

# Phishing – What Happened?

- + 1980s Hacker Culture
  - Mostly Harmless, rarely malicious,
- + 1990s Internet Vandals
  - + Mostly attention seeking juvenile delinquents
    - + Typical attack: Social Engineering of Journalists
  - + Often Malicious, rarely for monetary gain
- 2000s Professional Internet Crime
  - + The Juvenile Delinquents have grown up
    - + This is their job
    - + This is only the start
  - + Spam: The true face of 'cybercrime'
    - + 419 Advance fee frauds, Consumer frauds, Hijacked software, Phishing
  - + Brand Impersonation Phishing
    - + The current, most blatant tactic



## The Basic Plan

The cyber criminal can break their head against the steel walls of the bank's Internet security plan, or they can take the easy approach and just ask customers for the username and password for their account. This turns out to work rather often.



## **Phishing Tactics**

#### Hack a Merchant Site

Hope the merchant is silly enough to leave database of plaintext card
#s

#### + Pretend to be a Merchant

- + You give me your credit card number, I will give you hijacked software
- + Old tactic, spam filtering may have made it unprofitable

#### Pretend to be a Trusted Brand

- + Or how to get the undivided attention of the brand owner
- + Risky, but can be profitable

#### + Trojan a Machine

- Load spyware onto a consumer machine
- Currently a boutique approach



# Phishing Attack Components

#### + Capture Site

- + Usually a Zombie host or ISP account bought with phished card#
- Impersonates a merchant or trusted brand
- + Takes the username/password, card #s, SSN, etc.

## + Means of Advertising Capture Site

- Usually Spam sent out from Zombie hosts
- Often uses misleading domain name [payments@brand-billing.com]

#### + Means of Covering Tracks

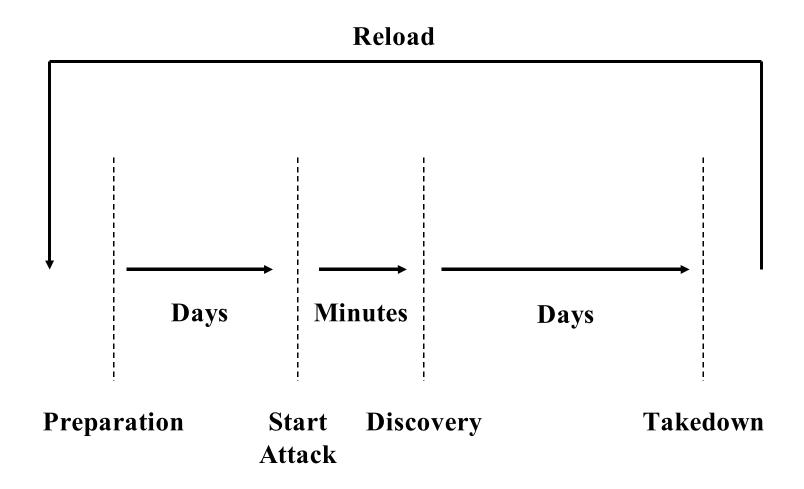
- + Recover data from the capture site
  - + Often use US hosted email provider
- + Internet Cafes are popular

## + Its Easy to get Caught

+ Several successful phishing prosecutions, many pending



# Phishing Attack Timeline





# The Phishing Value Chain

- + Botnet Acquisition
  - + Strong evidence that botnets are being traded to phishing gangs
- + Arms Suppliers
  - + Successful phishing gangs have access to sophisticated technology
  - + Phishing tools with full Windows GUI interfaces recovered
- + Phishing Spammers
  - + Specialize in evading spam filters
- + Carding gangs
  - + Phished data is sold on to specialists in exploitation
  - Existing organized crime rings



# Some Phishing Myths

- + It is hard to get the attention of foreign law enforcement
  - + Police can easily understand the crime and its seriousness
    - + A story that looks good in the papers in any language
    - + Organized crime is usually perpetrating domestic crime as well
  - + Even corrupt police (usually) demand a change of target
- + Foreign ISPs are unwilling to take action
  - + Once the language issue is addressed action is usually immediate
  - + Some US ISPs will wait on legal advice
    - Usually comes as "Shut down the machine immediately"
- Phishing is an Easy Crime
  - + If this was the case specialization would not be necessary
  - + The only easy part is getting caught



