SSAC since last RIPE 55

ICANN SSAC

What is SSAC?

- The Security and Stability Advisory Committee advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.
  - operational matters
  - administrative matters
  - registration matters
- http://www.icann.org/committees/security/

SSAC Members

Stephen Crocker <steve@stevecrocker.com> – Chair

Dave Piscitello <dave.piscitello@icann.org> – ICANN Senior Security Technologist

Jim Galvin <galvin+dnssac@elistx.com> – eList eXpress

Alain Aina (Consultant)
Jaap Akkerhuis (NLnet Labs)
Jeffrey Bedser (Internet Crimes Group)
Lyman Chapin (Interisle), RSTEP Liaison
KC Claffy (CAIDA)
Steve Conte (ICANN)
Patrik Faltstrom (Cisco Systems)
Robert Guerra (Privaterra), ALAC Liaison
Rodney Joffe (Neustar)
Olaf Kolkman (NLNet Labs), IAB Point of Contact
Mark Kosters (ARIN)
Warren Kumari (Google)
Matt Larson (VeriSign)
Danny McPherson (Arbor Networks, Inc.)
Ram Mohan (Afilias)
Russ Mundy (SPARTA, Inc.)
Frederico Neves (NIC.br)
Ray Plzak (ARIN), Vice-Chair
Ramaraj Rajashekhar (Sequoia Capital, India)
Barbara Roseman (ICANN), IANA Liaison
Mike St. Johns
Shinta Sato (JPRS)
Mark Seiden (Yahoo!)
Doron Shikmoni (ForeScout, ISOC-IL)
Bruce Tonkin (Melbourne IT)
Stefano Trumpy (IIT/CNR), GAC Liaison
Paul Vixie (ISC)
Rick Wesson (Support Intelligence)
Suzanne Woolf (ISC)

A few reports have been released

- [SAC022]:Domain Name Front Running
- [SAC023]:Is the WHOIS Service a Source for email Addresses for Spammers?
- **[SAC024]:Report on Domain Name Front Running**
- **[SAC025]:Fast Flux Hosting and DNS**
- **[SAC026]:SSAC Statement to ICANN and Community on Deployment of DNSSEC**
- [SAC027]:SSAC Comment to GNSO regarding WHOIS studies
- [SAC029]:SSAC Endorsement of Proposed Amendment to the ORG registry agreement, Security Extensions for the DNS – DNSSEC [**RSTEP: phoffman@proper.com**]
  - http://www.icann.org/announcements/announcement-23apr08.htm

SAC024

Report on Domain Name Front Running

Background

- SSAC issued Domain Name Front Running Advisory (October 2007)
- Advisory offers preliminary findings:
  - Some Internet users claim that parties associated with the domain name registration process participate in domain name front running (DNFR)
  - No Internet user had presented sufficient information to support or disprove such claims
- Advisory called for community input

Disposition of Claims

- SSAC members reviewed each claim using information provided by claimant
  - Registration records, domain history, current status of domain, DNS checks, and current use of domain name used to create chronology of registration related events
- Majority of claimants were contacted by email for additional information
- Majority of claimants were informed of SSAC's interpretation of the chronology of events leading to the claim that front running occurred

Analysis and Classification of 120 Claims

No “smoking gun”

SSAC identified alternate, plausible explanations for all of the claims

Noteworthy statistics

- Of the 120 domains studied…
  - 38% are “live” and host advertising
  - 27% are registered using private/proxy services
  - 15% were available at time SSAC studied the domain
    - SSAC found that many of these were tasted and returned to the available pool
  - 14% were available for purchase in after market
    - Many of these domains host advertising
  - One domain is locked (redemption grace period)
  - 6% relate to a back-order process
  - 2% appear to be candidates for UDRP

Observations (from the Report)

- 74% of front running claims can be attributed to domain tasting and secondary market activities
  - *The community does not understand the complexities of the domain registration process and the domain name marketplace*
- Domain names believed to be of limited or exclusive interest are not as unique as claimants imagine.
  - *Competition for domain names containing commonly used or popular words, phrases and even surnames is intense*
- Measurable interest in typo-squat and visually deceptive names (often to host PPC)
- Tasting of non-renewed domains is a problem for many Internet users
  - Interest in tasting deleted names intensifies this problem

Conclusions

- SSAC can neither confirm, nor deny, any incident of DNFR **based on community responses**
- **SSAC is continuing too look at DNFR**
- Many internet users do not approve of domain name kiting, front running, hijacking, and tasting and conclude that the registration process is not trustworthy
  - SSAC observes a deteriorating trust relationship between registrants and registrars
- Any agent who collects information about an Internet user's interest in a domain name and who discloses it in a public way violates a trust relationship
  - This violation is exacerbated when agents put themselves or third parties in an advantageous market position with respect to acquiring that domain name at the expense of its client

Recommendations

- All parties should help educate registrants about the global market for domain names, the existence of after markets and how these affect registrants
  - Eliminate the use of industry jargon wherever possible
- Registrars should
  - Clearly state how they treat information Internet users submit when checking the availability of a domain name
  - Seek to eliminate the apparent confusion over the nature and benefits of back ordering domain names
- Registrants should appreciate that
  - Domain names are a speculated and sought-after commodity
  - Availability checks may disclose an interest in a name
  - Preparing in advance and registering a name at the time they perform an availability check is the surest course of action

SAC025

Fast Flux Hosting and DNS

What is Fast Flux Hosting?

