Trust & Trade

Matthew Edwards

Focus: Security Economics

November 15, 2020

Section 1

IRC Carding Markets

2006: IRC analysis

Entire IRC networks are devoted to cybercriminal trade. Mostly card details from compromised vendors, but also lively secondary services economy and malware trade.

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

IRC: Sales

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

IRC: Support Services

```
<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
```

IRC: Moderation

Typically a self-regulating process for dealing with rippers.

```
<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
```

IRC: Specialisations

Typically advertised through bots spamming channels.

```
<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
```

cashiers people who extract funds from accounts given details.

drops both physical addresses, and stolen accounts used to launder funds;

IRC: Cashiers

Responsible for getting funds out of accounts and evading fraud checks. Sometimes also extract money in person from transfer services like Western Union.

Take a cut (usually 50%) for the risk they take, need to trade on their reputation.

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

When accounts are held by a female, male 'cashiers' struggle to extract funds. Thus, gender-based services at a premium (remember: heavy male bias).

IRC: Drops

Service charges between 30-50% of the take.

Physical drops often ship via homes/businesses, with owner having no idea what is in package. Usually stolen or fraudulently-obtained goods. Location can be critical, due to restrictions on overseas shipping (demand highest for U.S. drops).

```
<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
```

Section 2

Cybercrime Exchanges: Carding Fora

Carding Fora

Simple web forums (e.g., phpBB), operated either in the open or by closed invite-only schemes.

Products offered for sale by creating a thread, often with a sample to prove authenticity. Customers respond either in the thread or via PM.

Major categories of good:

- **CVVs** credit card numbers (incl. name, expiration, security code).
- **dumps** scans from magnetic strips of cards, for physical cloning.
- **fullz** full information on the cardholder, including e.g., DOB, social security.

Goods Pricing[1]

Prices for CVV can vary significantly, from $\approx$ \$0.50 to \$20.00, average cost of \$10.00. Major factors are the card type and region.

Dumps and fullz have an average price of more than \$30.00 each, reflecting easier access to funds.

[1] Haslebacher A, Onaolapo J, Stringhini G. "All your cards are belong to us: Understanding online carding forums". In *2017 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 41-51). IEEE.

Market Properties

Substantial imbalances in the markets. Up to 70% of sellers attract no obvious business, while a few top users can dominate 40-50% of all business.

Forums are profitable for high-profile traders, but hard for newbies to break into. Buyers vouching for sellers is a strong indicator of success.

Limited escrow systems (with a cut to administrators) exist to counteract the risk of fraud, but underused.

Section 3

Cybercrime Exchanges: Cryptomarkets

How Bitcoin+TOR Set the World on Fire

Traditional problems for cybercriminals

- Financial system checking/investigating use of stolen accounts, catching cashiers at point of extraction, shutting down payment processors.
- Forum/chat servers being located and seized by police, taken over and used to identify buyers by IP address, leading to arrests.

Meanwhile, in the cypherpunk movement

- Development of decentralised, cryptographically-backed currency that would lie outside of traditional institutional controls.
- Development of practical 'onion' anonymisation routing network (TOR), so servers and clients don't know each other's address.

Silk Road

"Silk Road doesn't really sell drugs. It sells insurance and financial products, [...] It doesn't really matter whether you're selling T-shirts or cocaine. The business model is to commoditize security"

Nicolas Christin

- Hosted as a hidden service.
- Posts authenticated and secured with public-key cryptography.
- Use escrow schemes to pay sellers only on receipt.
- Sellers post bonds before selling.
- Buyers always rate sellers after purchase (lemons).
- SR paid a percentage of transactions.

Silk Road: Summary

The market was viewed primarily as a safe, reliable ‘last mile’ of drug distribution. Political/ethical motivations, echoes of cypherpunk origins, all contributed to appeal.

Most major scams on the market were due to ill-advised ‘early finalisation’.

The market survived for an impressive 2-year run from 2011 to 2013, despite massive press and law enforcement interest, before being taken down by a targeted investigation that led to the arrest of the owner, “Dread Pirate Roberts” Ross Ulbright.

Silk Road: Aftermath

After the dramatic takedown in 2013, the number of sellers on competitor and newcomer markets *increased*. The online crypto-drug-market was *growing* either in spite of or *because of* law enforcement interventions.

As technology became more widely understood, markets proliferated. Hundreds of cryptomarkets. Many ran **exit scams**.

Despite subsequent large-scale action by law enforcement, including mass takedowns of marketplaces in 2015, cryptomarkets are still around.