Private Domain Registrations: examining the relationship between private domain registrations and malicious domains at 3FN

Dave Piscitello
ICANN Sr. Security Technologist
(All views expressed are my own)

Background

3FN shut down by FTC

FireEye studies 3FN content

Why use 3FN as the basis for a case study?

FTC shuts down 3FN

- 4 June 2009: District court judge orders shut down of 3FN Service at the request of the FTC
- FTC alleges that 3FN
  - "actively recruits and colludes with criminals seeking to distribute illegal, malicious, and harmful electronic content including child pornography, spyware, viruses, …
  - advertised its services "in a forum established to facilitate communication between criminals."
  - actively shielded criminal clientele by ignoring take-down requests issued by security community, or shifting its criminal elements to other IP addresses it controlled to evade detection. *http://www.ftc.gov/opa/2009/06/3fn.shtm*

FireEye studies 3FN content

- FireEye Malware Intelligence Labs
  - approached by law enforcement (not FTC) looking for evidence of malicious activities at 3FN
  - analyzes content hosted at addresses from IP blocks allocated to 3FN
  - Publishes results in the *Bad Actors* series at *http://blog.fireeye.com/research/*

Why 3FN as basis for a case study?

- 3FN is an alleged locus of malicious domain activity
  - Over 400 domains from multiple GTLDs and registrars
  - Multiple private domain registration services
  - Black- and block-lists have data associated with many 3FN domains
- Concentration of alleged miscreant activity creates opportunity to study private domain registrations to answer a specific question:
  - How prevalent are private domain registrations among domains hosted at 3FN?

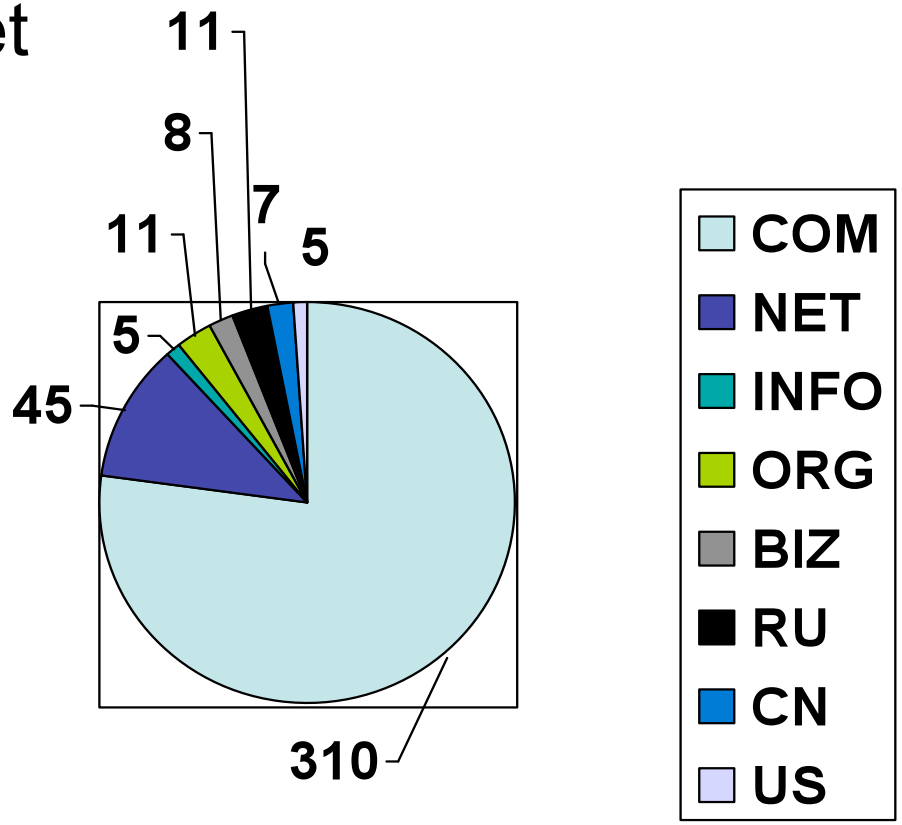
How prevalent are private domain registrations among domains hosted at 3FN?

