A Year's Evolution in Attacks Against Online Banking Customers

Matthew W A Pemble
Information Security Crystal Ball
Phishing, Trojans & other scams

- Despite appearances banks are actually (ish) secure
- Home-user security is terrible
- Serious, **professional**, organised crime
- Go where the money is:
  - Compromise bank staff
  - Place bank employees
  - Attack the communications chain outside of the Bank’s control
  - Attack the customers (and their computers)
The situation at Singapore

- Significant increases in basic numbers
  - Majority of attacks still non-financials
  - Attacking biggest English-speaking orgs
  - US / Aus / NZ / UK + ?
- Rapid rise in use and utility of trojans
- Losses (corporate) still low
  - Absolutely
  - Compared to other fraud (card, 419 etc)
  - Compared to cost of solution
Where are we now?

- Concentration on money making
- More sophistication in strategy
- More sophistication in technology
- Mule recruitment
  - More effort
  - Fewer mugs?
- Use of non-internet channels for initial theft
- First 4 / 5 / 6 (BIN) “email personalisation”
- More languages (German, French, Spanish & …)
  - spulling dreadful still
  - and grimer
“Nothing is worse than active ignorance”
*Goethe*
Phishing – main trends

• Flat simple numerics
  • Inexorable rise in finance attacks
  • Significant (lesser) rise in reported losses
• Change of tack
  • Non-English (at last 😊)
  • Failure of non-strong auth (Tan etc)
  • Focus on smaller institutions (UK & US)
  • Demand for (and use of) telephony credentials
• Technical sophistication of supporting infrastructure
• Balkanisation
• Nigerianization
“Weak” hosting

• Single email
• Extremely poor English
• No geographical customisation (i.e. $ not £)
• Single host (hacked virtual hosting box)
• DNS
  • Often on the same box (old)
  • Or by legitimate server owner (ISP)
• No resilience in site
• New kit wave within 3 hrs of site takedown.
“Strong” Hosting

- *This is not the “Rock” group MO.*
- 1 email wave – standard wording
- Up to 4 “confusingly similar” domain names
- “Fraudster friendly” registrar
  - + don’t work weekends 😞
- Separate DNS
  - “Sensible”, fraudster owned, DNS service domain
  - 5 live A records at a time
  - Slow rotation (≈ 30 mins)
- Botnet hosting
  - 30 + IP addresses seen in 32 hr lifetime
What does this mean?

- 2-factor approaching economic
- Attributable cost of IR on order of financial loss
- Education appears to be reducing customer response
  - But when you get an attack after 14 months …
- Inter-bank recovery rates are consistent to improving
- Wider scale spam filtering seems to be helping
- Grip slowly tightening on phishing gangs
- Law Enforcement effort needing
  - Low value crime, international & difficult
“Spear-Phishing”

• Pick your definition
  • Well targeted attack (only genuine customers)
  • Attacking only one email domain
  • Personalising attack emails
• Scripted emails with unique identifiers
  • Active email / mug verification
  • Avoid dilution & decoys
  • Future proofing
Perseverance is a great element of success: if you only knock loud and long enough at the gate, you are sure to wake up somebody.

*Henry Wadsworth Longfellow*
Pharming

• I would exclude “etc/hosts” changes
• Rare, but difficult to spot
  • Why?
    • Spam is easy, fools are plentiful?
• Spectacularly successful when implemented
• Potential for “transparent proxy”
• DNS surveys suggest wide-scale susceptibility
Trojans

• Remain the “iceberg issue”
• Many customer machines multiply compromised
• Vast range of applicable threats
  • Key-logging
  • Keyword tailored key-loggers
  • Screen scraper
  • Disk search utilities (inc grep)
  • MITM Proxies (Browser Help Objects)
  • Etc/hosts file alterations
Trojan Impact

- Very few customers per identified variant
- Spread between many banks (over 200 in some etc/hosts)
- Auto-updates
- Well-established malware author shops / kits
- Botnet hosting
- Nasty suspicion?
  - What happens to real 1st-party fraud?
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.14.38.190</td>
<td><a href="http://www.halifax-online.co.uk">www.halifax-online.co.uk</a></td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>ibank.barclays.co.uk</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>online.lloydstsb.co.uk</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>online-business.lloydstsb.co.uk</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td><a href="http://www.ukpersonal.hsbc.co.uk">www.ukpersonal.hsbc.co.uk</a></td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>banesnet.banesto.es</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>extranet.banesto.es</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>ebanking.bccbrescia.it</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td><a href="http://www.bankofscotlandhalifax-online.co.uk">www.bankofscotlandhalifax-online.co.uk</a></td>
</tr>
<tr>
<td>24.14.38.190</td>
<td><a href="http://www.rbsdigital.com">www.rbsdigital.com</a></td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>oi.cajamadrid.es</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>bancae.caixapenedes.com</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>banking.postbank.de</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>meine.deutsche-bank.de</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>myonlineaccounts2.abbeynational.co.uk</td>
</tr>
<tr>
<td>24.14.38.190</td>
<td>ibank.cahoot.com</td>
</tr>
</tbody>
</table>
Non-IT Attacks

• Telephony
  • Auto-diallers (espec VOIP)
  • SMS

• Paper
  • Interference with the Mails
  • Statement stuffers

• Marketing departments don’t help
A good End cannot sanctify evil Means;
nor must we ever do Evil,
that Good may come of it.

William Penn
Summary: The state at Baltimore

- Attacks steadily ramping up
  - Spam volumes erratic
  - No real learning on “hook”
  - Minor variations in favourite targets
- $millions per month
- International
  - Multiple languages
  - Transnational targeting
  - West Africans now playing
- Technology improving
- Almost time to do something about it 😊
So what for next year?

• Cleverer targeting
  • Cleaner spam lists
  • More / better personalisation
  • Theft of customer (marketing) databases
• Money movement?
  • Away from Western Union
• Suborned registrars?
• Strong 2-factor transaction data signing
  • 2FA is not enough (though necessary)
Just remember it’s not the only problem …

The “Enron 3”

Donald MacKenzie

Group Security & Fraud

29th June 2006
Some perspective

Phishing & trojans
• Organised crime
• Hundreds of attacks
• £23.2m UK admitted loss
• Thousands of hours ISIRT
• Mostly getting away with it
• Apparently below LE “radar”

Donald MacKenzie
• Business Relationship Mgr
• 5 year rolling scheme(r)
• Prosecuted for ≈ £21m loss
• Loan & dormant account fraud
• 5 man-days
  • Computer & phone forensics
  • Statement writing
• Sent down for 10 yrs on Tuesday 27th June 😊
Questions ?