Phishing and Pharming Attack

Phishing

❑ Dangling "bait" in front of a user.

- Promise of riches/fame
- Urgency (must act immediately)
- Veiled threat (or your account will be locked)
- Pay-off (your banking details, your money, your reputation)

❑ Characteristics

- Poor spelling/grammar/punctuation
- May contain randomly generated-text
- From someone you don't know* … but…

Spear-Phishing

- ❑ Phishing can be targeted to specific companies / groups / individuals.
- ❑ E-mails contain very relevant contents and are plausible.
- ❑ No poor grammar/spelling.
- ❑ Malicious attachments
  - RSA hack
  - Gh0st-NET

More Phishing

❑ Whaling

- Spear-Phishing of CEOs and high profile victims.
- Public information easy to find.

❑ Watering-hole attacks

- Instead of phishing individuals, criminals target web sites and forums where potential spear-phishing victims meet.
- Infect the sites
- Infect the visitors or publish mis-information (spoofed links)

Pharming – no bait needed

- ❑ The goal is the same as phishing – to steal your user name and password.
- ❑ Tools exist for duplicating a web site without the consent or access privileges if site administrator, so these sites are easy to set up.
- ❑ The user needs to look for inconsistencies in the appearance or behaviour of a site.
- ❑ Performing a ***traceroute*** on the domain name will pick up a change in the location of the spoofed site.
- ❑ Plug-ins like Certificate Patrol will detect changes in SSL certificates.

Pharming

❑ Pharming involves setting up fake web sites that users will log into.

❑ **Cybersquatting** - Registering a domain name that is almost the same as the real one. This picks up traffic from users who type in the URI incorrectly. This practice is regulated (and mostly prevented) for the .au domain, but it is not prevented in the .com and other USA domains.

❑ **DNS cache poisoning** so that a user's DNS cache points to the wrong IP address when they have typed in the correct domain name.

Pharming

Links on the page may appear to go to legitimate sites, but actually go to bogus ones rich in scripting and other nasties.

e.g. http://www.e-bay.com/

Actual domain names may be obfuscated:

http://spam-world.net@0xCE.191.0236.0x37/obscure.htm

Log files

How do you know if you're being attacked?

- ❑ Check your bandwidth usage
- ❑ Use *Netstat* / *wireshark* to see what connections / traffic is going in / out of your site.
- ❑ Use tools such as *Tripwire, sfc (Windows)* and *ArpWatch* to detect modifications to system files
- ❑ Look at system logs:
  - /var/log/httpd/access_log, /var/log/httpd/error_log
  - \Windows\System32\Logfiles\MSFTPSVC1\ex*.log
  - \Windows\System32\Logfiles\W3SVC1\ex*.log
- ❑ Use tools like *LogCheck / logwatch* to monitor log files.

Recent Web Security Research: Case Study and Intelligence Trend

- Lekies, Sebastian, Ben Stock, and Martin Johns. “25 million flows later: large-scale detection of DOM-based XSS.” In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 1193-1204. ACM, 2013.
- Lin, Guanjun, Sheng Wen, Jun Zhang, Yang Xiang. “Software Vulnerability Intelligence for Cyber Security: A Survey.” *Proceedings of the IEEE*, 2020. DOI: 10.1109/JPROC.2020.2993293