We want the Internet to work better.

**BIND 10**
The next big thing in DNS

**ISC Professional Services**
support  development
training  consulting
audit  design
Call in the experts!

**SNS@ISC**
The ultimate insurance policy for your DNS

**ISC is Public Benefit**
F-root  DHCP
SNS-PB  AFTR
BIND  and more
Do what you can to support us

**SIE**
Changing how the security communities productively collaborate

**RPZ**
New method for DNS-based policy enforcement
Taking back the DNS!

**RPKI**
Securing BGP from route hijacking

You are here
Conficker

- Background
- What we (still) do
- How you can help

This is old news isn't it?
What is it?

- It's a worm/virus/superbug.
- Background reading:
  - http://www.confickerworkinggroup.org
  - http://mtc.sri.com/Conficker/
- Security community stepped up
- The developer fought back.
- We're not winning, but we haven't lost.
- Whatever doesn't kill you makes you stronger.
  - Cabal -> CWG -> more
Easy to detect

- Changes host computer so it cannot access domains that help fix a computer.
DNS Containment (A/B)

- Started with a single-domain DNS callback mechanism
  - Stomped a few domains
- Modified to domain auto-generation
  - 500 domains / day
  - Predictable date-based pseudo-random domain generation for callbacks
    - COM, ORG, NET, INFO, BIZ, etc
- Developed auto-registration process
  - Contained (?)
Sinkhole

- Register 3 nameservers for every domain
  - Fate sharing
- Nameservers point web callback hits to a web server (specially designed)
- Clients get nothing – contained (?)
Sinkhole

- Web hits used for mitigation – clients exposed themselves
- Can generate reporting and feedback for remediation
Containment (C)

- Modified domain auto-generation
  - 50000 domains / day
  - Included ccTLDs
  - Exposed weakness in registries
- We tried to contain
  - Norm at ICANN 35 (Sydney, June 2009)
  - Some success
  - Without 100% success -> fail
- Other methods
  - P2P

Not!
In the meantime...

http://spartanlaser.gtisc.gatech.edu/reports/
Winning!

- Wel, no
  - ccTLD participation
  - What did the registries learn?
  - Mostly unfunded mandate (*)
    - Security products (free or unpaid)

- Old focus: Containment + SSR efforts
- New focus: Keep chasing the long tail (~5)
How to help

- You are a ccTLD.
- Domain AXFR/IXFR of fake root from CWG
- Script to extract and manage domains
  - 3-day focus: yesterday/today/tomorrow
  - `extract-domains $TLD`
  - You provide two programs:
    - `add-domain $domain`
      - We check if already registered
      - If not, register (reserve, just like IANA does)
    - `remove-domain $domain`
      - if registered to CWG nameservers
Sinkhole++

- Want to run a sinkhole?
- Httpk
- Keep data for yourself – contribute to CWG
- Risk-spreading

<info@sie.isc.org>
Thank you (specific)

- Specifically:
  - ICANN
  - Microsoft
  - GTISC
  - [redacted]

- Generally:
  - Sinkhole operators
  - DNS Hosters
  - Public benefit mitigators
  - TLD operators who participate