ccNSO Members Meeting

Support your local Sheriff

Rodney Joffe
SVP and Senior Technologist, NeuStar

Jun 23rd, 2009

ICANN sydney No.35 21 - 26 JUNE 2009

NEUSTAR™

Introduction

=== Action : C I HAVE
SHELLS,ROOTS,PSYBNC,BNC,DDOS BOTS, IRC
FLOODERS,100 IRC SCRIPTS (FULL PROTECTION
AND ENTERTAINMENT), HACKING
STUFFS, BULLETPROOF .ZZZ DOMAINS AND MUCH
MORE MSG ME FOR TRADE I VERIFY 1ST
AND DONT MSG ME FOR SAMPLES.

D: HOW BULETPROOF?

C: REGISTRY IGNORES COMPLAINS

NEUSTAR™

WHY DID NEUSTAR GET INVOLVED IN 2006?

- Feedback / avoid “dangerous domain” blacklist
  - We did not want to be .zzz
- Internal desire to stop abuse of NeuStar infrastructure.
  - We did not want to give malicious parties the ability to organize their attacks
- Technical and legal expertise was available
  - Legal expertise required to formulate contractual obligations and discover and mitigate liability issues
  - Technical expertise required to perform verification and validation of complaints and proactively investigate domains

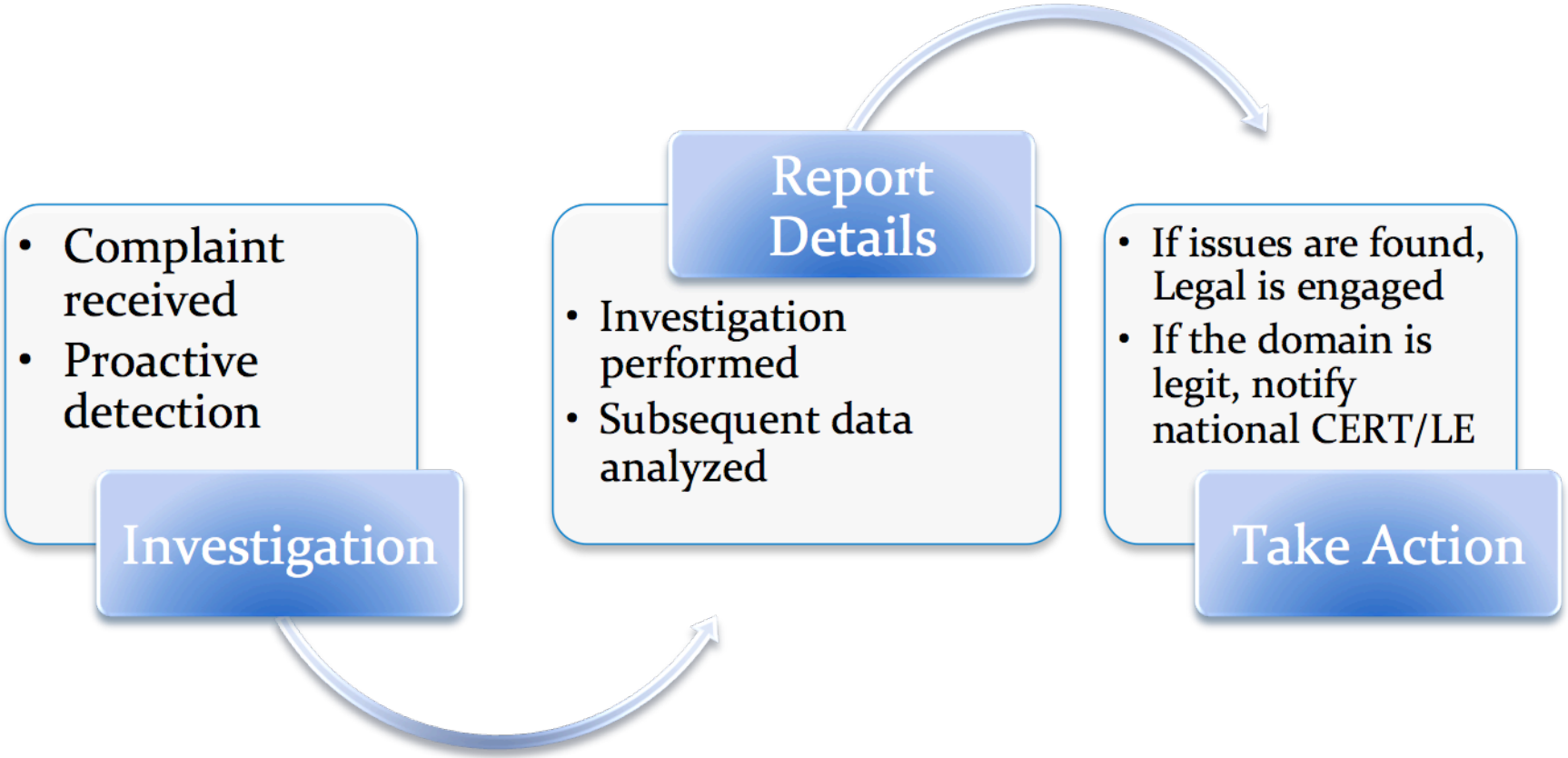
NEUSTAR™

DEFINITION OF ABUSE

- Appendix 11 .BIZ Registry Agreement
  - "Using the domain name for the submission of unsolicited bulk e-mail, phishing, pharming or other abusive or fraudulent purposes."
  - "reserves the right to deny, cancel, place on registry-lock or hold, or transfer any registration that it deems necessary, in its discretion, (i) to protect the integrity and stability of the registry . . (iv) to enforce, at its sole discretion, any of the Restrictions above….
- Does not include IP infringement, defamation, content or other use of a domain name.

NEUSTAR™

THE INVESTIGATIVE PROCESS



“TAKE ACTION”

- Once verified, we send report to Registrar sponsoring registration.
- Report contains a subset of investigation results
- Gives Registrars 12 hours to take down the name
- If no response, or if Registrar does not comply, we take the name out of the zone (Note Delete)
- Large majority of take down performed by Registrar within time
- Thousands of names taken down in .biz in past 3 years
  - No complaints, No legal actions.

NEUSTAR™

“TAKE ACTION”

- Industry participation a critical factor
  - Security forums
  - Security conventions
  - Security groups (private/public)
- Integration of law enforcement into processes
  - Collaborative effort to share/verify data
    - Verification of Child Porn done by LE
    - Results of our investigative process shared with LE
  - Do not want to hinder current investigations
  - Still need to continue these efforts (lots of work to be done still)

NEUSTAR™

So where does the Sheriff come in to it?

- Respond promptly to LE Questions
- Claim “privilege” only when it is real
- Privacy and ToS are not necessarily in opposition
- Respond to Complaints from LE
- Have a clear and public policy

NEUSTAR™

And what can you hope to gain?

<B> C got busted

<A) Lamo noob. Why?

<B> fool *** scammed with a .zzz domain They dropped a dime on him to Feds

<A> lol

<A> I wont **** with them any more.

Prefer ***** at .AAA or .BBB. Bulletproof.

NEUSTAR™

And what can you hope to gain?

- When you have a problem, the Sheriff rides in
- Bad guys go elsewhere
- Networks don’t block domains
- Complaint numbers drop
- Legitimate users prefer your TLD
- More $$$

NEUSTAR™

Confidential and proprietary