

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Hackback? Claptrap! - An Active Defense Continuum for the Private Sector

SESSION ID: LAW-R02

Moderator: Randy V. Sabet, J.D., CISSP
Special Counsel, Cooley LLP

Panelists: Stewart Baker
Partner, Steptoe LLP

Dr. Irving Lachow
Principal Cybersecurity Engineer, MITRE

Steve Chabinsky
General Counsel and Chief Risk Officer,
CrowdStrike

James Denaro
Partner, CipherLaw



DISCLAIMER

- ◆ **Legal disclaimer:** Nothing we discuss today constitutes legal advice. For any specific questions, seek the independent advice of your attorney, query the cloud, or ask your social network. Furthermore, Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet...



“Claptrap”

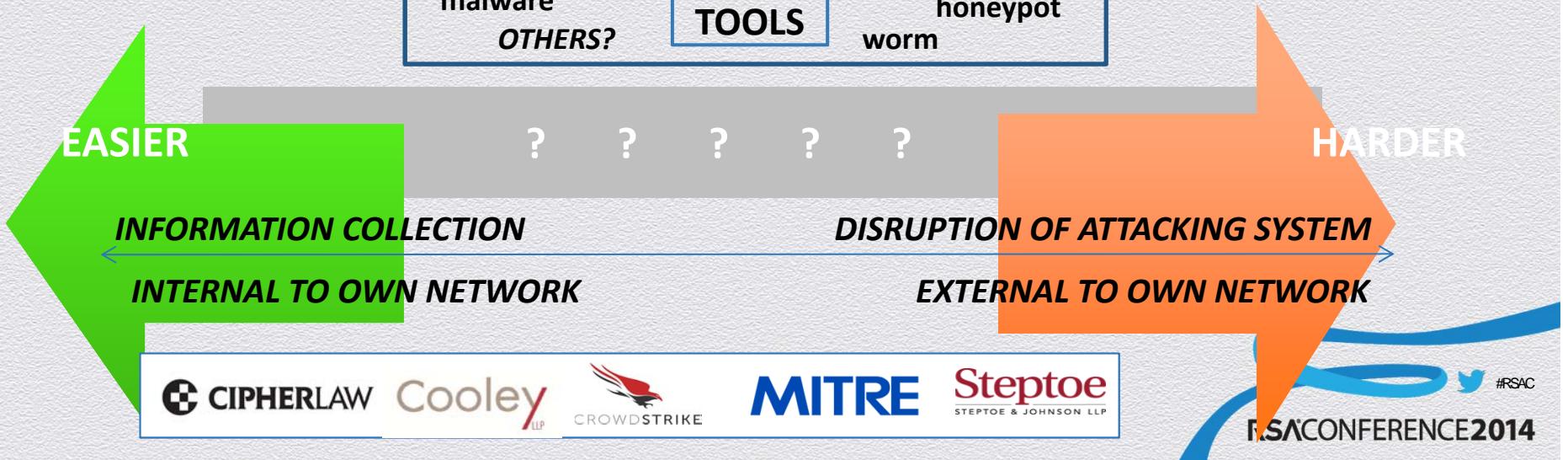
- ◆ For those of you who didn't get a chance to look it up:
 - ◆ “absurd or nonsensical talk or ideas”
 - ◆ “words, ideas, etc., that are very foolish or stupid”
 - ◆ “bombast”



| | | | | | |
|-------------------------|----------------------|------------------|------------------|---------------------|------------------------|
| Destroy incoming attack | Identify DDoS | Disrupt attacker | Destroy own data | Locate | Access |
| Destroy attacker | Plant misinformation | Disable own data | GOALS | Collect information | Determine capabilities |

Active Cyber Response: a diverse set of TTPs (a) used for identifying, detecting, analyzing, and mitigating network threats and (b) classified along a spectrum of risk and permissiveness

| | | | |
|-------------------|----------------|---|------------------|
| ping/echo SNMP | nmap beacon | self-encrypting or self-destroying files malware <i>OTHERS?</i> | honeypot worm |
|-------------------|----------------|---|------------------|



(Any more) questions?



Cooley
LLP



MITRE

Steptoe
STEPTOE & JOHNSON LLP



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Hackback? Claptrap! - An Active Defense Continuum for the Private Sector



CIPHERLAW

Cooley
LLP



CROWDSTRIKE

MITRE

Steptoe
STEPTOE & JOHNSON LLP