Special Use Domain Names of P2P Systems

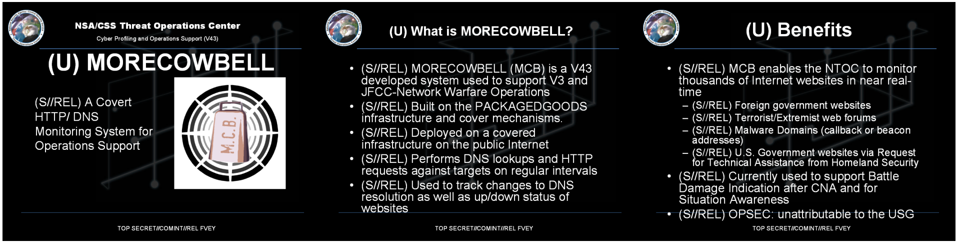
Christian Grothoff

July 20, 2015

1+1=2

- NSA “kills based on meta data” –Michael Hayden (former NSA director)
- DNS makes it trivial to gather meta data about most Internet activities

“The Domain Name System is the Achilles heel of the Web.” –Tim Berners-Lee



NSA/CSS Threat Operations Center

Cyber Profiling and Operations Support (V43)

(U) MORECOWBELL

(S//REL) A Covert HTTP/ DNS Monitoring System for Operations Support

TOP SECRET//COMINT//REL FVEY

(U) What is MORECOWBELL?

- (S//REL) MORECOWBELL (MCB) is a V43 developed system used to support V3 and JFCC-Network Warfare Operations
- (S//REL) Built on the PACKAGEDGOODS infrastructure and cover mechanisms.
- (S//REL) Deployed on a covered infrastructure on the public Internet
- (S//REL) Performs DNS lookups and HTTP requests against targets on regular intervals
- (S//REL) Used to track changes to DNS resolution as well as up/down status of websites

TOP SECRET//COMINT//REL FVEY

(U) Benefits

- (S//REL) MCB enables the NTOC to monitor thousands of Internet websites in near real-time
  - (S//REL) Foreign government websites
  - (S//REL) Terrorist/Extremist web forums
  - (S//REL) Malware Domains (callback or beacon addresses)
  - (S//REL) U.S. Government websites via Request for Technical Assistance from Homeland Security
- (S//REL) Currently used to support Battle Damage Indication after CNA and for Situation Awareness
- (S//REL) OPSEC: unattributable to the USG

TOP SECRET//COMINT//REL FVEY

Secure P2P systems explore alternative protocol designs.

.bit

Properties of NameCoin

- *name*`.bit` resolved using global timeline
- Timeline constructed using BitCoin technology
- NameCoin is an AltCoin (different block chain)
- Implemented in 2011, inspired by Aaron Swartz's Squaring Zooko's Triangle

.exit

Properties of .exit

- *domainname.relay*`.exit` used to explicitly select Tor exit node
- Useful to escape geo-blocking
- Implemented and deployed in about 2004
- x509 CA signing makes no sense ⇒ separate draft

.gnu and .zkey

Properties of the GNU Name System (GNS)

- Decentralized name system with secure memorable names
- Provides alternative public key infrastructure
- Interoperable with DNS (like gopher → http)
- Achieves query and response privacy
- Uses *name*`.gnu` for memorable names
- Uses *key*`.zkey` (zone key) for global identifiers
- Implemented since 2013 in GNUnet, discussions about adoption with I2P, Tor, GnuPG, Matrix and others

.i2p

Properties of I2P

- *name*.i2p resolved like /etc/hosts via local database
- *key*.b32.i2p again like .zkey and .onion
- Implemented and deployed in about 2002-2003

.tor

Properties of .tor

- *name*.tor resolved via consensus among Tor routers
- Allocation is first-come-first registered (in consensus)
- Global names, without the cost of NameCoin's proof-of-work
- Currently being implemented as part of OnioNS effort
- Do you want a draft?

.carrots

Properties of `.carrots`

- No real deployment **and**
- No technical innovation **and**
- No community support

Implication of special-use drafts

- IETF informs and advises ICANN and operators
- ICANN and operators can still do what they want!
- They may become obsolete in $<$ 30 years: `.bitnet`, `.csnet`, `.oz`, `.uucp`

Thanks to Hellekin Wolf (GNU), Jacob Appelbaum (Tor), Leif Ryge, Mark Nottingham, Martin Schanzenbach (GNUnet) Matthias Wachs (GNUnet), phelix (NameCoin), Richard Stallman (GNU), Seth Schoen (EFF), str4d (I2P), Werner Koch (GnuPG), Zooko Wilcox-OHearn, zzz (I2P) and anybody else who helped.