Evil Searching

Vít Rusňák

Fakulta informatiky
Masarykova univerzita, Brno

PV177 - Laboratoř pokročilých síťových technologií 14. 4. 2010

Obsah

- Úvod do problematiky
- Metodologie sběru dat
- Evil searching
- PhishTank
- Rekompromitace
- Obranné strategie

Zdroj: Moore T., Clayton R.: *Evil Searching: Compromise and Recompromise of Internet Hosts for Phishing*. 13th International Conference on Financial Cryptography and Data Security, Barbados, 2009.

Úvod do problematiky

- Provázanost internetových vyhledávačů s hrozbou phishingových útoků.
- Opětovně kompromitované weby a souvislost s předešlými útoky.
- Využití nedostatků a chyb webových aplikací s různými cíli – spam, šíření malware, ...
- První práce zabývající se touto problematikou s empiricky podloženými daty.

Metodologie sběru dat

- Zdroje dat: Anti-Phishing Working Group [1], dobrovolnické organizace (PhishTank [2], Artists Against 419 [3]), komerční společnosti.
- Sběr probíhal v období říjen 2007 – březen 2008.
- Demografie phishingových útoků:
  - **88 102 (75,8 %)** – kompromitované web servery (nahrání dat na kompromitované servery),
  - **20 164 (17,4 %)** – free web hostingy (využití free hostingů, bez kompromitace),
  - **7 927 (6,8 %)** – použití DNS wildcards a napadených proxy.
- Informace z Webalizeru a web logů.

[1] `http://www.antiphishing.org/`
[2] `http://www.phishtank.com/`
[3] `http://wiki.aa419.org/`

Evil Searching

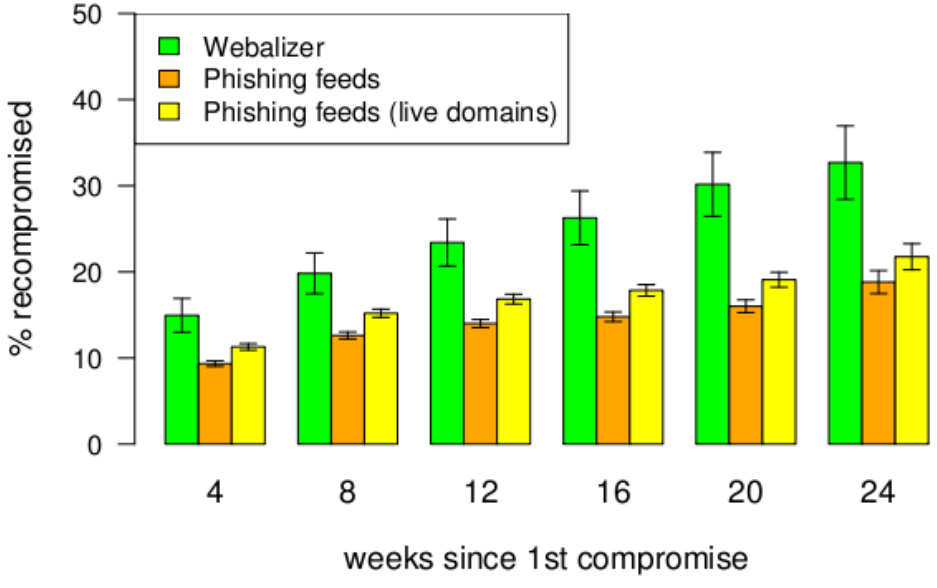
- Využití vyhledávače (nejčastěji Googlu) za účelem škodit.
- Typy:
  - **zranitelnost** – útok na konkrétní verzi aplikace, u které jsou známy bezpečnostní díry,
  - **kompromitace** – hledání existujících phishingových stránek,
  - **shell** – hledání PHP shellů.
- Prokázána souvislost Evil searching s následně napadenými stránkami.
- Zvýšená frekvence klíčových slov prokázána i Webalizerem, ovšem i ten má své limity (20 nejčastějších klíčových lsov).
- Určit přesně rozsah a vliv evil searching je těžké.