3FN Sample: domains, TLDs

Private domain registrations

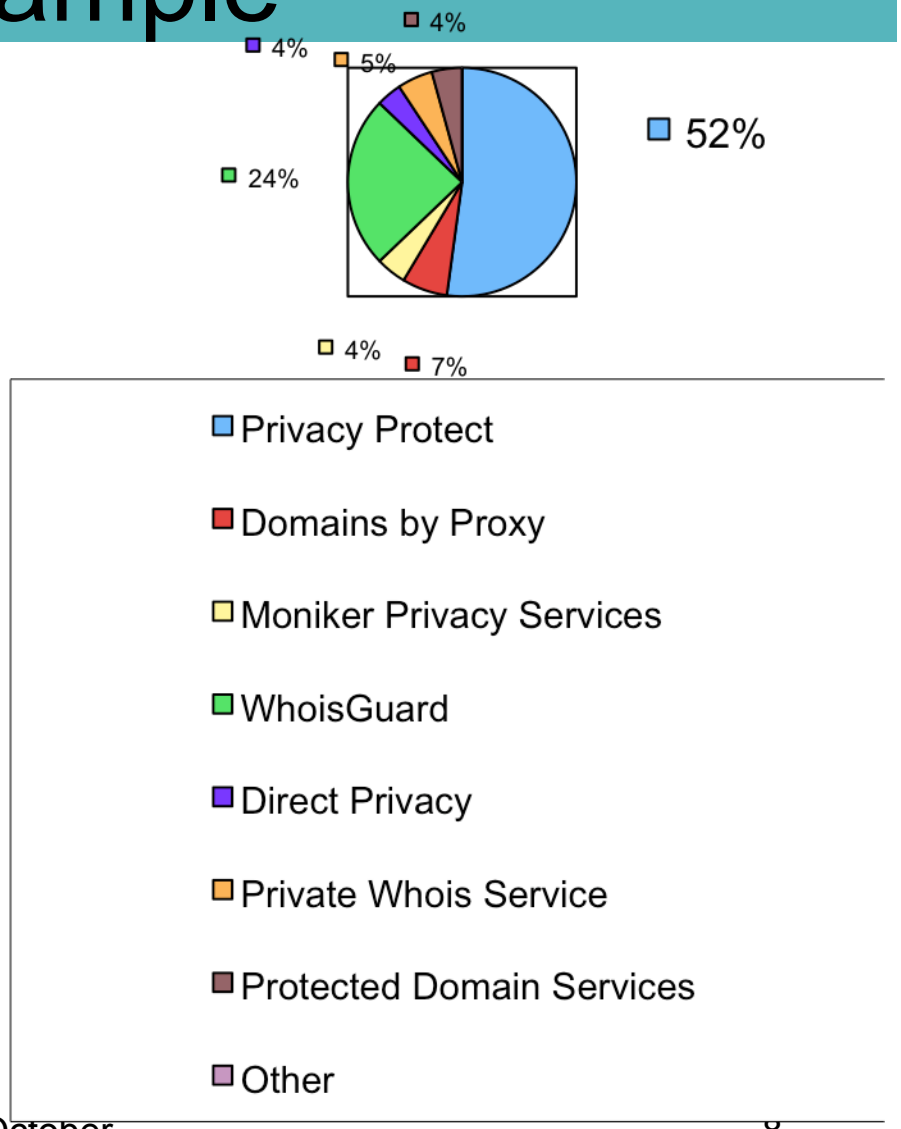
3FN sample: domains, TLDs

- 403 domains in data set
  - Included two CCTLDs
- Used 384 in study from
  - BIZ,
  - COM,
  - INFO,
  - NET,
  - ORG,
  - US



Private domain registrations in 3FN sample

- 3FN sample
  - 145 of 384 domains used in study were private domain registrations (38%)
- Other studies (NORC)
  - 580 of 2352 domains used in the study were private or
  - domain registrations (25%)



How many "3FN" domains with private domain registrations allegedly host criminal or malicious content?

