
Examining the Impact of Website Take-down on Phishing

Tyler Moore and Richard Clayton
CS, University of Cambridge

APWG eCrime Researchers Summit 07

Phishing

- Tricks people into visiting fraudulent websites
- Persuades them to provide personal data
 - Usernames, Passwords
 - Social Security Numbers
 - Credit Card Information
 - ...
- Attacks
 - Impersonate Victim
 - Empty Bank Accounts
 - Apply for Credit Cards/Loans
 - ...

Anti-Phishing

- Block Phishing Message
- Browser Plug-Ins to detect Fake Sites
- Blacklists and Whitelist
- Take-down malicious Sites



- Phishing Reports from PhishTank
 - URL, Time, Proof Screenshot

ID	URL	Submitted by
940532	http://www.paypalshops.us/	PhishReporter
940531	http://wqedfgre.mail2k.ru/signin-bay-com-ws-BayISA...	PhishReporter
940530	http://grewdsa.mail2k.ru/signin-bay-com-ws-BayISAP...	PhishReporter
940529	http://wefgdewq.mail2k.ru/signin-bay-com-ws-BayISA...	PhishReporter
940528	http://wewfrgfe.mail2k.ru/signin-bay-com-ws-BayISA...	PhishReporter
940527	http://www.promocoestam.com/CadastroPromocoetesTam.c...	fgs
940526	http://www.rap-05.com/ml/login/ci-g/index.htm	PhishReporter
940524	http://peypal-news.com/2/Confirm.php	PhishReporter
940522	http://secuweb.ns11-wistee.fr/paypal.fr/details.ht...	PhishReporter
940521	http://shop.buellhomecoming.com/images/123.gif/www...	PhishReporter
940520	http://csgilogin.lx.ro/SignIncopartnerId2pUserIdsi...	PhishReporter
940519	http://cellcaseworld.com/images/www.paypal.com/pay...	PhishReporter
940518	http://gigifrana.com/aus.php	PhishReporter
940517	http://ttio.sqweebs.com/	PhishReporter
940516	http://onlinesebay.t35.com/confirm.php	PhishReporter

- Where is a Site taken Down?
 - Lookup hostname to IP address
 - Reverse Lookup IP address to hostname
 - Continuous testing, every 30 minutes
 - Fingerprint Content to detect changes
 - Static Phishing Sites

- Visitor Statistics
 - Victim details hosted in plain text under the Site
 - Webalizer and other usage statistics services

Rock-Phish Attacks

- 53% of all PhishTank Reports
- Account for 30% of all Phishing E-mails
- Single Server loaded with 20+ phishing sites
- Compromised Machines run Proxy Instance
- A random short domain e.g. 1of80.info
- DNS resolves *.1of80.info to a Proxy IP addr
- Phishing Mails point to
 - <http://www.volksbank.de.netw.oid3614061.lof80.info/vr>
 - Include random text, GIF image with actual message

Rock-Phish Attacks

- Fast-Flux Phishing Domains
 - ❑ Resolve to a set of 5 IP addresses for a short period of time
 - ❑ Then, switch to another set of IP addresses
 - ❑ Cheap Compromised Machines
 - ❑ Compromised Machine Take-down Impractical

