VERISIGN™

Automated Indicators in Telecom

NIST Information Security and Privacy Advisory Board Panel Discussion

Danny McPherson
CSO, Verisign
February 15, 2013

Information Sharing – Means, Not End!

- 403M unique malware variants in 2011 [SYMC]
  - Traditional AV less than perfect..
  - Trend toward heuristics, behavioral, reputational (IP, name, etc.)
- > 80% of IT security spend for regulatory compliance
  - ~900 controls @VRSN just to check boxes
  - Most effective controls @VRSN rely on relational and behavioral techniques, number and namespace reputation, some heuristics
- "In Telecom" inherently assumes perimeter-based defenses
  - May control propagation –but only until new delivery mechanism employed

VERISIGN

Sharing Silos, C2 resilience…

- Sharing Silos..
  - Sector-specific ISACs, other silos create walls
  - How common are threats and adversaries across sectors; are the silos really necessary?
- Community-driven sharing today..
  - Lots of operational security “trust groups”, share C2, attack sources, malcode, etc…
  - Little return today today on sharing with upstream or [suspect] origin networks per ROI (just not there for ISPs)
- Forces diffusion to alternative techniques
  - C2 most resilient CDN functions
  - Herders evolved quickly (IRC, IP, names, P2P, DGAs, social and other rendezvous techniques)

VERISIGN

Challenges

- Trust Groups
  - Scope of sharing..
- Privacy
  - …
- Provenance & metadata
  - Who, when, methods, enriched?
- Reclamation
  - Bot hosts sanitized, how to get reputation back
- Intermediaries
  - NAT/NAT-PT and CGNs w/IPv6 transition
- Multi-tenancy
  - Virtualized infrastructure
  - Proxies
- Fragmented responses can be problematic
  - E.g., C2 disruption may impact surveillance or disruption, create zombies
- Classification and Terminology
  - Disparity across vendors causes confusion
- Effectuated controls MUST BE surgical
  - else impacted systems can't be sanitized
  - may impact converged services (e.g., NGA, 911, VoIP, etc.)

VERISIGN

Thank You

VERISIGN™