Methodology

Reporting tools, block-and black-lists

Results, Findings, Possible remedies

Methodology

- Query block- and black-lists for reports against
  - Domain name
  - IP address while hosted at 3FN
  - New IP address (if domain remains hosted)
- Spam/malware feed data (courtesy of FireEye)
- Count domains with 1+ reports of malicious activity
- Malicious activities reported among lists include:
  - Spam hosting
  - Phishing
  - Child pornography✪
  - Malware hosting
  - Search or click fraud
  - Illegal pharma
  - Digital rights infringements (illegal MP3 downloads)
  - Hosting DNS for any of above activities

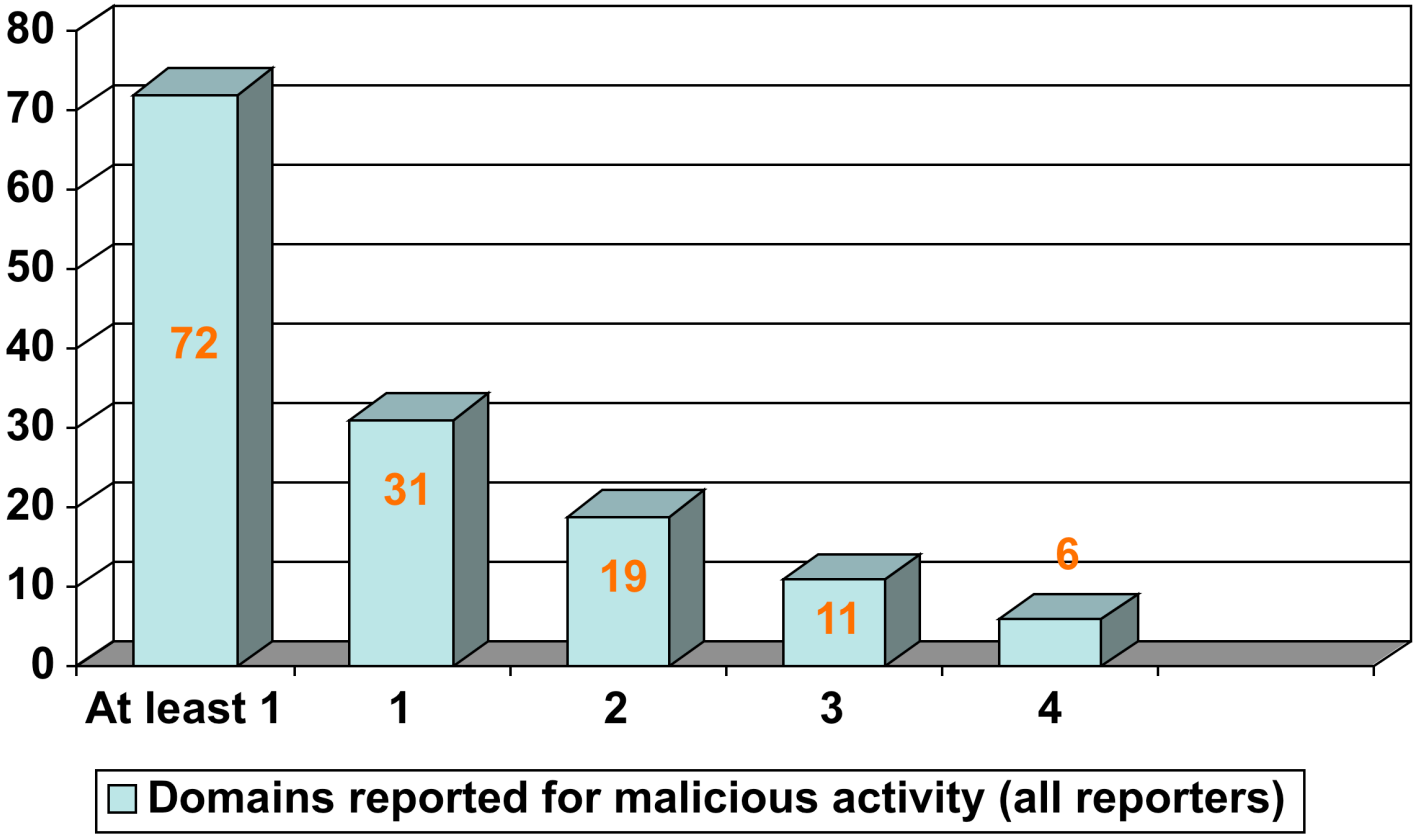
Reporting tools used

- SpamAssassin's Rules Emporium (SURBL+ checker)
  www.rulesemporium.com/
- RobTex Swiss Army Knife (RBL and DNS checks)
  www.robtex.com/
- Malware Domain List
  www.malwaredomainlist.com/
- Borderware (WatchGuard) Reputation Authority
  www.reputationauthority.org
- McAfee SiteAdvisor
  www.siteadvisor.com/
- Google Safe Browsing for Malware
  www.google.com/safebrowsing/diagnostic?site=<domain>

Block- and black-lists consulted

- sbl-xbl.spamhaus.org
- spam.dnsbl.sorbs.net
- Project Honeypot
- b.barracudacentral.org
- dnsbl-2.uceprotect.net
- dnsbl-3.uceprotect.net
- no-more-funn.moensted.dk
- dnsbl.sorbs.net
- ips.backscatterer.org
- web.dnsbl.sorbs.net
- spam.dnsbl.sorbs.net
- sbl.spamhaus.org
- ivmSIP24

How many "3FN" domains with private domain registrations are reported as hosting criminal or malicious content?



How many "3FN" domains with private domain registrations host commercial content?

- For this study, commercial content is defined as a having one or more properties
  - Access to site content is "for fee"
  - Products are sold at the site or promoted using email hosted from the domain or using URLs that direct visitors to the site
  - Site is supported through PPC, link, search, or other advertising
- Methodology for determining if content is commercial
  - Use search, search optimization, analytics and info sites
    - About US, Alexa, Domain Tools, SEO Browser, Wayback Machine
  - Visits to web sites, web site archives, or thumbnail views
    - In some cases, visits performed by FireEye
- All 3FN domains determined to be commercial sites using this methodology

