Examining the Impact of Website Take-down on Phishing

Martin Jantošovič
jantosko@mail.muni.cz

PV177 - Laboratoř pokročilých síťových technologií

28. apríla 2010

Obsah

Čo je to phishing?

Phishing je proces, kedy sú ľudia lákaní na falošné (podvodné) webové stránky pod zámienkou presvedčiť ich, aby zadali svoje informácie ako sú napríklad užívateľské meno, heslo, adresa, PIN, číslo kreditnej karty, prípadne iné hodnoverné dáta, ktoré sa dajú využiť. Následne sú tieto dáta použité k ukradnutiu identity obete.

Priebeh

- útočníci rozošlú množstvo spamu s URL na ich stránku
- obeť sa pripojí na stránku
- stránka sa snaží imitovať originál
- užívateľ zadá dáta
- dáta sú následne preposlané e-mailom alebo uložené na stránke
- vybieli sa obeti účet :(

Ochrana

- zo strany užívateľa: kontrola URL, spam filter
- zo strany organizácií: postarať sa, aby stránka bola čo najskôr odstránená

(Ideálny) Priebeh obrany

- niekto nahlási podvodnú stránku
- stránka sa pridá do blacklistov
- odošle sa "take-down request"
- stránka sa zneprístupní (ISP, registrar, . . .)

Obsah

Rozdiely

- na kompromitovaný server sa nahrá proxy systém, ktorý presmerováva na back-end server
- back-end server obsluhuje viacero podvodných stránok
- nakúpi sa množstvo domén s krátkym názvom (napr.: lof80.info)
- rozošlú sa e-mailové správy zakaždým s inou URL (napr.: http://www.volksbank.de.networld.id2435432.lof80.info/r1), čím sa zhorší spam filtrom prácu
- vďaka proxy môže byť back-end server schovaný kdekoľvek
- v e-mailoch používajú obrázky

Obsah

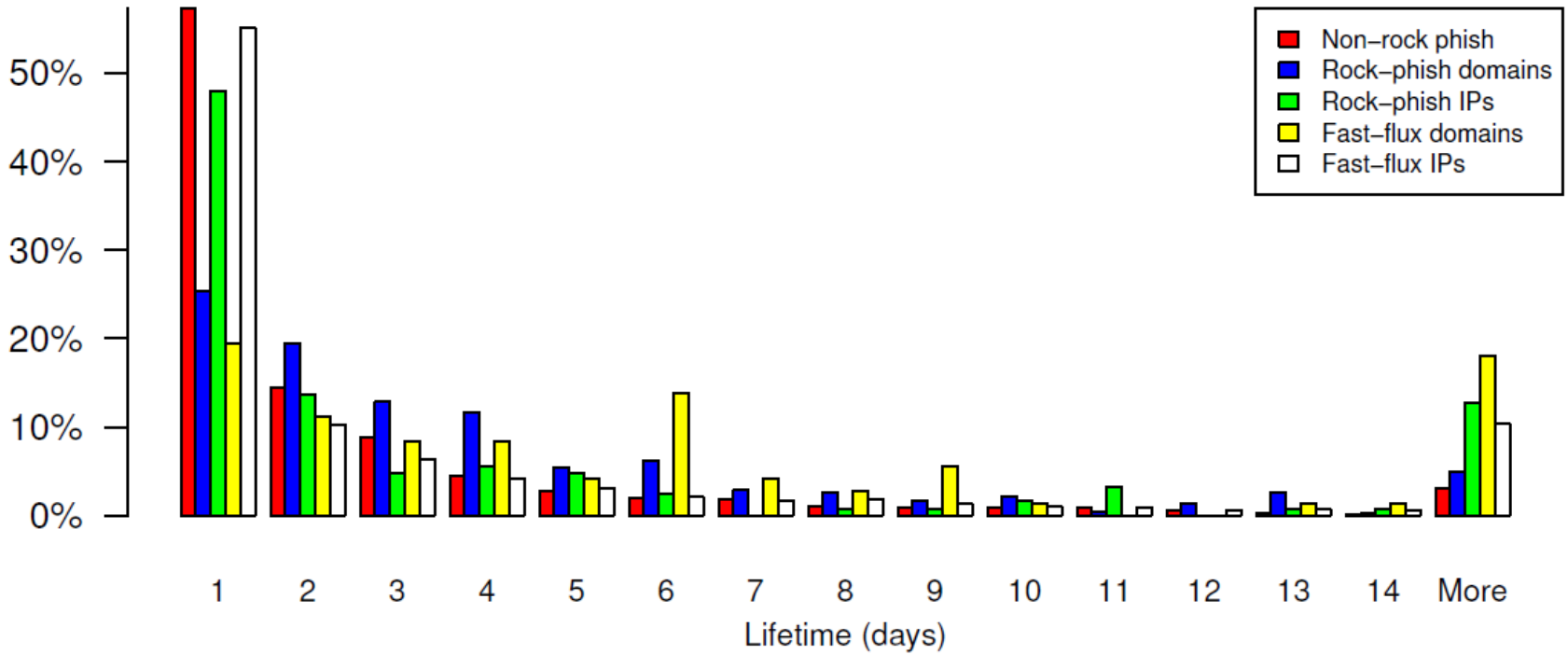
Zber dát

- zber reportov z PhishTank-u
- URL, čas reportu, whois data, screenshots -> chýba čas odstránenia
- pravidelné dotazovanie na hostname, reverse DNS, IP adresu - 2x za hodinu
- ak stránka vrátila 404, bola odstránená z pravidelného testovania, ale stále bola aspoň raz za 48 hodín otestovaná
- údaje o návštevníkoch: z textového súboru na stránke, Webalizer

Štatistiky

- "rock-phish"cez 50% phishing útokov
- životnosť klasickej phishingovej stránky približne 62 hodín (medián 20 hodín)
- životnosť rock-phish domény okolo 95 hodín (medián 55 hodín)
- finančné zárobky klasického phishingu približne $160.4m ročne
- rock-phish približne $320m (iba odhad) ročne

Životnosť



	Sites	Mean lifetime (hours)	Median lifetime (hours)
Non-rock	1 695	61.69	19.52
Rock domains	421	94.68	55.14
Rock IPs	125	171.8	25.53
Fast-flux domains	57	196.2	111.0
Fast-flux IPs	4 287	138.6	18.01

Záver

- približne 18 užívateľov nechá svoje dáta počas prvého dňa
- každý ďalší deň sa k ním pridá 8 nových