

Misuse of Domain Privacy Protection Services by Spammers: Act II

ICANN: Dave Piscitello, Steve Sheng
CMU: Ryan Su, Nicolas Christin
Presented at APWG eCrime Researchers
Summit 2010



**General Members Meeting &
eCrime Researchers Summit**
October 18, 19 & 20, 2010 – Dallas, TX

APWG

Domain Name Privacy Conundrum

- Privacy is the ability to control what one reveals about oneself over the Internet and who can access that personal information
- Privacy controls for domain name registrations vary across registries and registrars
- Criminals exploit privacy controls to evade detection



**General Members Meeting &
eCrime Researchers Summit**
October 18, 19 & 20, 2010 – Dallas, TX

APWG

Relevant prior studies

- Prevalence of private registrations among malicious domains hosted at 3FN (Oct 2009)
 - 38% of malicious domains hosted at 3FN used privacy protection services
- Misuse of Domain Name Privacy Protection Services (Act I, Apr 2010)
 - 31% of domains randomly selected from SpamHaus DBL used privacy protection services
- NORC WHOIS data accuracy study (Sep 2010)
 - 18% of domains randomly selected from general population used privacy protection services

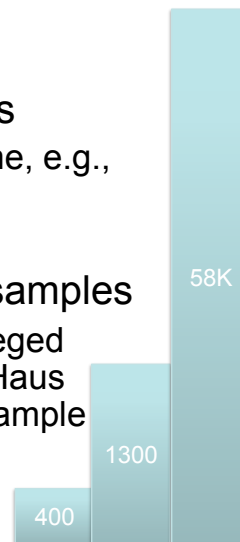


General Members Meeting &
eCrime Researchers Summit
October 18, 19 & 20, 2010 – Dallas, TX

APWG

Current activities

- Iterate prior study of spam domains
 - Look for patterns of behavior over time, e.g., flocking or migratory behaviors
 - See where the data lead us
- Improve automation, study larger samples
 - **ICANN**: collect random sample of alleged spam domains in *gTLDs* from SpamHaus DBL, retrieve Whois records as we sample
 - **CMU**: Develop parsers to overcome variation among WHOIS data stores



General Members Meeting &
eCrime Researchers Summit
October 18, 19 & 20, 2010 – Dallas, TX

APWG

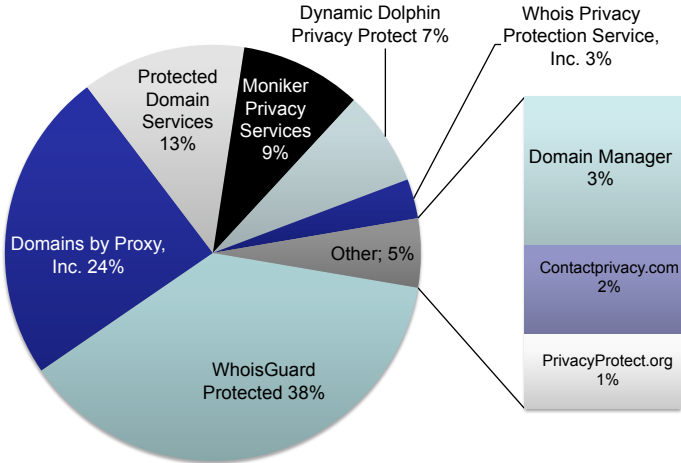
Study Results, Comparisons

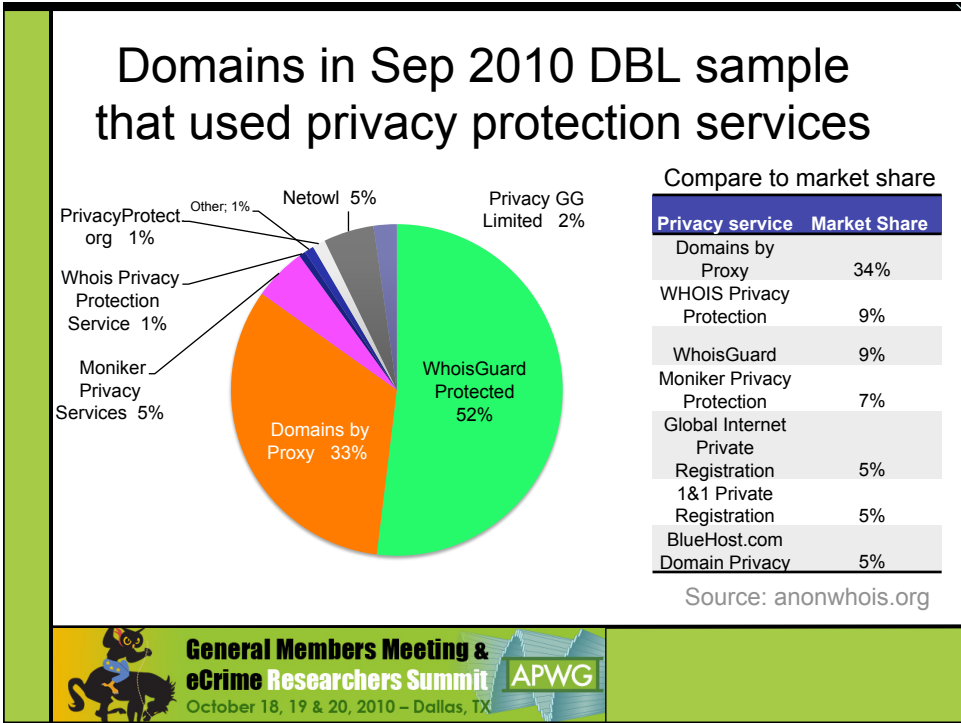
Total general population of domains used in NORC study	1419
Percent of domains NORC identified as using privacy protection service	25%
Total number of alleged SPAM domains in our MAY 2010 sample	1286
Percent of spam domains that used privacy protection services	31%
Total number of alleged SPAM domains in our SEP 2010 sample	57998
Percent of spam domains that used privacy protection services	31%

