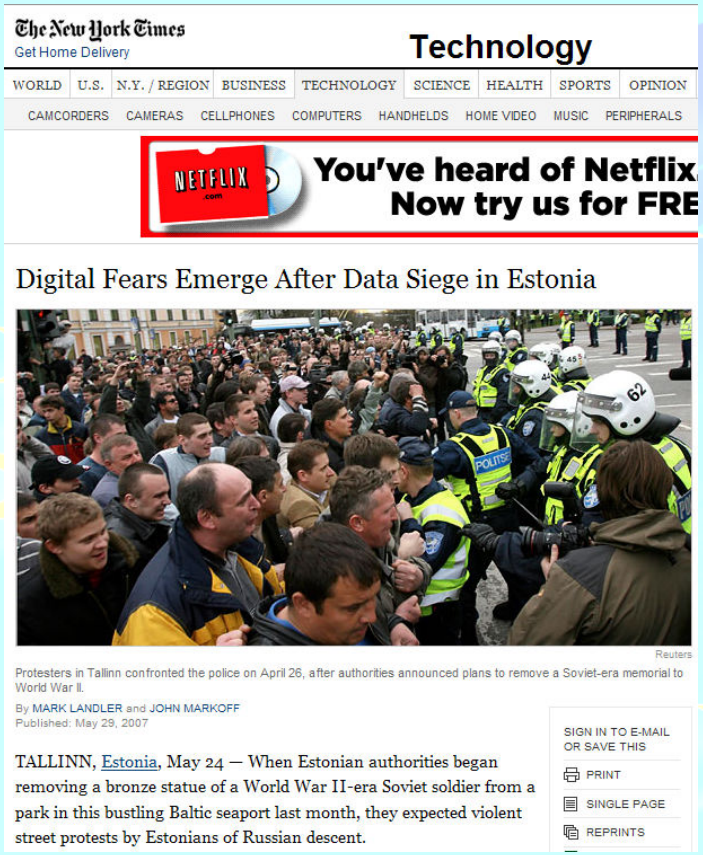
Council of Europe
Octopus Interface Conference
Cooperation Against Cyber Crime
March 10-11, 2009
Strasbourg, France

e-crime from a Technology Point of View

Chet Hosmer, President

WetStone Europe

eCrime Technology Impact



The New York Times
Get Home Delivery

Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

CAMCORDERS | CAMERAS | CELLPHONES | COMPUTERS | HANDHELDS | HOME VIDEO | MUSIC | PERIPHERALS

Digital Fears Emerge After Data Siege in Estonia

Reuters

Protesters in Tallinn confronted the police on April 26, after authorities announced plans to remove a Soviet-era memorial to World War II.

By MARK LANDLER and JOHN MARKOFF
Published: May 29, 2007

SIGN IN TO E-MAIL OR SAVE THIS
PRINT
SINGLE PAGE
REPRINTS

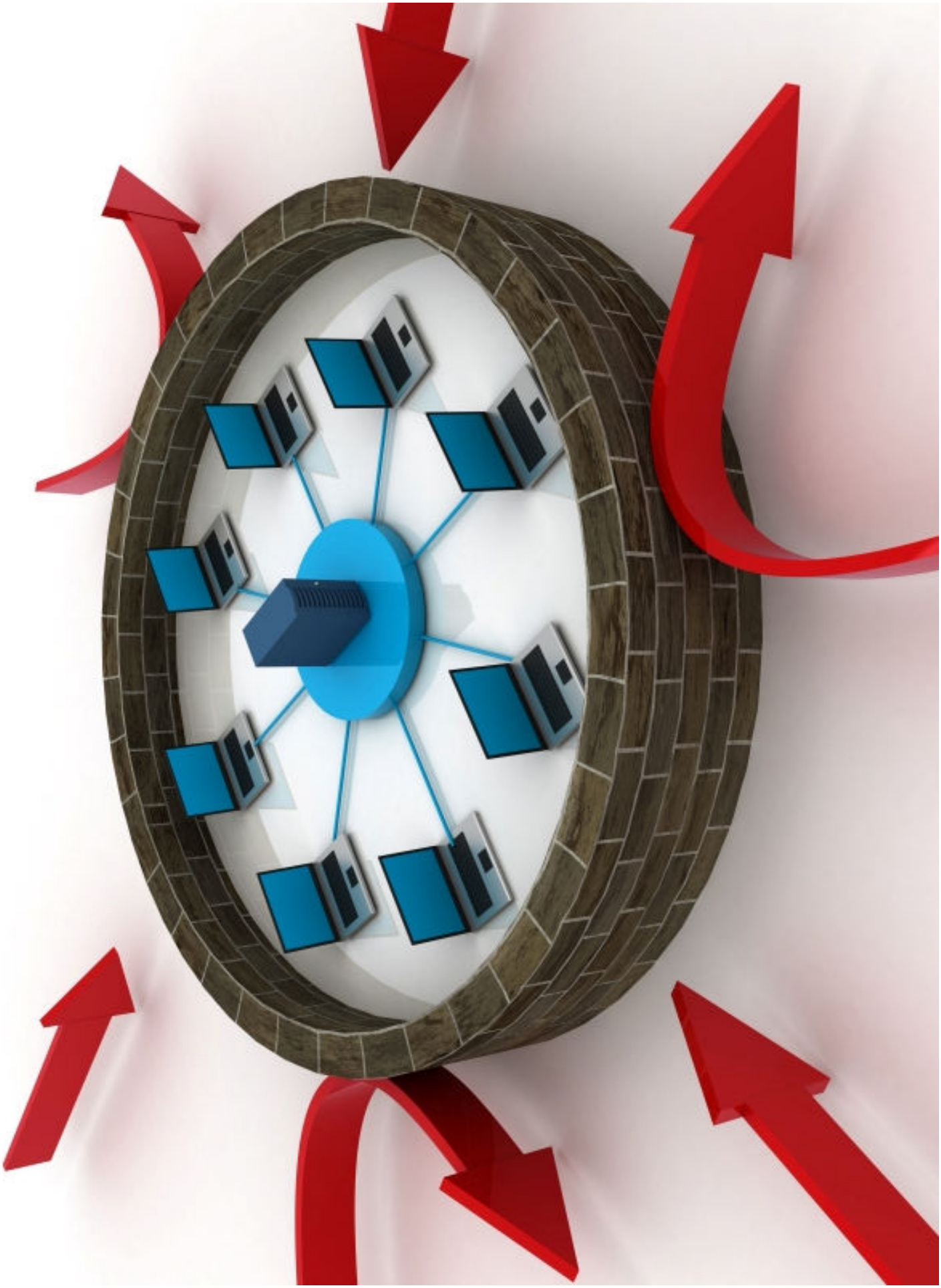
TALLINN, Estonia, May 24 — When Estonian authorities began removing a bronze statue of a World War II-era Soviet soldier from a park in this bustling Baltic seaport last month, they expected violent street protests by Estonians of Russian descent.

