Cyber Crime

The world of Spam, Malware, Drugs and Scams

Agenda

- The Story of Everyday Cyber Crime
- How does the Cyber Crime Supply Chain work
- Revenue in Cyber Crime
- Why cant we stop it?
- Affiliates and Affiliate Programs
- Spam Value Chain
- Legal Limitations

Cyber Crime

- Theft by leveraging computer systems or electronic media
- Encompasses everything from Spam, Malware, Keyloggers, Rootkits, Exploits, Social Engineering, etc…
- The objective is simple

Make Money

And a LOT of it

The Emergence

- In the last decade, Emergence of Profit making malware
  - Anti Spam -> More Value for Spam
- Commoditisation
  - Value added compromise
  - Each entity has some value
- Sophistication in Malware
  - Higher market for goods

Business Models

- Advertising via Spam
- Theft via Keyloggers, Phishing
- Fraud via Fake AV etc…
- Extortion via DDoS, Ransomware
- Support Services for supporting all above

Elements of the Economy

- Illicit Goods
    - Tier -1 (Credit Card Data, PayPal, etc…)
    - Tier -2 (Bots, Exploits, Malware, Accounts)
    - Tier -3 (Money Laundering Schemes)
- Online Markets
- Scams
    - Spam, Phishing, DDoS, Extortion, etc…
- Liquidation
    - Indirect: More Spam (Potentially Legal), Stock Pump/Dump
    - Direct: Cashout, (Web Money, Money Mules,) (Recently: Bitcoin)

SPAM!

- Cost of Spam
  - > **100 Billion Spam emails sent per day**
  - Billions in direct costs
- But it exists because - **Its Profitable**
- Documented evidence of $100M/y for Russian Pharma Spam
- Pharmaceutical goods, Replica Goods, Software, Pornography, Gambling, etc…

Affiliate Programs

- Provide franchise business for advertisers
    - Content » Web page templates, advertising literature
        - Payment services » Visa/MC – typically via third-party structure
            - Fulfilment » Goods relationship, drop shipping
                - Customer service
- Individual affiliates paid on commission basis
- Many advantages:
    - Push risk to spammers
    - Efficiencies due to outsourcing advertising innovation