Rock-Phish Statistics

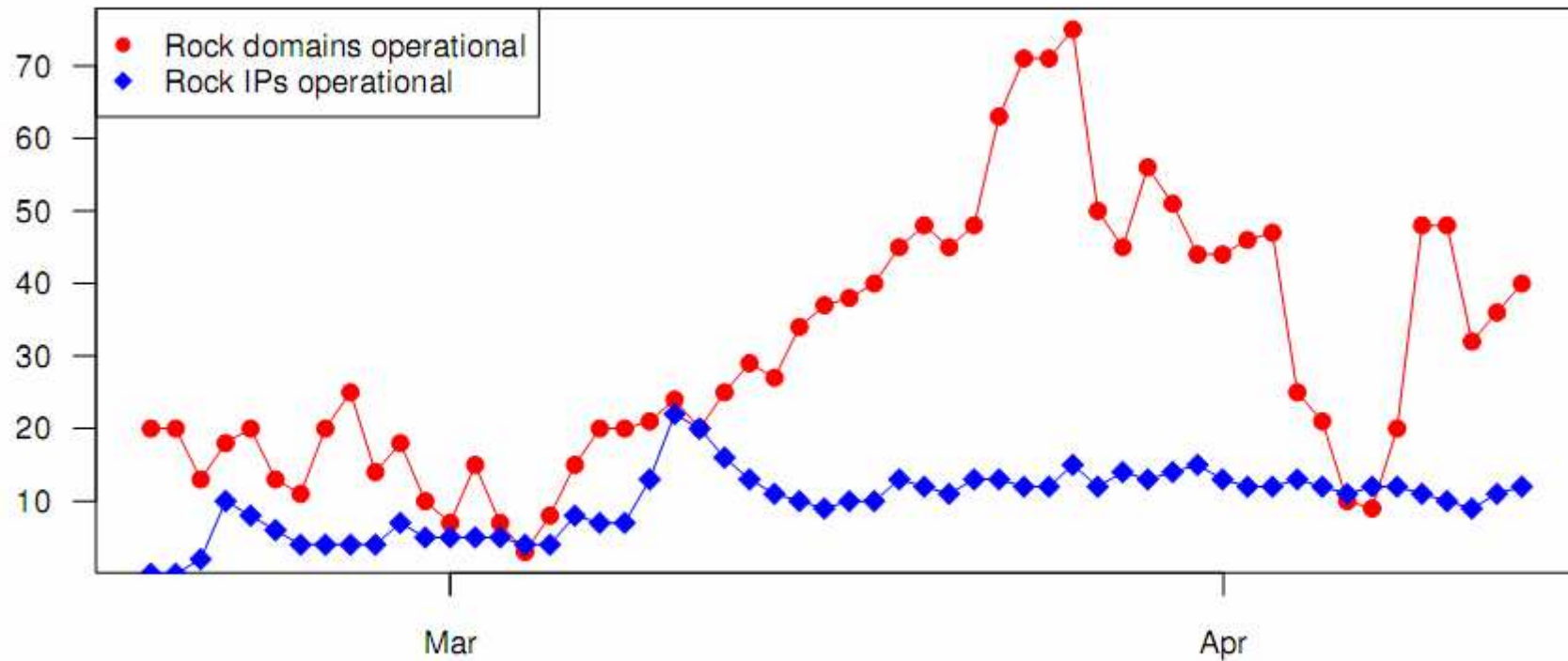
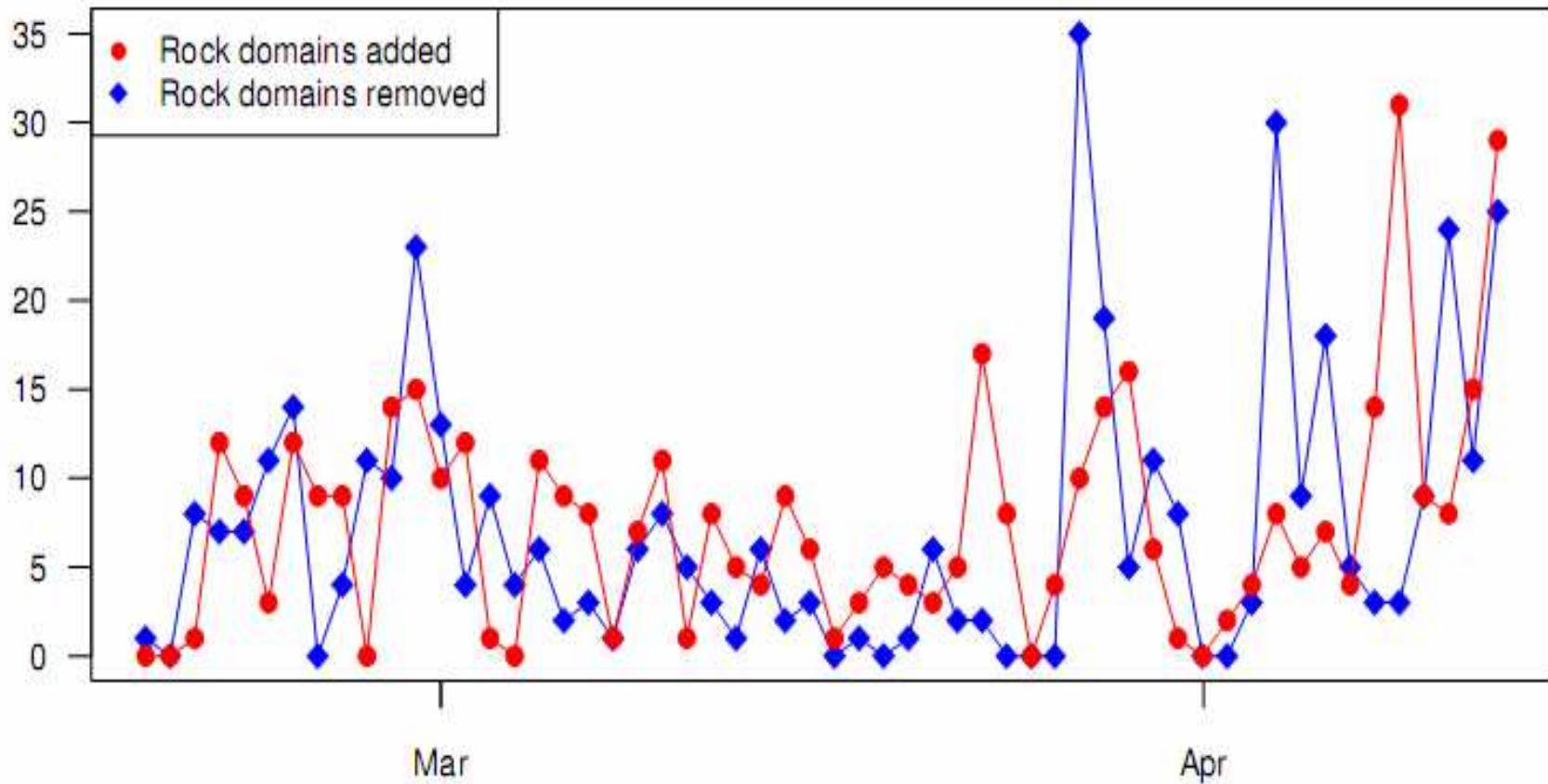


Figure 1: Rock-phish site activity per day.

