

"Phishing" - basics and experience in Austria

Some Numbers


- phishtank.com:
 - ~ 400 new phishing websites per day
 - 15.000 active phishing websites
- Anti-Phishing WG: August 2007
 - # unique phishing reports: 25.624
 - # unique phishing sites: 32.079
 - # of brands affected: 129
 - Country hosting the most phishing websites: USA

 - No hostname; just IP address: 16 %
 - Average time online for site: 3.3 days
 - Longest time online for site: 30 days

Botnets

- PCs taken over by malware
 - Drive-by downloads from websites
 - Social engineering via email („greeting cards“)
- Command & Control
 - „bot-master“ can give commands to zombies (Spam, Click fraud, ddos, keylogging, scan, proxy, webserver, update)
 - Central IRC server / channel
 - HTTP
 - P2P mechanisms (e.g. Storm worm)
- Numbers are tricky:
 - 25 % of all PCs are Zombies (Vint Cerf, 2007)
 - Microsoft: Sept update found „Storm“ on 275k of 2.6M PCs = more than 10 %

„Old style“ Phishing

1. Register a domain similar to the bank's
2. Build a fake website, don't bother with SSL, or just use  as favicon.ico
3. Send out spam to lure users to this site
4. Ask for credentials (Passwords, TANs)
5. Transfer money to a „money mule“
6. Pick up laundered cash



A Story of
Spy vs. **Spy**



Taking down the Webspaces

- Banks complain to operator of the webspaces

- Countermeasures:
 - Multiple webspaces, DNS points to active ones
 - Sites hosted on zombies
 - Zombies acting as reverse proxy to real host (no incriminating content on zombies)

Taking down the Domain (1)

- Banks use trademark law to get domains deleted.
- Countermeasures:
 - URL obfuscation like <http://www.bank-of-america.com.%31%43.kufzy.cn/>
 - Don't bother, users are careless and banks use multiple domains themselves. (e.g. boa.security.com does not violate trademarks)

Taking down the Domain (2)

- Banks complain to the nameserver operators

- Countermeasures:
 - Multiple nameservers, delegation data changes as needed
 - Zombies as nameservers
 - Zombies as port 53 proxies
 - Using glue records (no nameservers needed)



Taking down the Domain (3)

- Banks or other parties complain to domain registry / registrar.

- Problems:
 - What legal argument?
 - ◆ Domain itself is often harmless
 - ◆ Owner data often looks legit
 - Normal procedures are too slow to be really helpful



Securing the Banking Site

- Accept the fact that the Internet is not designed to deliver application security

- **The web-application itself needs to be secured**
 - SSL alone is not enough (users don't understand X.509)
 - TANs instead of username/password
 - Indexed TANs
 - Secure authentication (e.g. crypto-token)

- **Countermeasures:**
 - Manipulate the user's computer
 - If the user can't trust his browser, he is really doomed



State of the Art: e-Banking

- Digital signatures with trusted viewer, or
- Two-channel systems:
 - Web is used to enter a transaction request
 - A summary of this transaction plus a confirmation code is sent to the user via a different channel (mobile)
 - User needs to check whether this is correct and then enters that code on the web
- Implementations:
 - Mobile-TAN (SMS as channel)
 - Email is not sufficient (the malware can interfere there as well)

State of the Art: Phishing

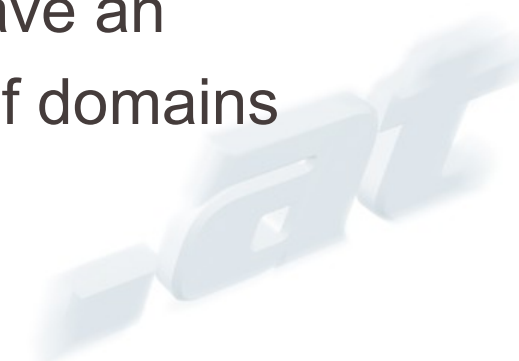
- Browser Helper Objects:
 - Modifies transaction requests on the fly
 - Confirmation screen shows original request
- Not just email / web:
 - Instant messaging
- Massive use of zombies
 - Rockphish gang
- Not just banks + ebay:
 - > generic identity theft



Sidestep: „Spamhaus.org“

■ dispute with Spamhaus.org :

- “nic.at (registry) received list of domains that should be removed because of being used for phishing”
- “other Registries regard the take-down of phishing domains as a high-priority obligation”
- “threat to take action, which could have an adverse impact on our connectivity, if domains will stay active”



Reply from nic.at

- we do in no case support potentially illegal activities e.g. spam, phishing or other crimes
- explained reasons why we cannot withdraw a domain (legal reasons, the domainname itself was not the problem)
- Solution: if we receive a proof of wrong domain holders data, we could withdraw domain according to our T&C



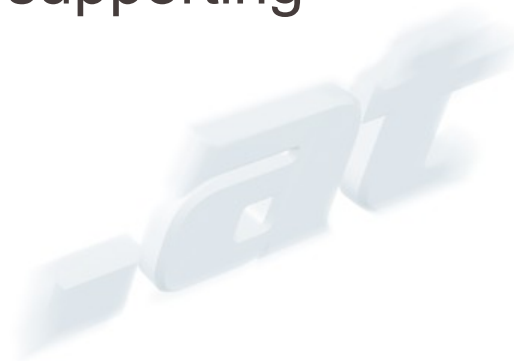
Reply: „Spam Block List“

- various IP-ranges of nic.at were put on Spam Block List from Spamhaus.org
- consequence: majority of e-mails could not be delivered to our domain holders and registrars
- nic.at formally requested IP-range to be deleted from list
- nothing happened



Contacting Spamhaus.org

- try to get in contact with spamhaus.org
- talking to Richard Cox (CIO of Spamhaus)
- english lawyer contacting spamhaus.org on behalf of nic.at demanding immediate deletion of the entry on Spam Block List
- finally most IP-ranges were taken from list, no further technical blocking of nic.at (after 1 week !!!!)
- just a formal announcement, that nic.at is supporting phishing ?????



LIC-Feedback

- broad support from public for our policy
- numerous positive articles in the press
- nevertheless discussion with Austrian LIC on future behaviour of nic.at as registry regarding SPAM / Phishing



Final Board Decision

- nic.at does definitely not support any illegal activities on the Internet
- we do not block or cancel any domains, if it does not violate our T&C
- we follow Austrian Law and Court decisions
- we will inform the relevant registrar and domain holder
- we forward necessary (hidden) information from our database to reporter of spam or phishing to help them
- new e-mail adress: domain-abuse@nic.at



Thank you

Any questions ??

Richard Wein, General Manager nic.at
wein@nic.at