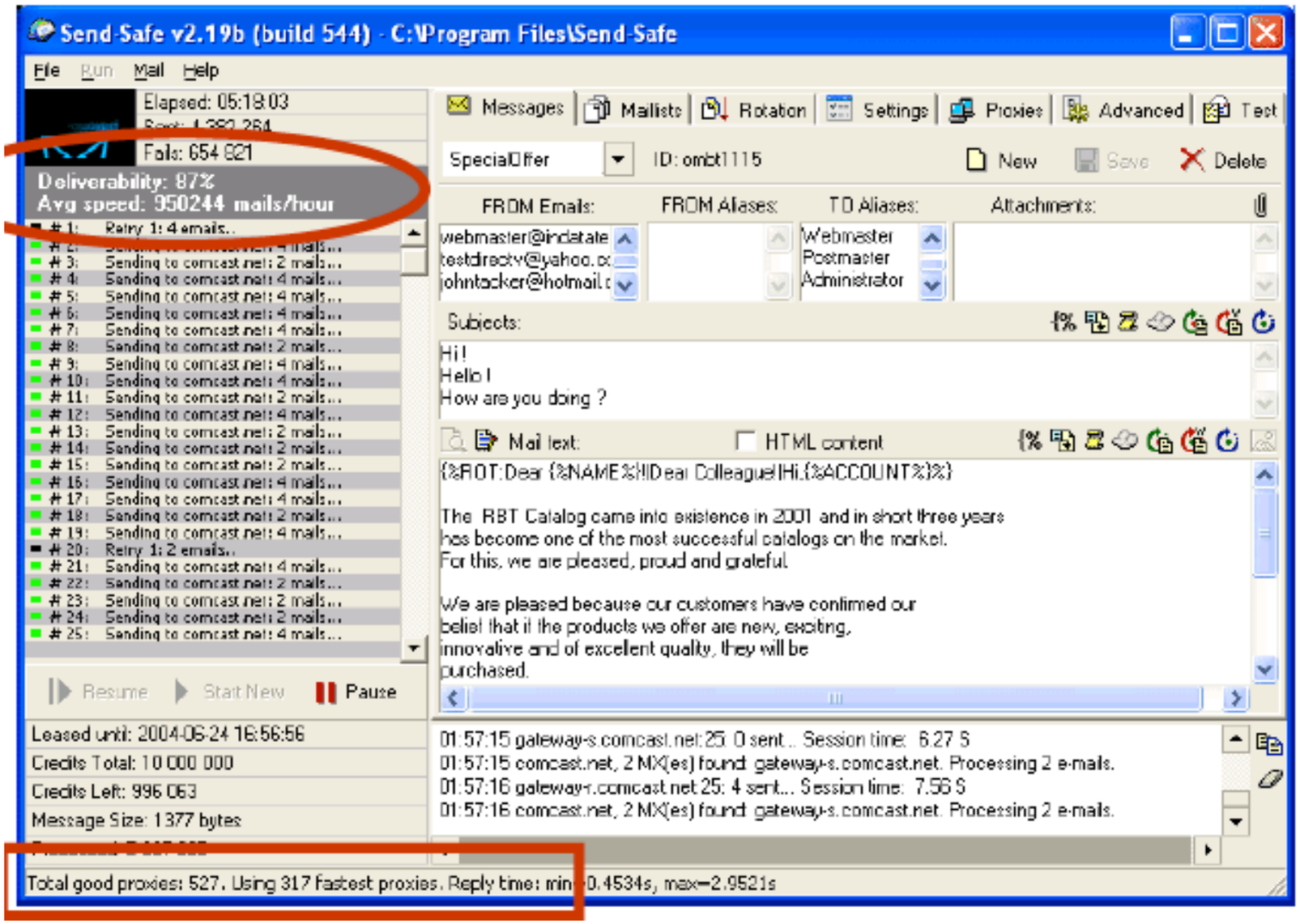






But why Spam?

- Can send email to anyone
- Can send email “from” anyone
- Can send email with any content
- Can send email as fast as you want
- Natural Advertising Channel



Send Safe

950244 Mails/Hour

Side Note: Botnet

- Network of Compromised Hosts
- Central Machine to command them all

- A bot-master can
  - Send Spam
  - Denial of Service
  - Steal Local Data
  - etc…

History of Botnets

- IRC Based Bots
  - Eggdrop
- DDoS
  - eBay attack
- Malware
  - Storm
  - Zeroaccess, Zeus

Innovation

- Before 2000, spammers could generally get away with sending lots of spam from a single server
  - Spam-based blacklists become into being
  - “Don’t accept e-mail from IP address 132.239.4.5”
    - Effectively forces spammers to send from many
- Different IP address
  - First solution: open proxies
  - Mail servers that will accept mail from any source
  - Provokes blacklisting of such servers
- **Botnets provide a better solution (2004/5)**

Arms Race

What we did	What they did
Real time IP Blacklisting	Send via relays/proxies
Clean up open relays/proxies	Delivery via Compromised Botnets
Content Based Learning	Polymorphic Spam, Spam Generators
Site Takedown	Fast Flux DNS, Transparent Proxies
CAPTCHAs	CAPTCHA Outsourcing, OCR

Rent Spam-Bot

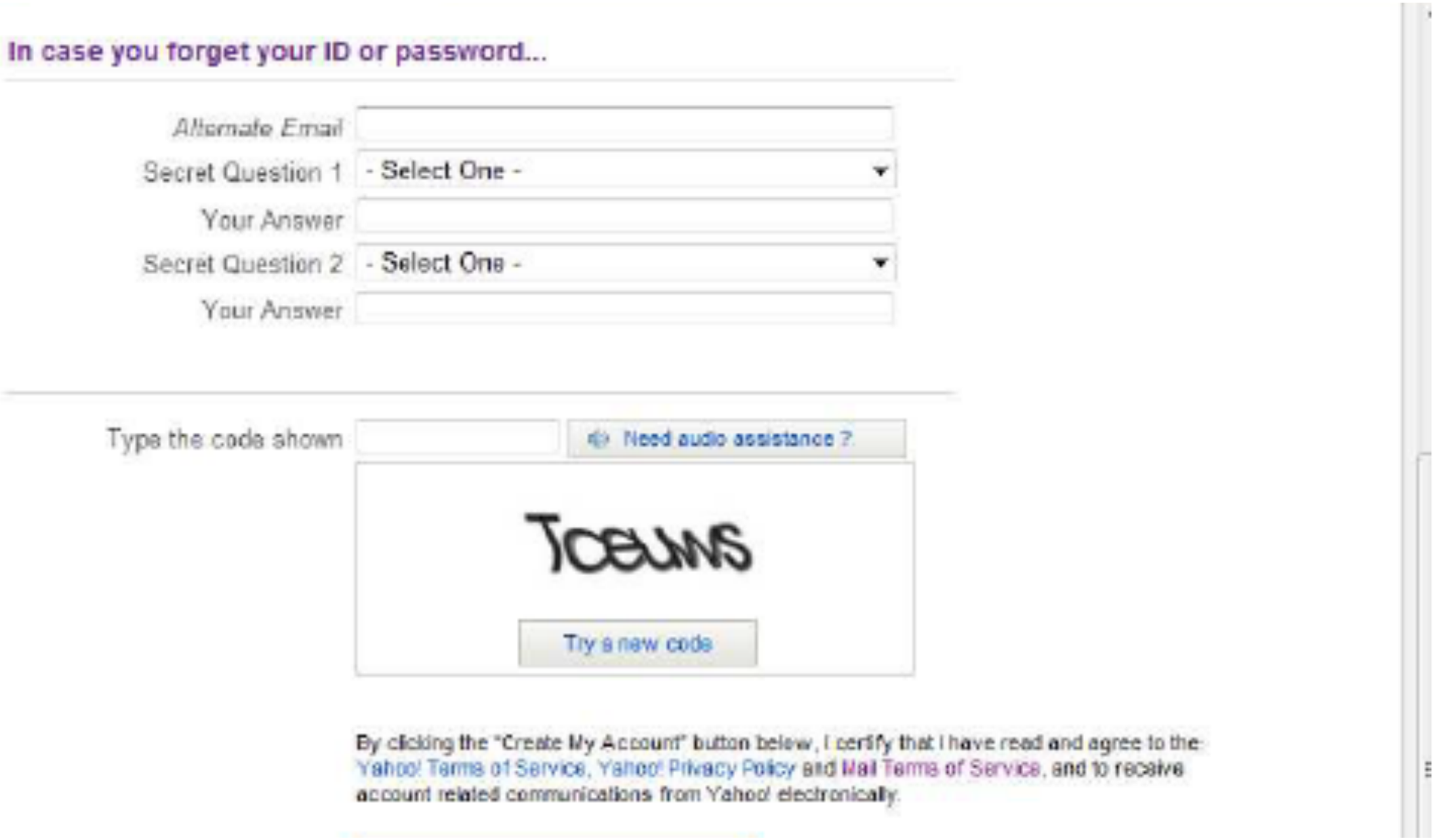
Bring to your attention the updated version of the lease Spam Bot