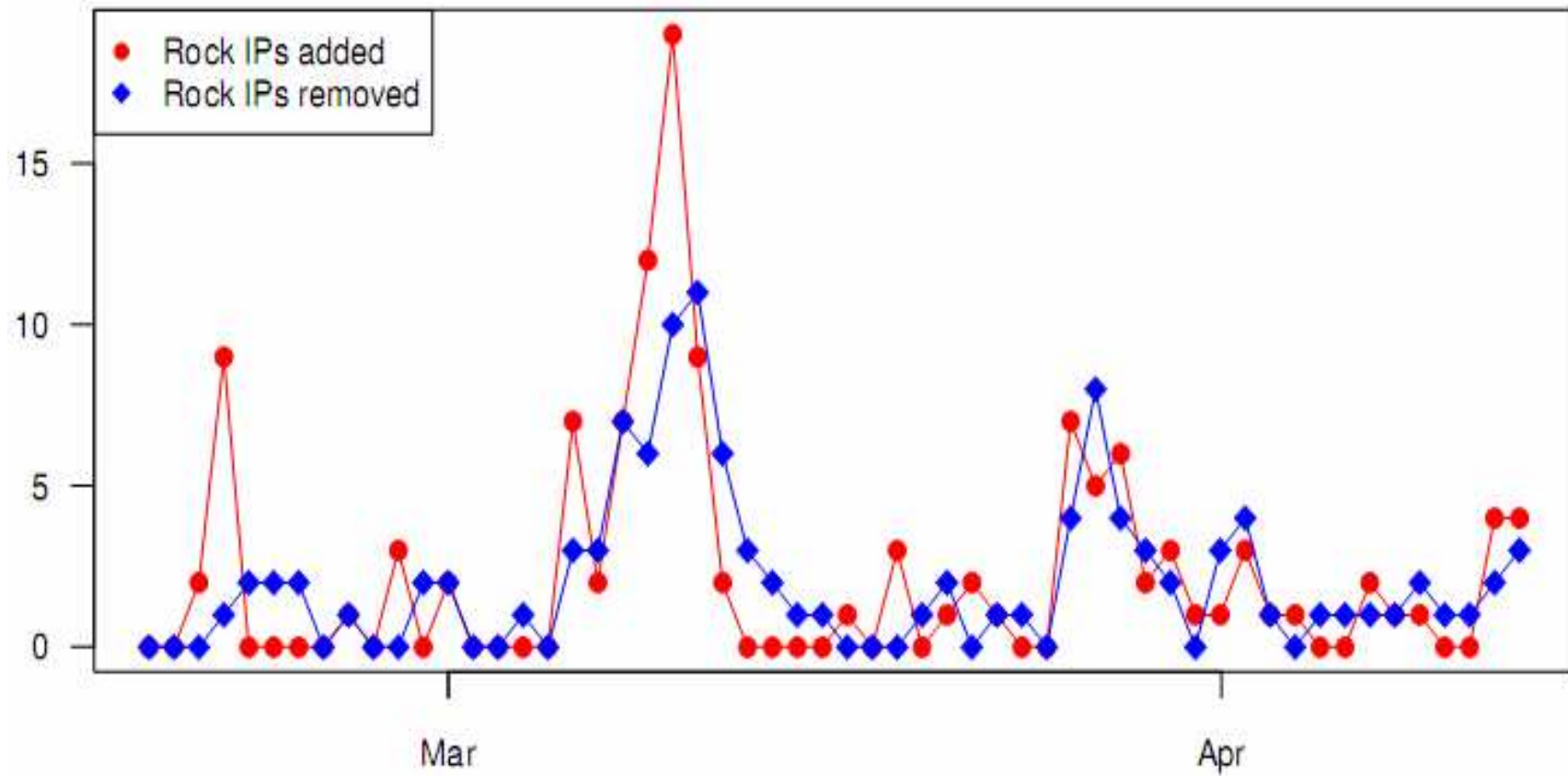
Rock-Phish Statistics

■ Why buy more domains?



