No Plan Survives Contact
Experience with Cybercrime Measurement

Chris Kanich    Neha Chachra    Damon McCoy
Chris Grier    David Wang    Marti Motoyama
Kirill Levchenko    Stefan Savage    Geoffrey M. Voelker

UC San Diego
UC Berkeley
Security Experiments

- Modern testbeds enable controlled study:
  - DDoS defense, Routing security…

- Passive measurement captures real-world malice:
  - Prevalence of BGP hijacking, DNS attacks…

- But some questions require actively engaging with an adversary:
  - How much can you earn solving CAPTCHAs?
  - Do spammers steal your CC or send you pills?
Engaging the Underground Economy

Started in 2006 with numerous projects since:

• Early infrastructure supporting scams [Security07]
  • Crawl network & host infrastructure from 1M spams

• CAPTCHA-solving ecosystem [Security10]
  • Customer and worker for 8 CAPTCHA-solving services

• Spam value chain [Oakland11]
  • Crawl infrastructure for 1B spams, 100s of purchases

• Order volume, customer demand [Security11]
  • 100s of purchases, inference of revenue & demands

• Freelance marketplace of abuse jobs [Security11]
  • Crawl 7 years of Freelancer.com, hire workers to validate
Requirements

• We have learned the hard way that engagement has two key requirements

• Verisimilitude
  - Attackers defend themselves
  - Need to appear as who they expect
  - Makes engaging at scale more challenging

• Scale
  - Attackers operate at scale
  - Have to engage at scale to observe big picture
  - Need infrastructure to collect, analyze huge data

• Goal: Explain methods and lessons learned to help future security researchers with similar goals
Two Kinds of Engagement

Cover two kinds of engagement in this talk:

- **Engagement as an underground peer**
  - Buy cybercrime software, CAPTCHA solutions, Facebook Likes, …
  - Appear to be a “normal” cybercriminal
  - These guys don’t take VISA! (much less English…)

- **Engagement as a customer**
  - Crawl 100s of millions of URLs, buy 100s of items
  - Appear to be a “normal” customer
  - At scale requires sophisticated identity management
INTERMISSION
Engaging in the Underground

Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

ПРИЕМУШЕСТВА

🔗 Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миксы стран по вашему выбору.
🔗 Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
🔗 Договоритесь по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!
Underground Forums

• Miscreants openly describe their activities and methods on underground forums & IRC
  - Tremendous source of useful information
  - Learned much about affiliate programs
• Forums also serve as a marketplace for buying and selling digital goods
  - Items, quantities, prices, contacts, …
Underground Purchases

• Kinds of purchases we made
  ▪ CAPTCHA services ($3,400)
  ▪ Underground software ($640)
  ▪ Hiring freelance workers ($2,100)
  ▪ Web mail accounts…

• All negotiated online
Sale of accounts: Yahoo, Gmail, Aol, Hotmail, Mail.ru, Yandex and others.

Yahoo.com 1K = 8 $
Gmail.com 1K = $ 11
Hotmail.com 1K = $ 10
Aol.com 1K = $ 30
Mail.com 1K = $ 10

GoogleGroups
Mail.ru 1K = 9 $
Yandex.ru 1k = $ 10
Pochta.ru 1k = 9 $

Buy Akki? It's easy!
When ordering from 10k discount of 20%.
Flexible system of discounts when working with regular clients.
The same work under the order (other services), knocking - discuss.

ICQ 425-448-092
e-mail: [To view this link to Register]
Challenges and Lessons

• Language and culture
  - Russian (human translated) was critical
    » Group member is a native speaker
  - Full of slang, interaction requires a real voice

• Means of payment
  - Visa/MC/Paypal not accepted
  - WebMoney/LibertyReserve popular
  - Non-reversible online transactions

• IP address cloaking not necessary
  - Can do it from your desk: IM and VPNs effectively hide IP origination
Engaging as a Customer
Visiting Their Sites

When visiting 1B URLs over three months...

- Full-featured browsers necessary for verisimilitude
  - **Redirection**: Flash/javascript, clicking on popups, …
  - More danger, more complexity, beefier machines
- IP diversity is **necessary** at scale
  - **Deterrence**: You will get blacklisted, plan for it
  - Cloud providers and IP-hiding services easy to use
Crawling Challenges

• Blacklisting by bad guys
  - Hierarchical IP space usage

• Scale
  - Dozens of machines, 100s of browsers/machine
  - Central dispatcher, distributed client

• Poisoning by bad guys
  - A spammer started inserting well-formed junk URLs
  - Added an importance-based crawl scheduler
#!/bin/bash

tables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -F INPUT
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p udp --dport 53 -j DROP

if [ "$1" = "zeus" ]
then
  sh google_block.sh
  sh zeustracker_block.sh
fi

iptables -A INPUT -s 149.20.54.132 -j DROP #pt1b.phishtank.com
iptables -A INPUT -s 149.20.54.134 -j DROP #pt2b.phishtank.com

iptables -A INPUT -s 133.5.16.238 -p tcp -m multiport --dports 80,443,8080 -j DROP #HidemaruMail SpamFilter Agent Kyushu University
iptables -A INPUT -s 198.134.135.0/24 -j DROP

#University of California at San Diego FAKE UA,REF
iptables -A INPUT -s 216.163.176.0/20 -j DROP #Commtouch Inc.
iptables -A INPUT -s 95.211.120.0/24 -j DROP #leaseweb.com BAD BLOCK
Purchasing as a Customer

• How to do this at scale?
  ▪ 100s of purchases, $17K spent on items + shipping

• When buying from an online pharmacy you need:
  ▪ Name, shipping address, email, phone number
  ▪ IP address from which to make the purchase
  ▪ Method for receiving and cataloging the goods

• And you want to collect:
  ▪ Virtual properties (site ID, communication style)
  ▪ Financial properties (VISA BIN, Bank name)
  ▪ Physical properties (where from, active ingredient)
Identity Management (Corporeal)

• Originally: Pseudonyms + “P.O. Box”
  ▪ Specialty issuer: no pseudonyms
  ▪ High volume spooked the P.O. Box guys

• State of the art: real names + home addresses
  ▪ Ordering legal, end user goods
  ▪ Odd orders, but our money is green

• Prepaid cell phones + add’l Google Voice #s
  ▪ Difficult to know which order/customer call is for
  ▪ Required on-the-spot creativity at times
Identity Management (Virtual)

- Email through Google Apps free account
  - Can create nonce address for each purchase
  - gmail/hotmail/ymail increases fraud score
- Purchase from SD residential IP addresses
  - IP Geo-location important for fraud score
  - VPN tunnel to home machine, 3G, stay home and buy drugs
Financial Transactions History

Proposed Treasury rules take hard line against prepaid card fraud
Move to help take on terrorist funding may impact average consumers, too

By Jeremy M. Simon

The government's efforts to crack down on criminal financing could make it tougher for consumers to buy gift cards, some experts warn.

- Couldn’t get BIN information
- Tried several other consumer-level cards
- CARD act is a major setback here
- Called several specialty issuers
- Specialty issuer finally played ball with us
  - Manual, batch-based process

Collecting data by phone very error prone
Internal red tape

• As involved as solving the technical problems

• Extensive oversight
  - Legal oversight
  - Research oversight

• Build trust slowly, incrementally
  Our capabilities are the result of years of trust-building
Final Takeaways

- Full-fidelity crawling architecture necessary for verisimilitude
  - But increases challenges for achieving scale…
- Underground forums provide “finger on the pulse”
- Acquiring payment data was priceless
- Engagement can lead to serendipitous opportunities