- An evasion technique
- Goal
  - Avoid detection and take down of web sites used for illegal purposes
- Technique
  - Host illegal content at many sites
  - Rapidly change pointers (IP addresses) so that no one site is used long enough to isolate and shut down

Variations on a theme…

- Basic fast flux hosting
  - IP addresses of illegal web sites are fluxed
- Name Server (NS) fluxing
  - IP addresses of DNS name servers are fluxed
- Double flux
  - IP addresses of web sites *and* name servers are fluxed

Anatomy of an attack

bot herder infects hosts, gathers herd into botnet

1

2

bot herder "leases" botnet to "customer"

3

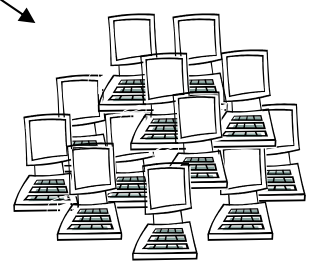
Customer "acquires" phishing kit from malware author

4

Via a registrar, customer registers `nameserverservicenetwork.tld` and `boguswebsitesexample.tld`

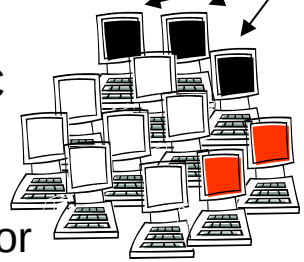
5

Via a registrar, customer fluxes NS records for `nameserverservicenetwork.tld` to TLD zone file with $TTL 180



6

Customer uses C&C to load zone file onto selected bots; flux host A records for `boguswebsitesexample.tld` have $TTL 180



7

Customer uses botnet C&C channel to load bogus web site onto hosts identified in the zone file for `boguswebsitesexample.tld`

8

Customer spams phishing email to lure victims to bogus web site

STEPS 5-7 repeat as TTLs expire…

Mitigation

- Authenticate contacts
- Prevent automated (scripted) changes
- Set a minimum allowed TTL
- Implement or expand abuse monitoring
- Enforce a Universal Terms of Service agreement
- Quarantine (and honeypot) domain names
- Rate-limit changes to a domain name
- Separate "short TTL updates" from normal registration change
- Use suspended domains to educate consumers

Findings

- Fast flux hosting exploits domain name resolution and registration services to abet illegal activities
- Current methods to thwart fast flux hosting by detecting and dismantling botnets *are not effective*
- Fast flux hosting hampers current methods to detect and shut down illegal web sites
- Frequent modifications to NS records and short TTLs in NS A records in TLD zone files can be monitored to *identify possible abuse*
- Blocking automated changes to DNS info and enforcing a minimum TTL > 30 minutes are effective countermeasures *but are not uniformly practiced*

Recommendation

- SSAC encourages ICANN, registries and registrars to
  - consider the practices mentioned in this Advisory,
  - establish best practices to mitigate fast flux hosting
  - consider incorporating such practices in future accreditation agreements.

SAC026

SSAC Statement to ICANN and Community on Deployment of DNSSEC

SAC026 – Statement on DNSSEC

- SSAC has been looking at the various deployment projects that exists for DNSSEC.
- SSAC recognizes that any technology deployment on global scale will reveal issues that could not be found even during tests.
- SSAC came with 4 recommendations.
- SSAC will also continue a review of readiness of DNSSEC, specifically in a few named areas.

SAC026 – Recommendations

1. As manager of the IANA function, ICANN should continue its efforts to support and facilitate deployment of DNSSEC.
2. GTLD registries should study business, technical and financial issues regarding DNSSEC deployment with ICANN.
3. ccTLD registries should also study business, technical and financial issues regarding DNSSEC deployment with ICANN.
4. Registrars should study business and technical issues related to (a) accepting keys on behalf of registrants with ICANN and registries, and (b) providing DNSSEC service for customers who use registrar's name services.

SAC026 – Review areas

- Protocol completeness.
- The key rollover process.
- Proposals for trust anchor repositories.
- Implementation and deployment testing.
- Performance and error analysis.
- End User Application development.
- Availability of DNSSEC on commonly used DNS server platforms.

SAC026 - Future

- SSAC is working on the continuation of SAC026
- More information will be available closer to summer (on northern hemisphere) 2008