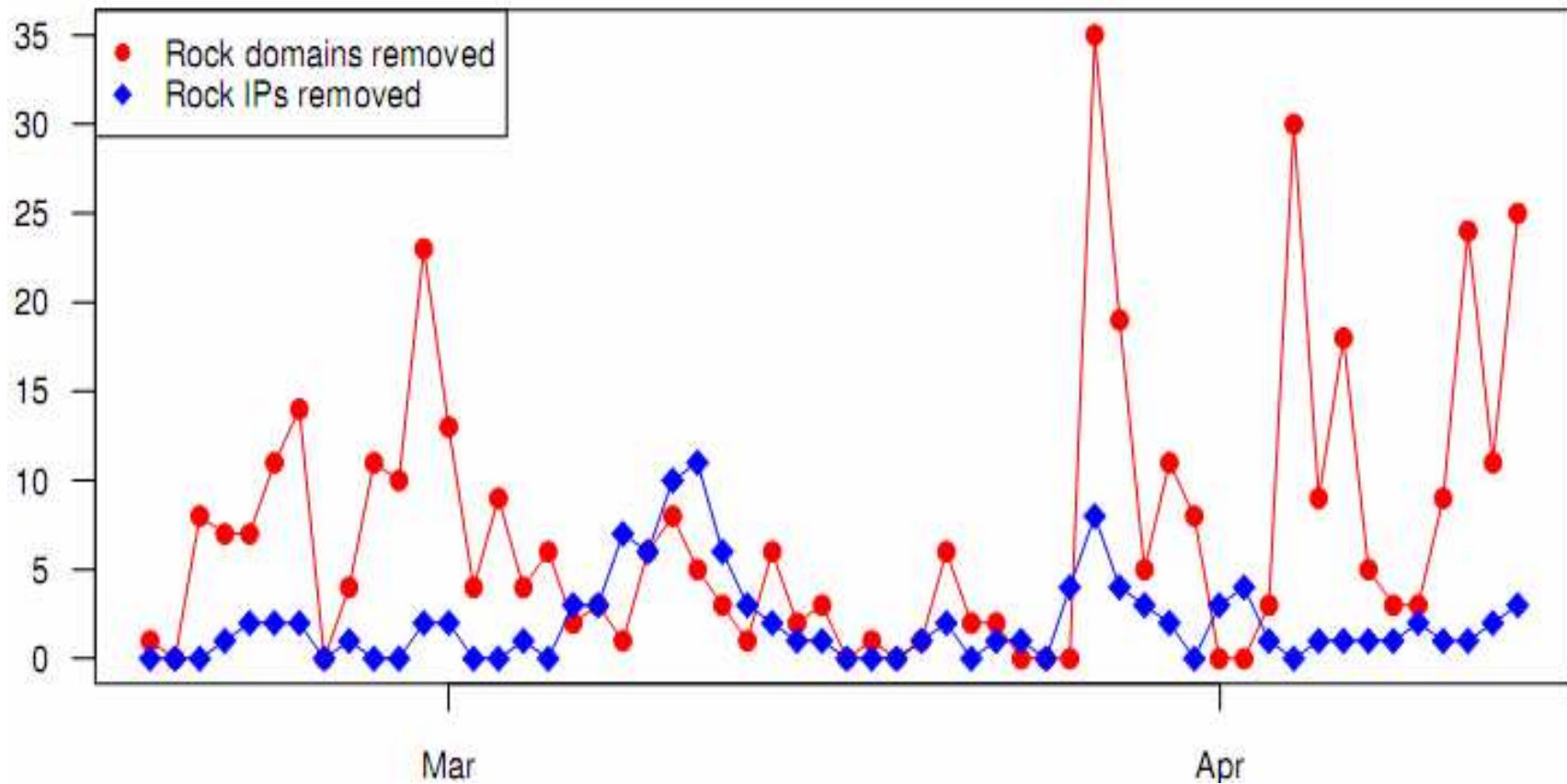
Rock-Phish Statistics

■ Machines behind the Domains

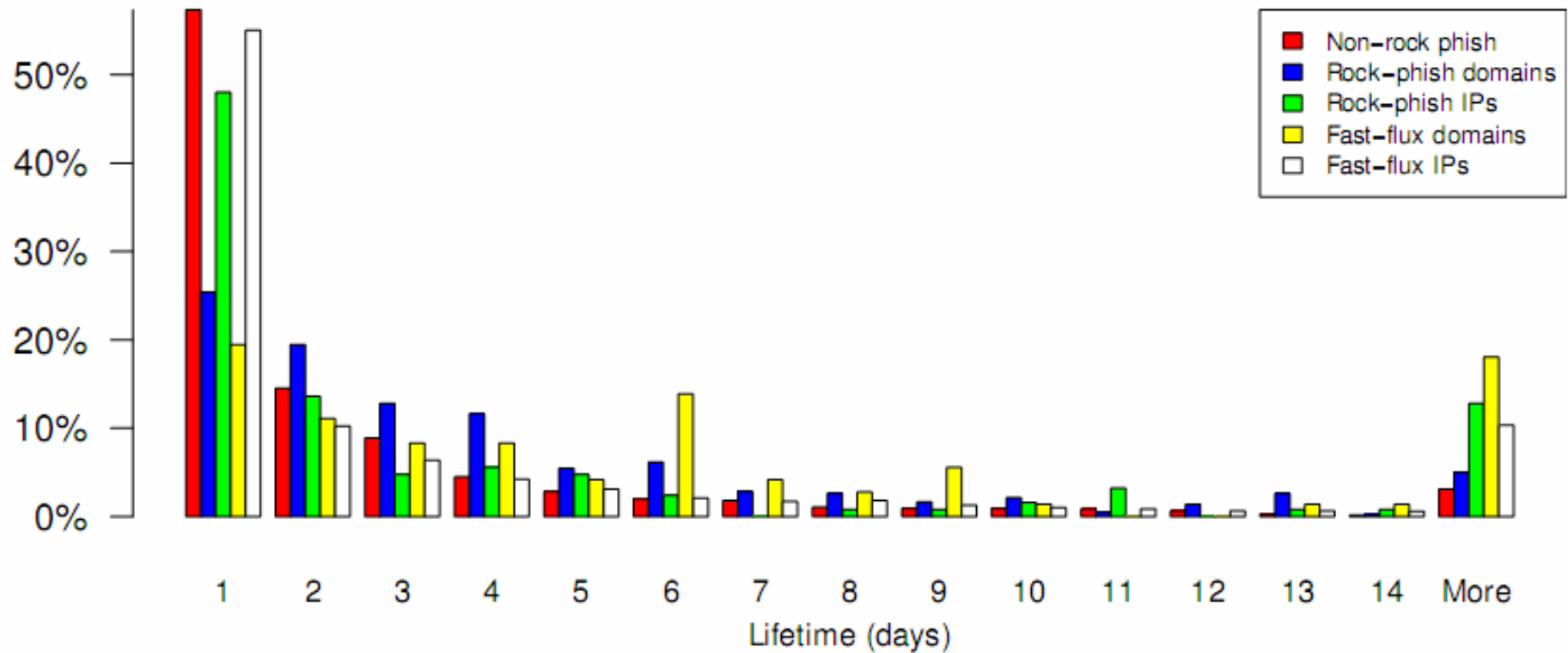


