Cybercrime

Scribe: Nick Hay

October 29, 2012

1 1. Be evil 2. ??? 3. Profit!!

Assume you can hack into machines. What can you do if you're evil? How can you make money? (Can you?)

To set the context, google for fullz. These contain full information for identity theft: logins and passwords for gmail, paypal, ...; credit cards; driver ids. Widely available, advertising blatantly on open forums; stolen goods too. (Or so they claim.)

- Steal online banking account info. What can we do? Really stupid to transfer to your account; banks can reverse the transaction, you can easily be caught.

  Buy bitcoins? US exchanges have to verify your identity. Worse, bitcoins are not actually anonymous: all transactions are public, and although users can have separate wallets, with work you can piece together identities.

  Webmoney, eGold, western union. These are options (see later).

- Sell compute cycles or access to machine. Compete with EC2. But have to find some other criminal to buy from us.

- Sell stolen credentials to other criminals.

- Corporate espionage. One problem with your reputation: the companies need to be willing to deal with you.

  Two major manufacturers for Pay TV smartcards competing. One hired security experts to break the competitors card, then published on all the forums. They then advertised how much more secure their system was: just look at their competitor's rate of fraud of fraud.

  But, they got caught doing this.

- Blackmail (personal) - affairs, porn. Compromise their machines, try to discover incriminating information. Challenge: very labor intensive. Machine learning to find incriminating evidence?

- DDOS / corporate extortion. "You have a nice gambling site, sure would be a shame if something happened to it...." Can work with sites that are solely web-based, that work in a gray area and might find it hard to go to the police e.g. online gambling and lottery; not clear if they're legal.

  Rumour between security professionals: a number of banks extorted, sometimes pay the money to avoid the bad publicity.

- Ransomware. Haven't seen so much Really nasty: encrypt all the data in your harddrive, ransom the key.
- Go "legit" and work for govts.
- Spam. Cooperation between three types of criminals:
  - Spammers/hackers who can find people to sell to.
  - Rogue employees in the factories in India, make/take extra drugs off the books.
  - Wholesalers who connect the two.

  Turns out there are two major wholesalers which handle fulfillment, payment (constantly shifting between banks), relationships to the rogue employees.

  The spammer/hacker affiliates' sites redirect to the wholesaler's for payment. Low barrier to entry.
- Credit card numbers.
- Ads, click fraud, ad theft. One of the few ways to get money from electrons. Click fraud malware. Ads can be paid per impression, or per click. The Google's of the world need to deal with this. Very difficult to detect if humans or malware are clicking.
- Pirate bay. Offer torrents, have ads. Very difficult today. Have to have content, lots of competitors. If the site is too sleazy, ad networks refuse to do business with you.
- Ad theft. Browser extension injecting ads into other people's websites. Act like a very popular website. Bad guys redirect DNS for doubleclick or other ad servers, to their ads.
- Private investigator / people search website. Technical hacking to a degree, but mostly social engineering. Convince a contact in a phone company to get reverse mapping of an unlisted number.
- WoW/digital goods. With stolen financial info, buy world of warcraft account. Or, hack into accounts, steal all their items, sell to legitimate players.
- Sell hacked computers as anonymous proxies; $10 a year?
- Hack companies.
- Fake antivirus; scareware (website pops up windows scanning machine). Make it looks like underlying operating system (can look pretty convincing). Scare people. If you think they're evil, you won't click on it, but if you do you probably think it's legit. Very low complaint rate.

There's a significant risk in all these. You have to accept payment from victims, they may be able to track you. If you drop off money in certain locations, the police can stake it out. The risk has to be pretty low if you want to repeat this a number of times.

There are lots of bad things bad guys can do, but it's surprisingly hard to extract money from this.

This gives an answer to why are credit cards being sold so cheaply, if they purportedly have large limits on them: its really hard to turn them into money.

- Risk tax. 1% risk of being caught each time...
- Ripper tax. No honor among thieves; significant chance it's worthless, so have to price that into this.

2 Market for lemons

Consider the market for used cars. There is asymmetric information: the buyer knows whether their car is good or not, but the seller is not sure. Suppose there are two cars:

- Lemon. Terrible. Worth $5000.
- Lime. Wonderful. Worth $9000.

Suppose 1/2 are lemons, 1/2 are limes, and the buyer cannot tell which is which. They are willing to pay $7000, except the limes won't accept this so the buyers get all lemons. Limes drop out of the market, now the buyers just get lemons. Buyer drop out if lemons pretend to be limes (by only accepting $9000). Only equilibrium point: limes drop out.

The solution is to reduce information asymmetry:

- Independent assessment.
- Random samples (cryptographic protocol to enforce this).
- Reputation system.

3 Specializations in the underground economy

There is structure in the underground economy. This specialization is very interesting from an economic perspective. Different roles:

- Admin. Run the markets; help buyer and seller find each other; fight rippers.
- Cashier. Low expertise; high risk. Get cash from cloned ATM card and get money from system; split 50/50. Pick up Western union money transfer.
- Confirmer. Western Union transfers money to a branch and has it held for pickup. Person gets cash into hand; irreversible way to get cash into hands. Policy: if you want to do a suspicious transaction, have to call WU on the phone, prove they are them.

  Confirmers do this, advertising the voices they can do.
- Mule. Evolved into widespread (nasty) scam. Attacker gets into bank account of small business, transfer thousands of dollars. They know this will be detected and reversed, so they transfer the money to the mule, get them to transfer 80% to WU or another account and keep the remainder. This could be a cashier's or tellers check (few people know that these can actually bounce). A week or two later, the transaction is reversed, law enforcement comes after the mule....

  Typically advertised by: "make lots of money to work from home". "We need a local financial agent, who has a bank account, is detail oriented..."

  This looks like an attack on the small business, but is actually an attack on the mule.
- Drops. Pick up physical goods. Attach new shipping stick, ship elsewhere. Significant fee.

4 What can we do?

How to fight this? Follow the money. Monetization is the hardest thing to do, so make this harder. Increase the risk tax.

- Fight monetization. Really cool idea: make end users more secure by financial measures and bank policies. Study bad guys, the understand economy, find choke points in the value chain e.g. there are five banks handling transactions. Stop attacks from earning money.
- Law enforcement fights the markets which blocks specialization. When LE were told about one particular market, it seems like they were doing nothing for long time. However, they had been slowly infiltrating these markets, then shut down in a sequence of very successful operations.

  Operation firewall:

  - Prosecute one of the admins of the main website.
  - FBI took over handle of admin.
  - Fake admin offered VPNs and hosting, secretly provided by FBI.
  - Got info about other five admins.
  - Went after them one by one, took them out.
  - This one guy then rose all the way to the top.
  - Tracked what everyone was doing for 1 year doing nothing but watching.
  - In one day: coordinated raids, arresting 100 people.

Evolution in security. Up to about 2003-2005 attacks were overwhelmingly done by vandals for fun and bragging rights. After this the kinds of attacks fundamentally changed, went up hugely in scale, motivated by profit.