The Underground Economy

CDT Threats & Risks: Session 8

Matthew Edwards

Dec. 5th, 2019

Section 1

Orientation

Overview

1. The botnet economy.
2. IRC exchanges.
3. Exploit & carding fora.
4. The modern darkweb.

Section 2

Botnets & Spam

Spam: Advertising gone wild

Business model: cheap product + low-value, low-return advertisement.

1. Harvest email addresses
2. Write spam email
3. Send spam in bulk
4. Process orders from responses

Single successful spam campaigns can generate up to $1 million in revenue, and sustained programmes can be multi-million-dollar industries.

Harvesters

Deploy crawling infrastructure, sometimes distributed across a number of machines.

Often run 'off the shelf' harvesting software ("ECrawl", "Email Harvester").

Seen spoofing the Google bot, even coming from a Google AS.

Turnaround times range from 5 days to 1 year.

Botnets

Modern email system effectively prevents bulk email from a single sender.

Spammers turn to distributed system of compromised machines.

Typical example: Curtwail

- Machine is compromised, executes a *loader* (Pushdo)
- Loader identifies victim system, contacts botnet C&C server, downloads malware modules, incl. rootkit, spam engine, server list.
- Spam engine spins up, contacts Curtwail C&C, waits for instructions
- Once paid by spammers, Curtwail C&C server provides spam template, target list, configuration file for behaviour.
- Compromised machine then uses spam engine to send email.

Curtwail continued

At the client-facing end, Curtwail presents a nice web interface for spammers (available in Russian or English).

All configuration options can be specified, including email header spoofing, etc. Local instances of SpamAssassin used to validate and tweak campaign effectiveness.

Includes an instruction manual, and a dedicated support team that help with setup and delivery.

Botnet competition

Botnet operators sometimes outsource the 'install' process, paying others to get their loader onto a machine (typically affiliates pushing traffic to drive-by-downloads).

Botnets can be competitive, often identify and delete other malware from victim systems, even applying security patches in order to retain ownership.

Bots query blacklists to learn their own reputation. Operators struggle to maintain capacity – bots available can drop by 50% per day.

Payments from spammers were the lifeblood of the botnet economy until $\approx$ 2013. \$100-\$500 per million emails. Returns were highly concentrated in a few key players. Infighting!

Spammer services

Some spam is also a scam (e.g., phishing), but a lot are genuine products, with attendant requirements:

- Taking customer payments
- Shipping goods
- Customer service

E-commerce software sold specifically for spam operations.
Outsourced customer service, shipping specialists, etc.

Spam economics

Conversion rates are terrible. Study of Storm botnet:

469 million	spam emails sent;
0.01%	actually reach an inbox;
0.005%	*of those* are clicked on;
28	people (0.000006%) purchased something.

Most successful campaigns use custom email lists not covered by other campaigns ("fresh").
Values of email addresses sold on fora are customised per provider (free webmail worth less than others) and region.

Follow the money

Researchers identified that there was a payment bottleneck in the spam economy[1]

Just **3** banks were providing payment processing for 95% of spammers studied.

New banks and payment processors were difficult and expensive for spammers to recruit. Subsequent enforcement action (in collaboration with card companies) crippled the flow of money into the ecosystem.

---

[1] Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Félegyházi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H. and McCoy, D., 2011. "Click trajectories: End-to-end analysis of the spam value chain". In *2011 IEEE Symposium on Security and Privacy* (pp. 431-446). IEEE.

The system adapts

Spam value faltered, intensifying internal competition. Some workarounds for scammers (money transfer services like MoneyGram, Western Union; giftcard economy), and phishing still profitable, but not 'legitimate' spam business.

Alternative revenue streams emerged to make use of botnets:

- Increased focus on (existing) financial malware, and associated reselling economy.
- Click fraud
- Cryptomining
- Ransomware

Section 3

Cybercrime Exchanges: IRC

2006: IRC analysis[2]

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

[2] Cymru, T., 2006. "The underground economy: Priceless". *login*, 31(6).