Rock-Phish Statistics

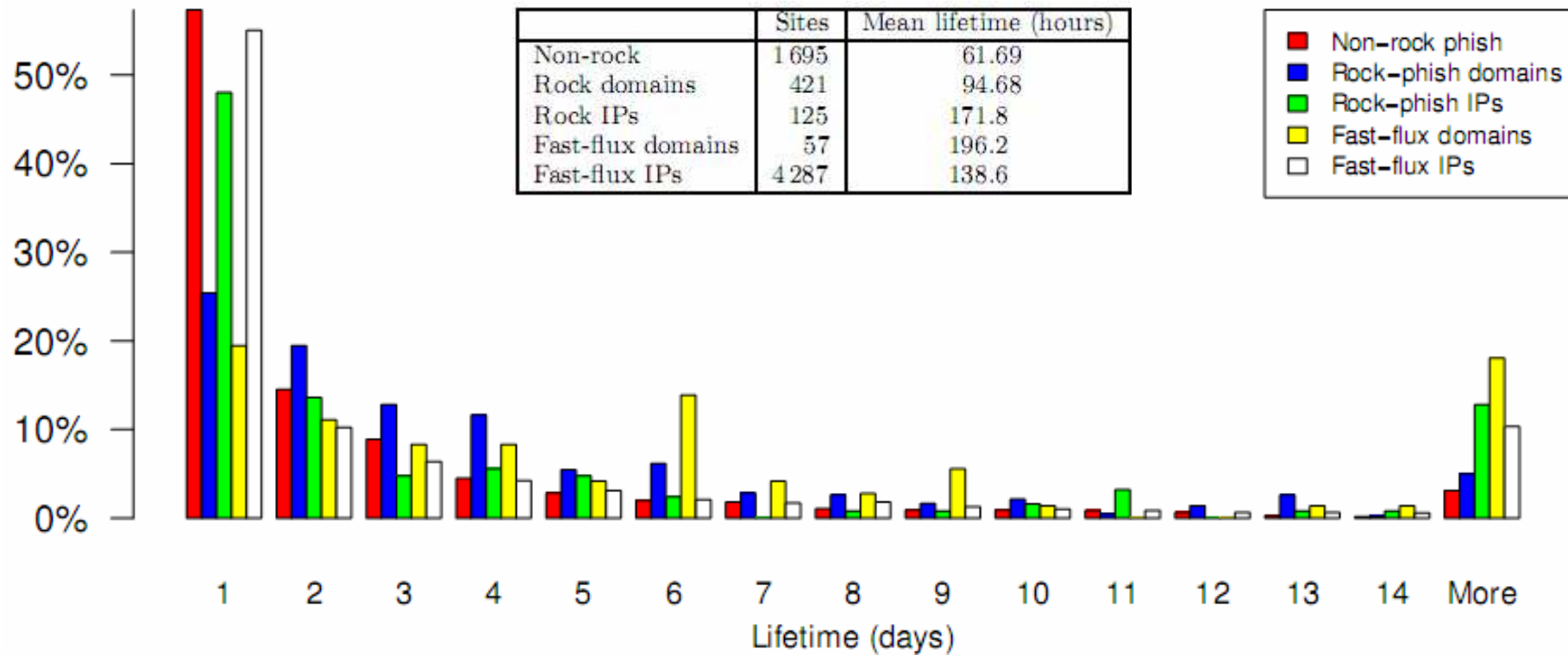
■ Cooperating Domain Registrars and ISPs?