- In both samples, spam domains have higher percentage of privacy protection services than general population domains
- Percentage did not change significantly from one study of alleged spam samples to next



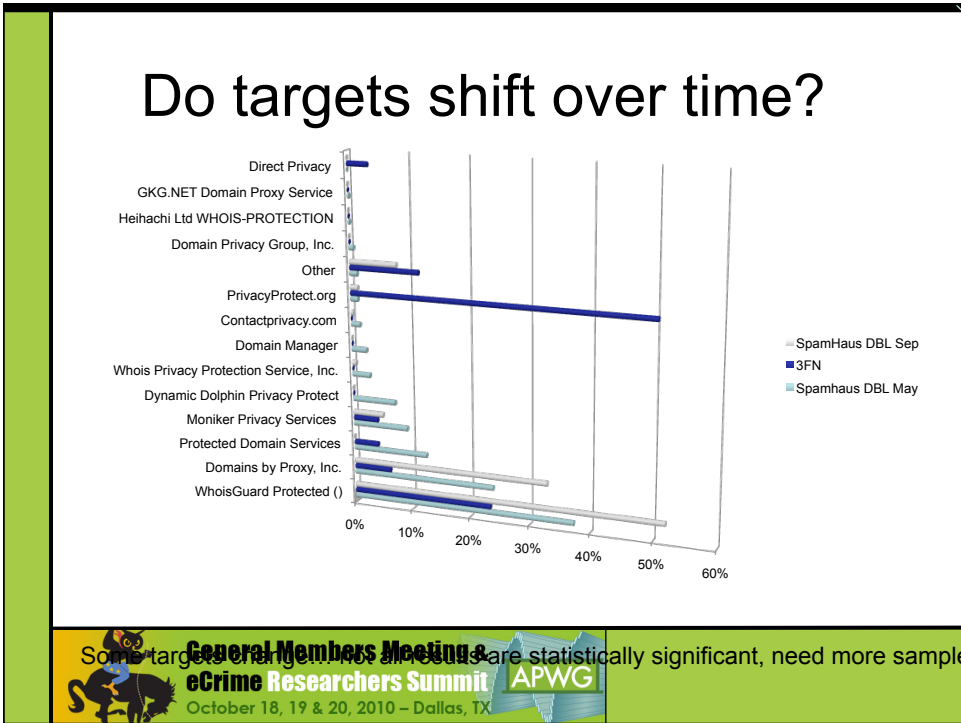
Domains in May 2010 DBL sample that used privacy protection services





General Members Meeting & eCrime Researchers Summit
 October 18, 19 & 20, 2010 – Dallas, TX

APWG



General Members Meeting & eCrime Researchers Summit
 October 18, 19 & 20, 2010 – Dallas, TX