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
```

Other 'drops' are bank accounts for moving money.

IRC: Developments

The trust-based ecosystem is always somewhat fragile. Scams and fear of scams are constantly visible.

IRC in particular has slowly lost favour, with web fora becoming more central to carding.

Law enforcement 'whack-a-mole' – distribution means new servers always spring up. Sting operations sometimes more valuable, but persistent security awareness (VPNs) makes this burdensome for targeting minor players.

Section 4

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[3]

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.

[3] 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.

While most are generalists, some sellers specialise in particular products (e.g., PayPal credentials specialist), and seem to offer cheaper products.

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

Section 5

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.

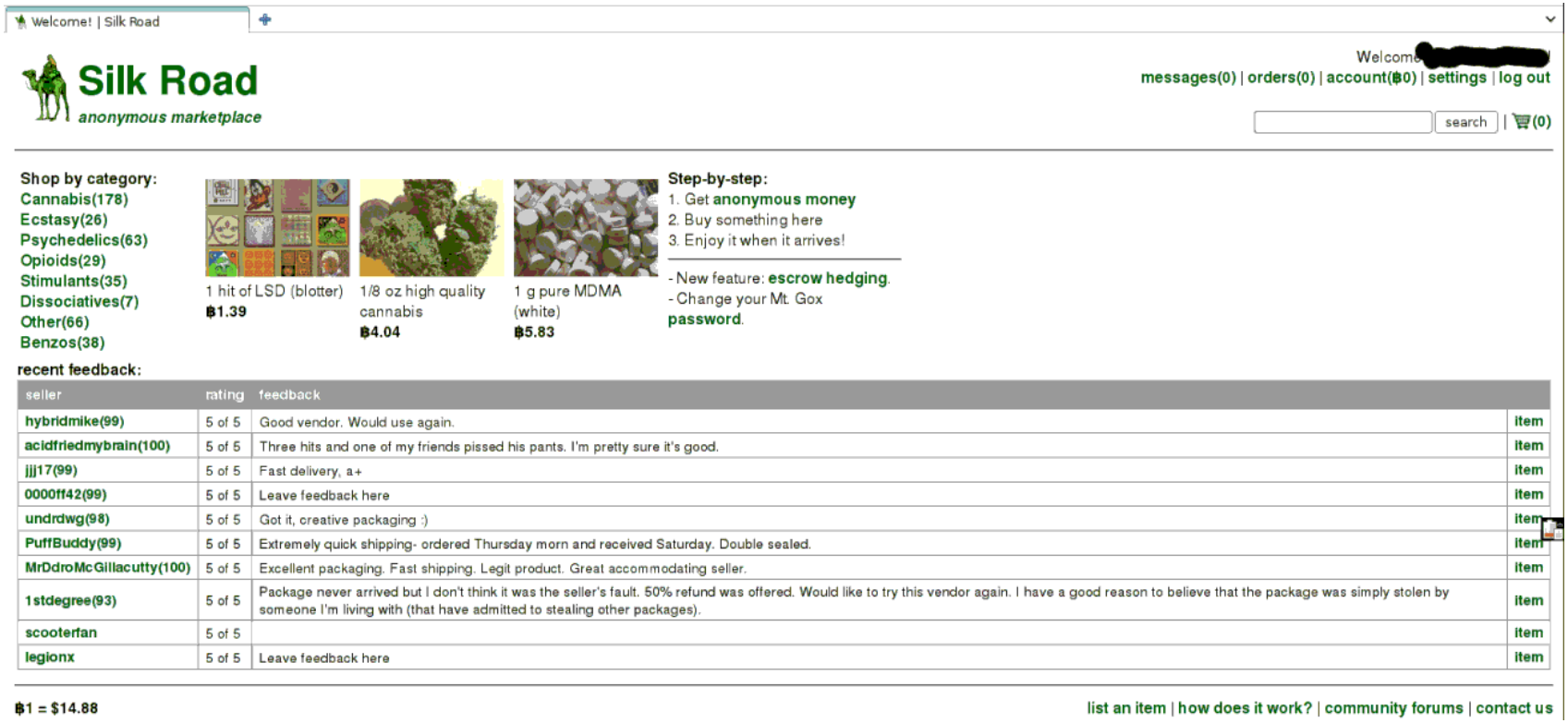
Silk Road

"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

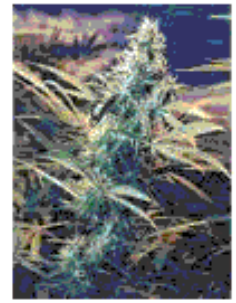

Welcome! | Silk Road
Silk Road
anonymous marketplace
Welcome [redacted]
messages(0) | orders(0) | account(฿0) | settings | log out
search | (0)
Shop by category:
Cannabis(178)
Ecstasy(26)
Psychedelics(63)
Opioids(29)
Stimulants(35)
Dissociatives(7)
Other(66)
Benzos(38)
1 hit of LSD (blotter)
฿1.39
1/8 oz high quality cannabis
฿4.04
1 g pure MDMA (white)
฿5.83
Step-by-step:
1. Get anonymous money
2. Buy something here
3. Enjoy it when it arrives!
- New feature: escrow hedging.
- Change your Mt. Gox password.
recent feedback:
seller | rating | feedback
hybridmike(99) | 5 of 5 | Good vendor. Would use again. | item
acidfriedmybrain(100) | 5 of 5 | Three hits and one of my friends pissed his pants. I'm pretty sure it's good. | item
jjj17(99) | 5 of 5 | Fast delivery, a+ | item
0000ff42(99) | 5 of 5 | Leave feedback here | item