Phishing Site Lifetimes



Phishing Site Lifetimes



User Responses to Phishing

- 50% is real

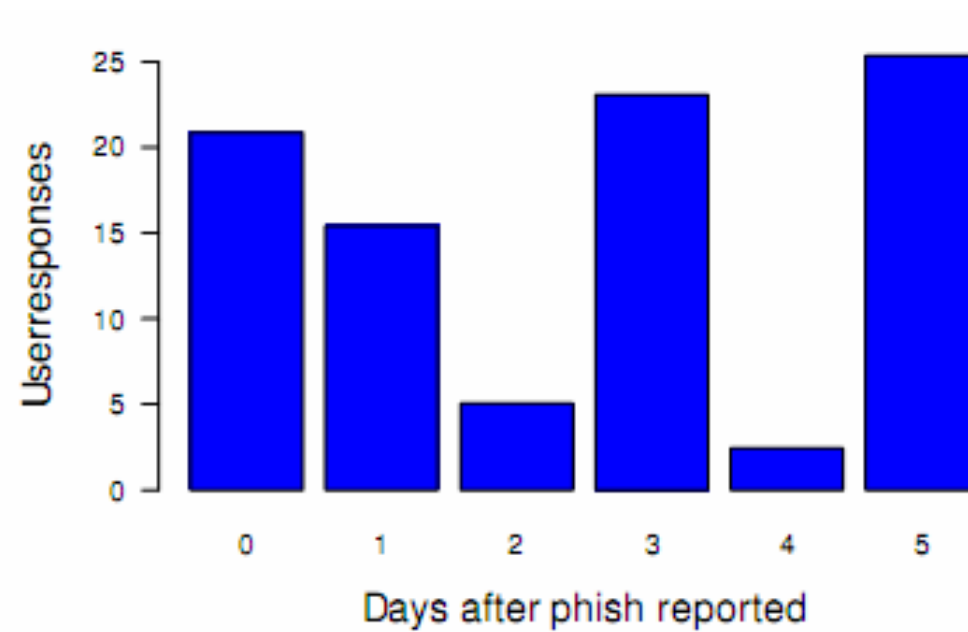
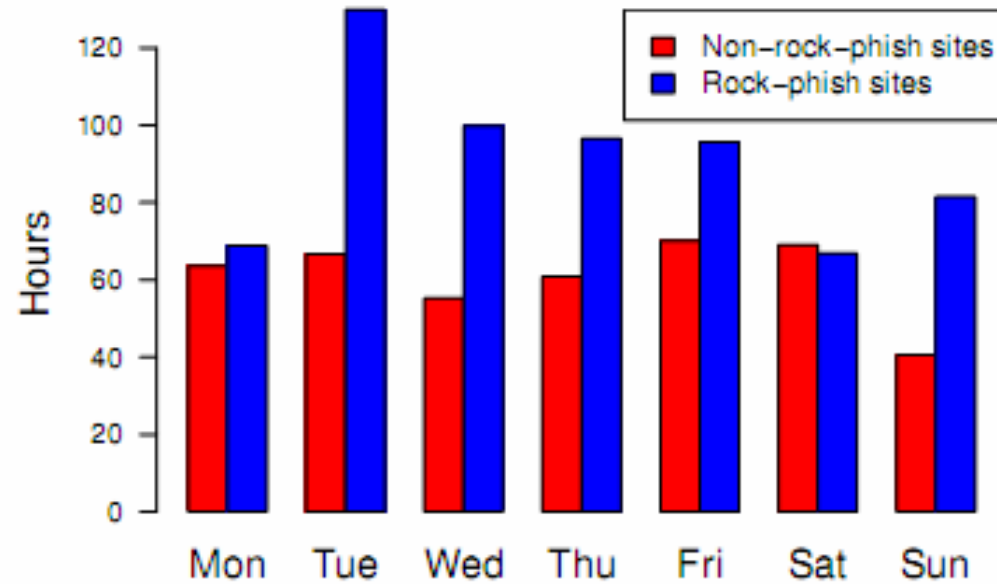
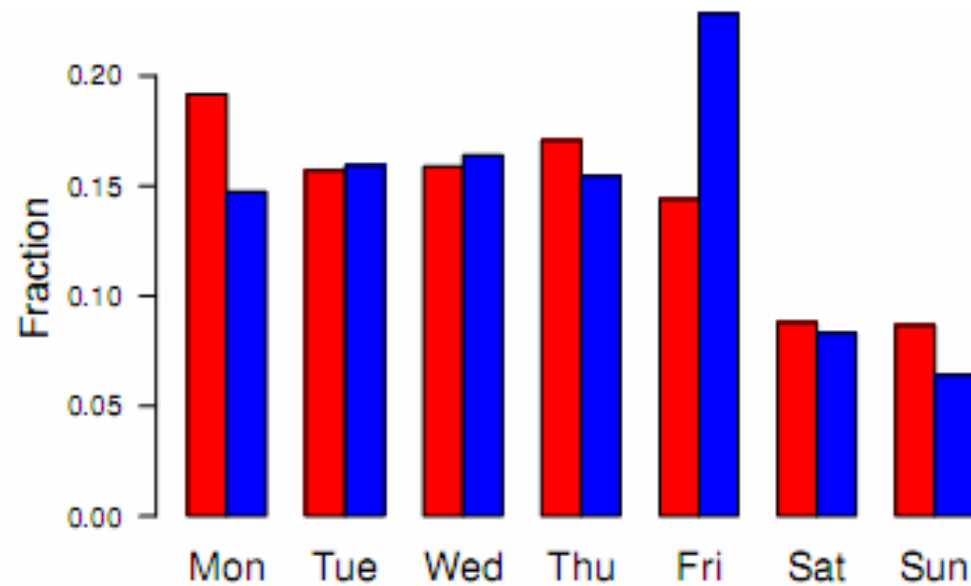


