(U//FOUO) QUANTUMTHEORY

(U//FOUO) name redacted S32X

TURBULENCE
GC HQ
MHS
TAO
This presentation is classified:

TOP SECRET // COMINT // REL TO USA, FVEY // 20320108
(U) What is QUANTUM THEORY

- (U/FOUO) Nothing to do with “Quantum Computing”

- (S//SI//REL) Protocol injection technique
  - Passive
  - Active

- (S//REL) Not Man-in-the-Middle
  - But can be used to gain that position

- (S//REL) Man-on-the-Side

- (S//REL) Mostly Low Latency… mostly
(C) Components of QUANTUM Architecture

- (S//REL) TURMOIL
  - (or LPT, LPT-D, what else can you kludge for tipping... cough.. NINJANIC)
  - Passive Sensor

- (S//REL) TURBINE
  - Active Mission Logic of Remote Agents

- (C//REL) ISLANDTRANSPORT
  - Messaging Fabric

- (S//REL) SURPLUSHANGER
  - High->Low diodes

- (S//REL) STRAIGHTBIZARRE or DAREDEVIL
  - Implant / Shooter
(C) Legacy QUANTUM THEORY techniques

- (TS//SI//REL) QUANTUM INSERT
  - HTML Redirection

- (TS//SI//REL) QUANTUM SKY
  - HTML/TCP resets

- (TS//SI//REL) QUANTUM BOT
  - IRC botnet hijacking
(U) New Hotness

- (TS//SI//REL) QUANTUMBISCUIT
  - Redirection based on keyword
  - Mostly HTML Cookie Values

- (TS//SI//REL) QUANTUMDNS
  - DNS Hijacking
  - Caching Nameservers

- (TS//SI//REL) QUANTUMBOT2
  - Combination of Q-BOT/Q-BISCUIT for web based Command and controlled botnets
(U) Experimental

- (TS//SI//REL) QUANTUMCOPPER
  - File download disruption

- (TS//SI//REL) QUANTUMMUSH
  - Virtual HUFFMUSH / Targeted Spam Exploitation

- (TS//SI//REL) QUANTUMSPIM
  - Instant Messaging (MSN chat, XMPP)

- (TS//SI//REL) QUANTUMSQUEEEL
  - Injection into MySQL persistent database connections

- (TS//SI//REL) QUANTUMSQUIRREL
  - Truly covert infrastructure, be any IP in the world
(C) Where/What can you QUANTUM

- (S//SI//REL) Menwith Hill Station (USJ-759, USJ-759A,...)
  - Operational: Q-INSERT, Q-SKY, Q-DNS, Q-BISCUIT, Q-BOT
  - Tested: Q-COPPER, Q-SQUIRREL, Q-BOT2

- (S//SI//REL) Misawa AFB (USF-799,...)
  - Operational: Q-INSERT

- (S//SI//REL) INCENSOR (DS-300) – with help from GCHQ
  - Operational: Q-BOT, Q-BISQUIT, Q-INSERT
  - Tested: Q-SQUEEL, Q-SPIM

- (TS//SI//REL) NIPRNET Gateways
  - Operational: Q-DNS

- (S//SI//REL) Coming Soon....
  - SMOKEYSINK
  - SARATOGA
Questions?

contact info redacted