undrdwg(98) | 5 of 5 | Got it, creative packaging :) | item
PuffBuddy(99) | 5 of 5 | Extremely quick shipping- ordered Thursday morn and received Saturday. Double sealed. | item
MrDdroMcGillacutty(100) | 5 of 5 | Excellent packaging. Fast shipping. Legit product. Great accommodating seller. | item
1stdegree(93) | 5 of 5 | Package never arrived but I don't think it was the seller's fault. 50% refund was offered. Would like to try this vendor again. I have a good reason to believe that the package was simply stolen by someone I'm living with (that have admitted to stealing other packages). | item
scooterfan | 5 of 5 | | item
legionx | 5 of 5 | Leave feedback here | item
฿1 = $14.88
list an item | how does it work? | community forums | contact us

Silk Road

Shop by category:
- Drugs(1964)
  - Benzos(147)
  - Cannabis(698)
  - Dissociatives(35)
  - Ecstasy(165)
  - Opioids(128)
  - Other(222)
  - Psychedelics(239)
  - Stimulants(193)
- Apparel(3)
- Art(26)
- Books(130)
- Collectibles(1)
- Computer equipment(7)
- Digital goods(96)
- Drug paraphernalia(37)
- Electronics(8)
- Food(1)
- Forgeries(13)
- Home & Garden(2)
- Jewelry(1)
- Lab Supplies(9)
- Medical(3)
- Money(91)
- Services(44)
- Weaponry(21)
- XXX(53)

Ephedrine HCL 2000mg (250 x 8mg)...
฿10.67

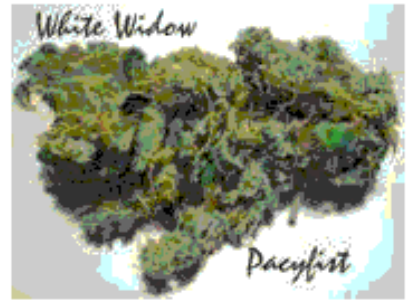
1 Gram 2C-I
฿18.87



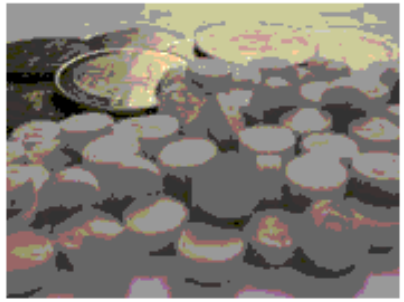
11 Titans Haze Seeds by Flying...
฿9.50

500 LSD tabs - Buddha/Ganesha
฿410.19

50 LSD tabs - Buddha/Ganesha
฿56.13

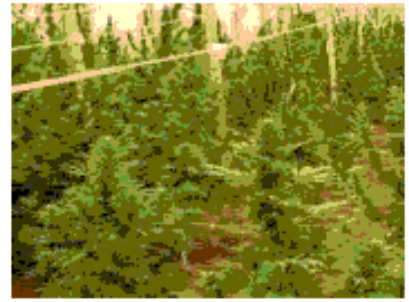


4 gram WHITE WIDOW SUPER QUALITY...
฿12.38



20x - Sonic - very good press...
฿34.46

10 Chronic Seeds by Serious
฿15.89



13 Reserva Connoisseurs Mix Seeds...
฿6.91

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.

Lots more!

If any of you are interested in this line of work for your PhD, I'm very keen to supervise or otherwise support it.

Next Week

Meeting on **Friday** (still at 11pm), rather than Thursday (swapping with Richard's RI module).