Phishing:
Can we measure the real risk?

Dr Richard Clayton

(joint work with Dr Tyler Moore & Henry Stern)

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

TWENTY-SEVENTH INTERNATIONAL SYMPOSIUM ON ECONOMIC CRIME
3rd September 2009

What is “phishing”

- Person receives email from their bank indicating their information must be updated
- URL looks convincing

  `http://session-10999042.www.mybank.com.info80.cn`

- Website looks convincing: so they login…
- Billion dollar losses occurring
  - exact amounts remain secret (except GB, FR)
  - “key loggers” and “man in the browser” attacks also occur, but phishing significant in many countries

Previous research results

- Studying phishing since early 2007
- Identified how technical innovation (such as “fast-flux”) has led to longer lifetimes
- Showed how “mule recruitment” sites ignored by the banking industry [ISEC XXV 2007]
  - no-one’s problem tackled by no-one
- Showed how the “take-down” industry was failing to cooperate [ISEC XXVI 2008]
  - 3.5 hours when known, 3.5 days when unknown

Have now looked at “spam”

- Email spam clearly important; it’s the main reason that people visit the fake websites
  - so combined spam data with website data
- Measured all the phishing spam sent to Ironport in period June to December 2008
- Also measured all the brand new phishing websites in the last week of September 2008

The website dataset

- 4084 different attacks on “free” webhosts (~25%) and compromised machines (~75%)
  - each site attacks just one bank
  - total lifetime of all these sites = 20603 hours
- 120 “fast-flux” domains (set up by a small number of gangs hosting sites on “botnets”)
  - domains may host attacks on multiple banks
  - total lifetime of all these domains = 9674 hours
- ie: ratio of lifetimes is about 2 to 1

The email spam dataset

- Ironport detected only 11% of the 4084 standard phishing attacks
  - about 1/3 of total phishing email volume
  - for some attacks saw just one email!
- But, detected 86% of the 120 fast-flux domains
  - about 2/3 of total phishing email volume
- ie: ratio of email spam is also 2:1
  - note that the 2:1 is the other way around

Fast-flux is more organised

- Spam for fast-flux domains started at almost the same time for “everyone”, and stopped abruptly when the domain was removed
  - probably automated systems under gang’s control
- Spam for some of the other sites trickled in weeks before the website came to wide attention – and would sometimes continue for several days after the site was removed!
  - manual systems, and outsourced spam sending

Who should we chase ?

- Fast-flux:
  - send more email, so more people may go to sites
  - BUT email is relatively easy to filter
  - seems to be a small number of organised gangs
- Others:
  - websites stay up longer, so overall exposure is more
  - email more likely to get through
  - may be chasing hundreds of “kids in bedrooms”
  - but if those kids didn’t feel quite so immune…

In practice…

- Police forces apparently concentrating on just one of the “fast flux” gangs
  - “amount of loss” rules preclude most targets
- Occasional arrests of “money mules”
  - no impact on the main criminals
- Occasional arrests of individual phishers
- Main risk to the banking sector remains loss of confidence and the necessity to return to a “bricks and mortar” High Street presence

Phishing:
Can we measure the real risk?

http://www.lightbluetouchpaper.org

UNIVERSITY OF CAMBRIDGE
Computer Laboratory