PhishTank

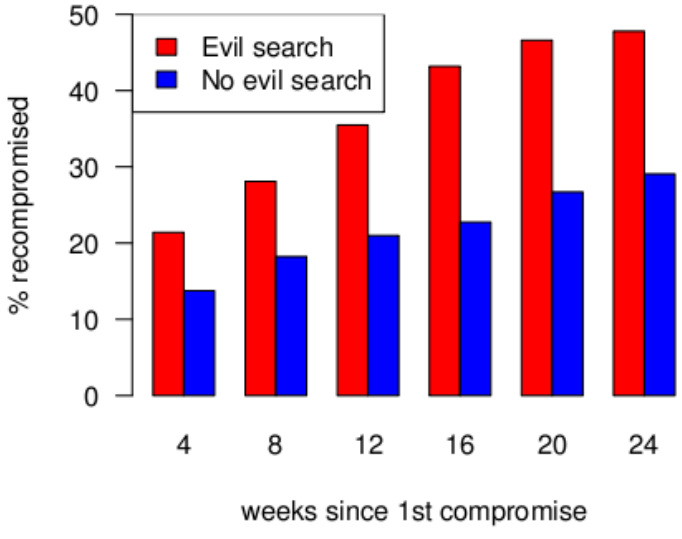
- Volně dostupný „blacklist“ stránek náchylných na phishingové útoky (narozdíl od seznamu APWG, jenž je určen pouze registrovaným členům).
- Permanentně uložené záznamy od roku 2006, ale i aktuální (dynamicky měnící se) seznam.
- Ač se snaží být uceleným seznamem, eviduje zhruba 48 % stránek náchylných na phishingové útoky.
- Je využíván spíše administrátory stránek než útočníky.

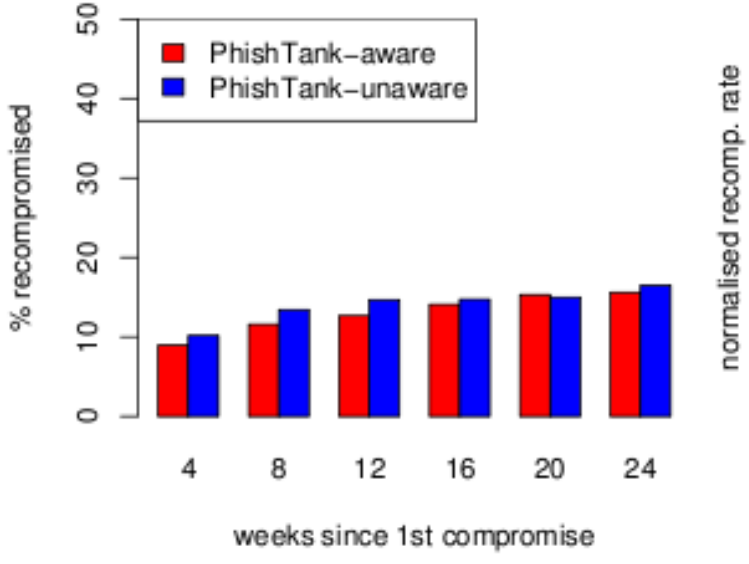
Rekompromitace I.

- Léčba symptomů mnohdy nevede k uzdravení – administrátoři se nepoučí z předešlých chyb.
- Rekompromitace stejným vs. novým způsobem.
- Míra rekompromitace je uvažována jako funkce času $\Rightarrow$ použitá metrika: 4týdenní plovoucí okno.



Rekompromitace II.





Obranné strategie

- Zahalení detailů cíle
- Testování na *evil search*
- Blokování dotazů
- Odstraňování známých phishingových stránek z výsledků vyhledávače
- Snižování reputace již jednou napadených stránek

Díky za pozornost.