System description:

+ Flexible and convenient WEB Admin, information in protstsese departure, change any settings (Appendix mail databases, text, macros).
+ Intuitive interface admin panel - easy to start sending ...
+ Intelligent choice to send such a bot would not you think about those protstsese and concentrate on your business.
+ Permanent update bot! Four programmers work on a daily basis to build the system. You only get a notice in ICQ already on the installed apdejtam ...
+ Vybrny bot type dispatch enables a maximum precision measurement inboks letter.
+ Optionally available condition monitoring your system to our qualified Spam engineer.
It supports your desired number of bots in the network, monitors Black boots,

Pharma Spam Value Chain

The Silk Road and TOR



CAPTCHA

Completely Automated Public Turing Test to Tell Computers and Humans Apart

Costs

- Retail Price

$1 = 1000 CAPTCHAs

- Wholesale will be far far lesser

Koobface

- Spread by spamming 'friends' from compromised accounts
- Distributed fake-AV
- Web browser hijacking
- Highly profitable
- Facebook named suspected operators
- Stanislav Avdeyko (leDed), Alexander Koltyshev(Floppy), Anton Korotchenko (KrotReal),Roman PKoturbach (PoMuc), Svyatoslav E. Polichuck (PsViat and PsycoMan)

Credential Theft

- Harvesting information
  - From point-of-sale: skimmers
  - From users: phishing
  - From user machines: information stealers; banking trojans
  - From server systems: data breaches
    - Extrapolation from other broken accounts
- Trading information
  - “Carder” forums
- Monetisation
  - Re-shipping
  - ATM/POS cashout (white plastic)
  - Western Union/MoneyGram
  - Role of Cashiers and “Mule” networks

Malware PPI

- PPI
    - Purchases compromised hosts from affiliates
    - Resells to clients
    - Decouples machine compromise from use
- Affiliates
    - Compromise machines
    - Execute the PPI's binary
    - Called a "dropper"
- Clients
    - Pay the PPI
    - Want malware installed
    - Broad array of uses: > Spambots, information harvesting, rootkits, fake AV

Malware Market

- Host compromise
  - Raw exploits (generally private sale only)
  - Exploit packs (packaged exploits in kit form)
  - Compromise as a market service (PPI)
  - Exclusives (typically via some kind of remote desktop tool)
- Payloads
  - Support software (e.g., evasion:rootkits,packers,AVtest, VMProtect)
  - Standard packages (Info stealers, spammers, proxy systems)
- Entire service offerings
  - Whole botnet: compromised hosts with payload installed
  - Typically for infostealing or spam
- **Innovation driven by pressure on uses of malware**

Current version 2.2.1 prices:

$400 - 1 License

1 License includes:

+ Domain locked one domain (subdomains unlimited)

+ **2** new domain builds if blacklisted

+ Support

+ Minor updates for free

+ Discount on new releases

Extras:

1. Domain re-build for other domain ($ 50)

*** NOTE: YOU ARE NOT ALLOWED TO RESELL / SHARE, IF WE CATCH YOU DOING THIS YOUR LICENSE WILL BE REVOKED ***

2. AV-Cleaning ($ 80 first time, $ 50 after)

Bottom Line

- Robust, diverse market for criminal enterprises
- Modest capitalisation sufficient to drive innovation
- Rapid evolution over short time periods
- Organised only loosely

- Indirect threat:
  - Marketplace available to all actors
  - More sophisticated targeting