Figure 5: User responses to phishing sites over time.

Do weekend affect take-down?



When are phishing sites launched?



Who is targeted the most?

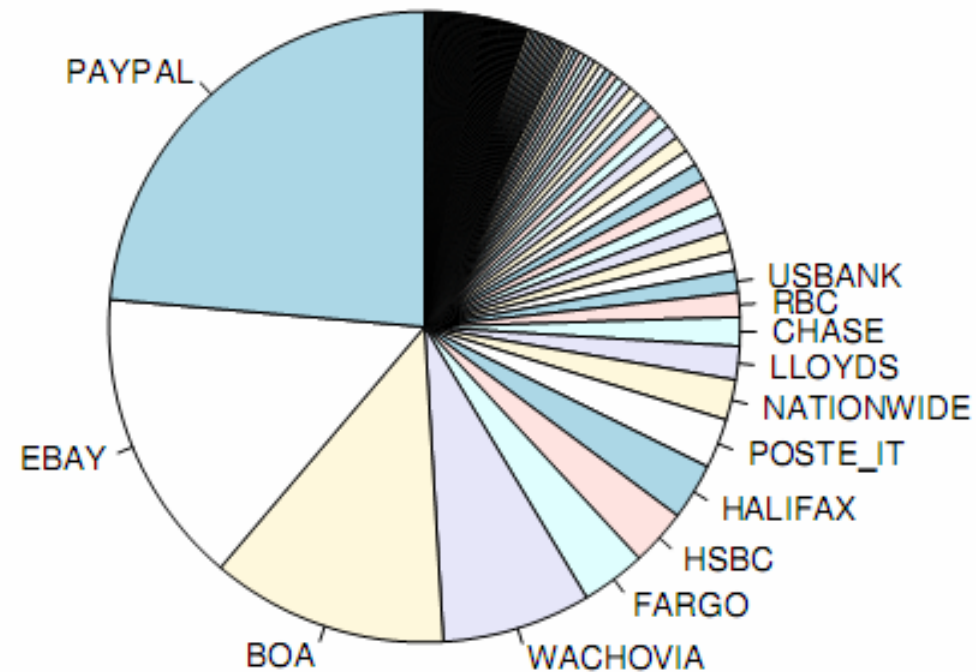


Figure 7: Proportion of ordinary phishing sites impersonating each bank.