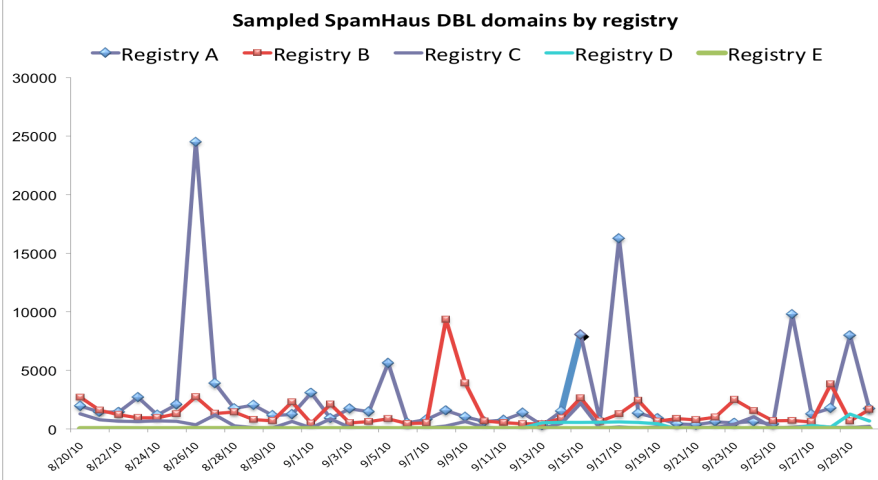
APWG

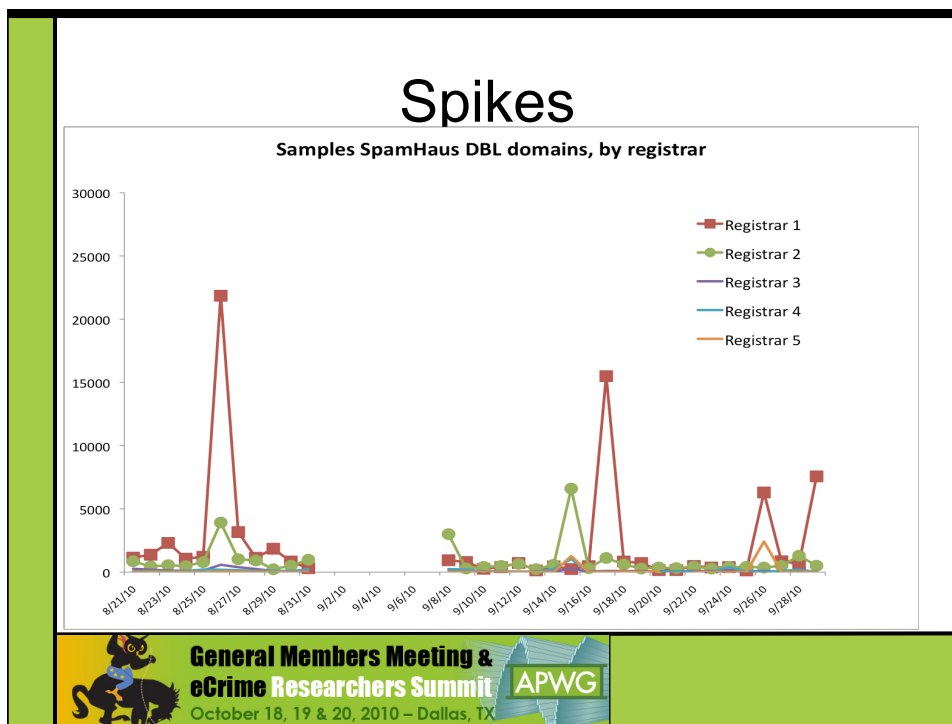
Automation offers new insights

- Our samplings are larger and span longer time periods
- We observe more from these than single {day, week, event} snapshots, i.e.,
 - When spikes in registrations occur
 - Who is targeted and when
 - Intervals between alleged SPAM campaigns
 - Frequency of alleged SPAM campaigns



Spikes





What causes spikes?

- Dates correspond to SpamHaus reporting all domains of a given spammer, or a SPAM campaign
- What made these dates attractive?
 - Will work with registrars and registries to see if there is any correlation to registrar promotions, discounts, bundling
- Worth pursuing?
 - If a correlation is found, can it be used to anticipate or detect early onset of spam attack?

Conclusions, future work

- Studies indicate that a higher percentage of spam domains use privacy protection registration services than the general population
- Continued sampling of DBL may provide additional insights, trends
 - Will increased frequency of samples tell us more?
 - Can we learn more from spikes if we correlate registrar promotions, discounts, or bundling? Do spammers see these as opportunities?
 - Can we apply what we learn to deter spam registrations?



**General Members Meeting &
eCrime Researchers Summit**
October 18, 19 & 20, 2010 – Dallas, TX

APWG

Thank you

- Contact information
 - Dave Piscitello
dave.piscitello@icann.org
 - Steve Sheng
steve.sheng@icann.org
 - Nicolas Christin
nicolasc@andrew.cmu.edu
 - Ryan Su
 - yulos@andrew.cmu.edu



**General Members Meeting &
eCrime Researchers Summit**
October 18, 19 & 20, 2010 – Dallas, TX

APWG

Related studies

- Private Domain Registrations at 3FN (APWG ceCOS, Oct 2009)
<http://securityskeptic.typepad.com/the-security-skeptic/2009/10/private-domain-registrations-at-3fn.html>
- Domain Name Privacy Misuse Studies (APWG ceCos, Apr 2010)
<http://securityskeptic.typepad.com/the-security-skeptic/2010/04/domain-name-privacy-misuse-studies.html>
- Privacy Proxy Registration Services Study Report (NORC, Sep 2010)
<http://www.icann.org/en/compliance/reports/privacy-proxy-registration-services-study-14sep10-en.pdf>



**General Members Meeting &
eCrime Researchers Summit**
October 18, 19 & 20, 2010 – Dallas, TX

