Robbing a bank with a computer (and what happens next)

Dr Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

CyberSecurity

29th November 2011

“Security Economics”

Security Group,

Computer Laboratory,

University of Cambridge

- Big focus on “security economics” the new (since about 2000) approach to the understanding of computer security
- Looks more at the “economics”; less at the “computer science”
- E.G. Who will lose money if this security problem is not addressed (and therefore has an incentive to fix it) ? But who did the security design and is actually in a position to fix it ?

Phishing (historic)

- Phishing dates back to the 1990s (stealing AOL accounts)
  - but took off for banking from 2003 onwards
  - the “underground economy” allowed criminals to specialise
- Initially used confusing domains: http://barklays.com
  - with a poorly spelled email threatening you with account closure
- Then phishers discovered that people didn’t understand URLs
  - http://www.barclays.com@example.com
  - http://www.barclays.com.example.com
  - http://www.example.com/barclays.com
- Next step was to stop using fixed websites
  - in “fast flux” hostname points at a relay (a machine from a botnet)
  - in 20 minutes time it points at a different relay

Phishing (today)

- Many attacks on non-banks (and the return of domain names)
  - http://eu.battle.net-account-blizzard-en-wow.in
  - http://www.battle.net.service-blizzard.net
  - attacks on HMRC (really attacks on credit cards)
- The fake web pages are now mainly in attachments
  - it’s considerably more complex to explain to a hosting company why a website with code to accept the HTTP POSTs should be disabled
- Moore&Clayton research results:
  - fake websites removed within 4 hours …
  - … or 4 days if bank does not know they exist
  - when URLs detected, no incentive to share them “for free”
- Data also revealed slow removal of “mule recruitment” websites
  - currently out of fashion, but were lasting ~13 days
  - no-one’s specific problem, so no-one deals with it

Malware

- Malware is general term for “malicious software”
  - never was very useful to distinguish virus / worm / trojan etc.
- 1980s-1990s Brain, LeHigh etc
  - spread on floppy disks – mostly harmless
- 1990s-2000s Melissa, ILoveYou etc
  - spread by email, still a very small number of variants
- Malware today spread by:
  - email (still! lots of examples stopped by your spam filter)
  - drive-by infection (on both good and bad websites)
  - over the network and via memory sticks (eg Stuxnet of course)
- Often every sample is different (so AV stats are meaningless)
  - “server side polymorphism” gives everyone a different copy
  - “if you see two samples the same, it’s a false positive”

Banking malware

- Zeus / SpyEye etc
  - these are families of malware
- Produced on a commercial basis
  - Zeus is (was?) sold ($700-$15K) to criminals
- Web server acts as C&C (Command and Control)
- Infected machines pass credentials back to server
  - captures FTP, email, banking, etc. usernames and passwords
- Some criminal gangs concentrating on business banking
  - much more efficient for the criminals to steal in $100K lumps from large businesses, school districts etc.
- Law enforcement having some impact
  - arrests made, servers disabled: and if the C&C is “sinkholed”, they learn the IP addresses of the machines that are making contact…

Cleaning up malware

- Inspection of C&C data yields IP addresses
- ISP ownership of IP addresses is known (RIPE, ARIN etc)
- BUT only the ISP knows which customer has which IP address
- So reports of malware infection must be forwarded by the ISP
- Many (most?) ISPs do not bother to do this
  - anyway, the customer may ignore an email message
  - expensive to phone them up (~8 months of profit)
- Some non-compete agreements (NL, DE, AU)
  - everyone has to call users, so all must factor costs into their prices
- Some free clean-up services (notably in DE)
- Almost no ISP proactively looking for infected users
  - Comcast an important exception (checks DNS for resolving of C&C)

DNSChanger

- Gang arrested Nov 9 used malware to change the IPs set by end-users for DNS servers; so hijacked search engine access
  - they made their money from displaying adverts
- Their software also interfered with AV updates
  - hence users at risk of all sorts of other infection
- FBI (and friends) currently running the DNS servers
  - hence they know IPs of the infected machines
  - feed of this data is available (26,158 IPs in UK ... to 23 Nov)
- ISPs need to clean up their customers before these DNS servers are turned off (and their users then have no working Internet)
- Will be fascinating to see whether this self-interest will make ISPs more incentivised to inform their users of their problem!

http://www.cl.cam.ac.uk/~rnc1

http://www.lightbluetouchpaper.org

Dr Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

CyberSecurity

29th November 2011