Take-Down Response Times

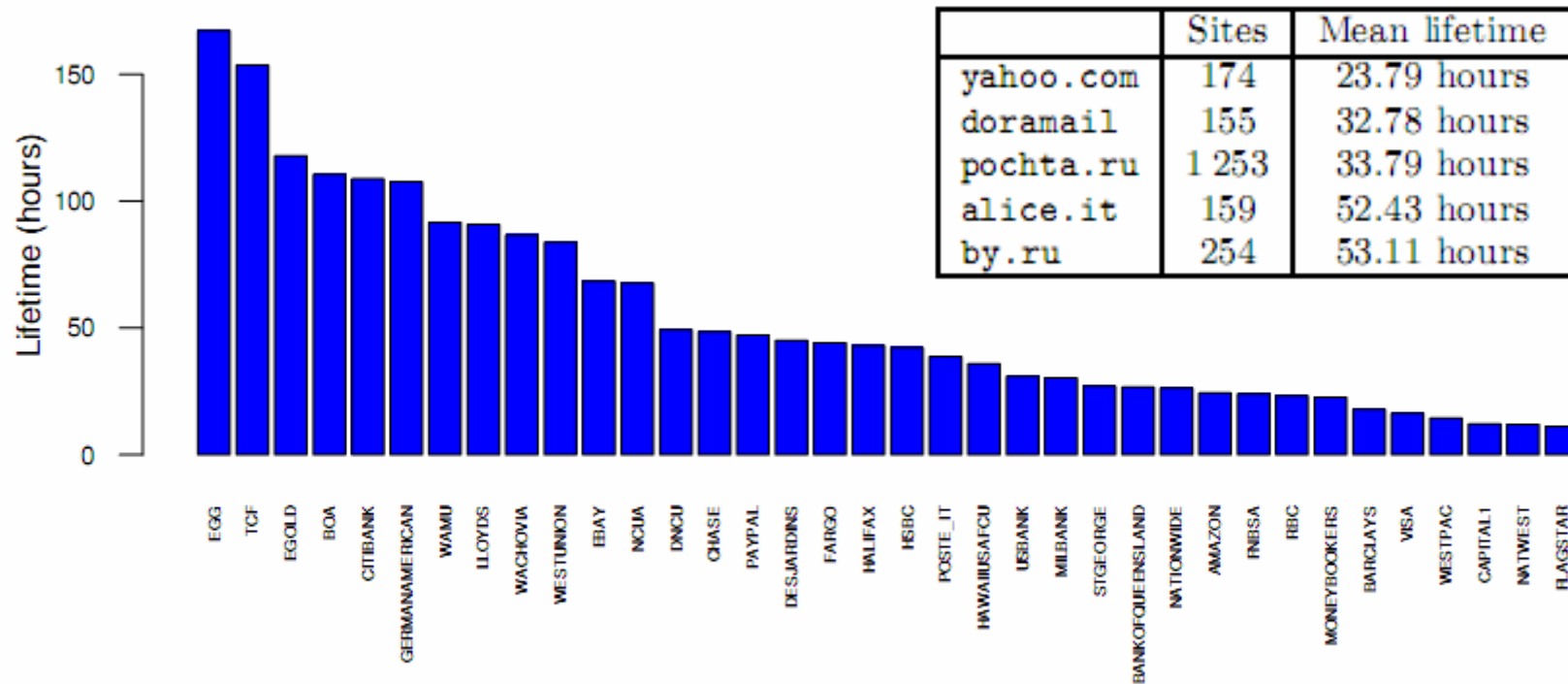


Figure 8: Phishing-site lifetimes per bank (only banks with five or more sites are presented).

Taken-Down Performance over Time

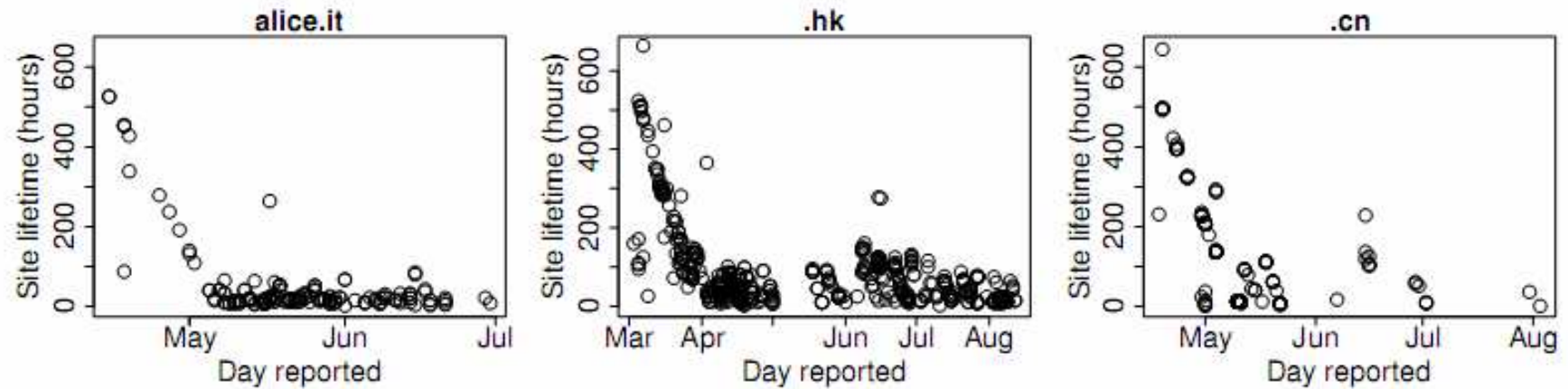


Figure 9: Scatter plot of phishing site lifetimes over time.

Conclusions

- Take-Down Efforts limit Phishing Attacks
- Not Fast enough against first wave Victims
- Sophisticated Methods increase Lifetime

That's it! Questions?

