details to be sent, or else ‘safe’ legitimate bank accounts for money to be transferred into illegally, and paid out of legitimately.

Mobs – professionally operating criminal organizations combining or utilizing all of the functions covered by the above. Organized crime makes particularly good use of safe ‘drops’, as well as recruiting accomplished ‘coders’ onto their payrolls.

Gaining control of a bank account is increasingly accomplished through phishing. There are other cyber crime techniques, but space does not allow their full explanation.

All of the following phishing tools can be acquired very cheaply: a scam letter and scam page in your chosen language, a fresh spam list, a selection of php mailers to spam-out 100,000 mails for six hours, a hacked website for hosting the scam page for a few days, and finally a stolen but valid credit card with which to register a domain name. With all this taken care of, the total costs for sending out 100,000 phishing emails can be as little as $60. This kind of ‘phishing trip’ will uncover at least 20 bank accounts of varying cash balances, giving a ‘market value’ of $200 – $2,000 in e-gold if the details were simply sold to another cybercriminal. The worst-case scenario is a 300% return on the investment, but it could be ten times that.

Better returns can be accomplished by using ‘drops’ to cash the money. The risks are high, though: drops may take as much as 50% of the value of the account as commission, and instances of ‘ripping off’ or ‘grassing up’ to the police are not uncommon. Cautious phishers often separate themselves from the physical cashing of their spoils via a series of ‘drops’ that do not know one another. However, even taking into account the 50% commission, and a 50% ‘rip-off’ rate, if we assume a single stolen balance of $10,000 – $100,000, then the phisher is still looking at a return of between 40 and 400 times the meagre outlay of his/her phishing trip.

In large operations, offshore accounts are invariably used to accumulate the criminal spoils. This is more complicated and far more expensive, but ultimately safer.

The alarming efficiency of cybercrime can be illustrated starkly by comparing it to the illegal narcotics business. One is faster, less detectable, more profitable (generating a return around 400 times higher than the outlay) and primarily non-violent. The other takes months or years to set-up or realise an investment, is cracked down upon by all almost all governments internationally, fraught with expensive overheads, and extremely dangerous.

Add phishing to the other cyber-criminal activities driven by hacking and virus technologies – such as carding, adware/spyware planting, online extortion, industrial spying and mobile phone dialers – and you’ll find a healthy community of cottage industries and international organizations working together productively and trading for impressive profits. Of course these people are threatening businesses and individuals with devastating loss, financial hardship and troubling uncertainty – and must be stopped.

On top of viruses, worms, bots and Trojan attacks, organizations in particular are contending with social engineering deception and traffic masquerading as legitimate applications on the network. In a reactive approach to this onslaught, companies have been layering their networks with stand alone firewalls, intrusion prevention devices, anti-virus and anti-spyware solutions in a desperate attempt to plug holes in the armoury. They're beginning to recognize it's a failed strategy. After all, billions of pounds are being spent on security technology, and yet security breaches continue to rise.

To fight cyber crime there needs to be a tightening of international digital legislation and of cross-border law enforcement co-ordination. But there also needs to be a more creative and inventive response from the organisations under threat. Piecemeal, reactive security solutions are giving way to strategically deployed multi-threat security systems. Instead of having to install, manage and maintain disparate devices, organizations can consolidate their security capabilities into a commonly managed appliance. These measures combined, in addition to greater user education are the best safeguard against the deviousness and pure innovation of cyber-criminal activities.

|  |
| --- |
|  |