Findings

- By applying data from multiple public resources one can determine with reasonable certainty whether a domain
  - Is registered using a private domain registration service
  - Is used for commercial purposes
  - Appears on public lists of “domains used to host or support malicious activity”
- The results used for this study are reproducible
- The methodology could be automated for larger samples
  - A larger, more general sample may show results are atypically high

Findings

- Private domain registrations are used by registrants of domains who host commercial content
  - All 3FN sites determined to be commercial sites
  - Finding debunks myths regarding who uses private domain registrations
- Many private domain registration services are used
  - Sampling too small to make further conclusions
- Private domain registrations are used by registrants of domains that appear on public lists of "domains used to host or support malicious activity"
  - 49% of domains with private registrations hosted at 3FN were reported for 1+ *malicious* activity
  - 50% of domains with private registrations are commercial sites with no reports of malicious activity

Possible ways forward

- Guidelines for private domain registrations?
  - Exempt commercial use from private domain registration?
  - Should private registrations only protect privacy of individuals or parties operating legitimately with need for anonymity? (e.g., “rights advocacy” group)?
    - Are Telco “Caller ID” policies helpful here? (Provider can refuse if applicant cannot provide valid reason)
- Requirements for private registration?
  - Proof that party seeking protection satisfies guidelines for private registration?
  - Include suspension in Terms of Service for cases where abuse or misrepresentation is reported and confirmed?

Next steps

- Study a statistically meaningful sample
  - Should (can) we assure a similar concentration of bad actors in the sample?
    - Other loci of alleged malicious activity not hard to find
  - What affect would a randomized sampling of domains have on findings?
    - Percentage of bad actors may change dramatically
    - Percentage of commercial actors may not change
- Present findings to ICANN community

Questions?

Dave.Piscitello@icann.org