WIRED MAGAZINE: ISSUE 15.09

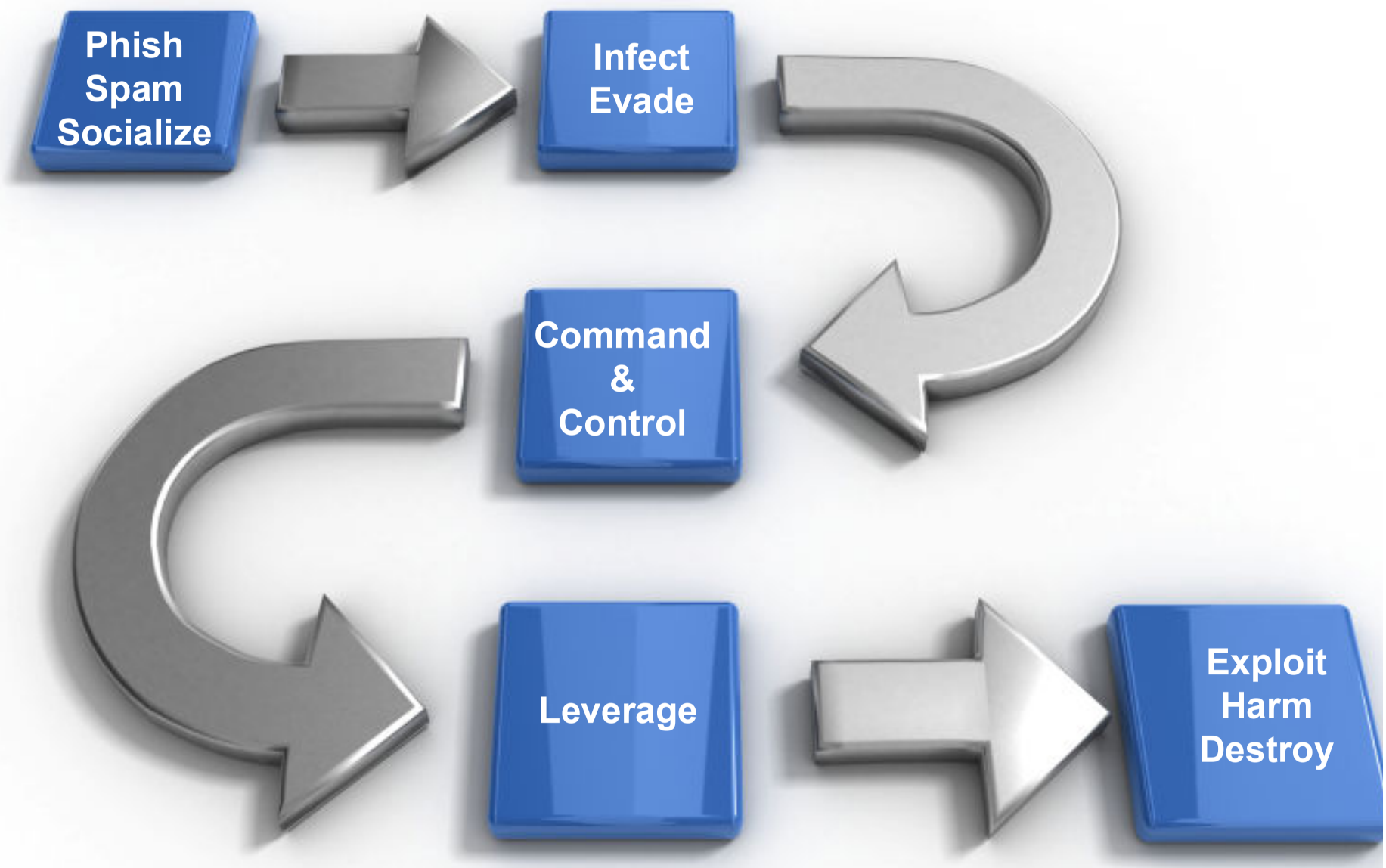
Hackers Take Down the Most Wired Country in Europe

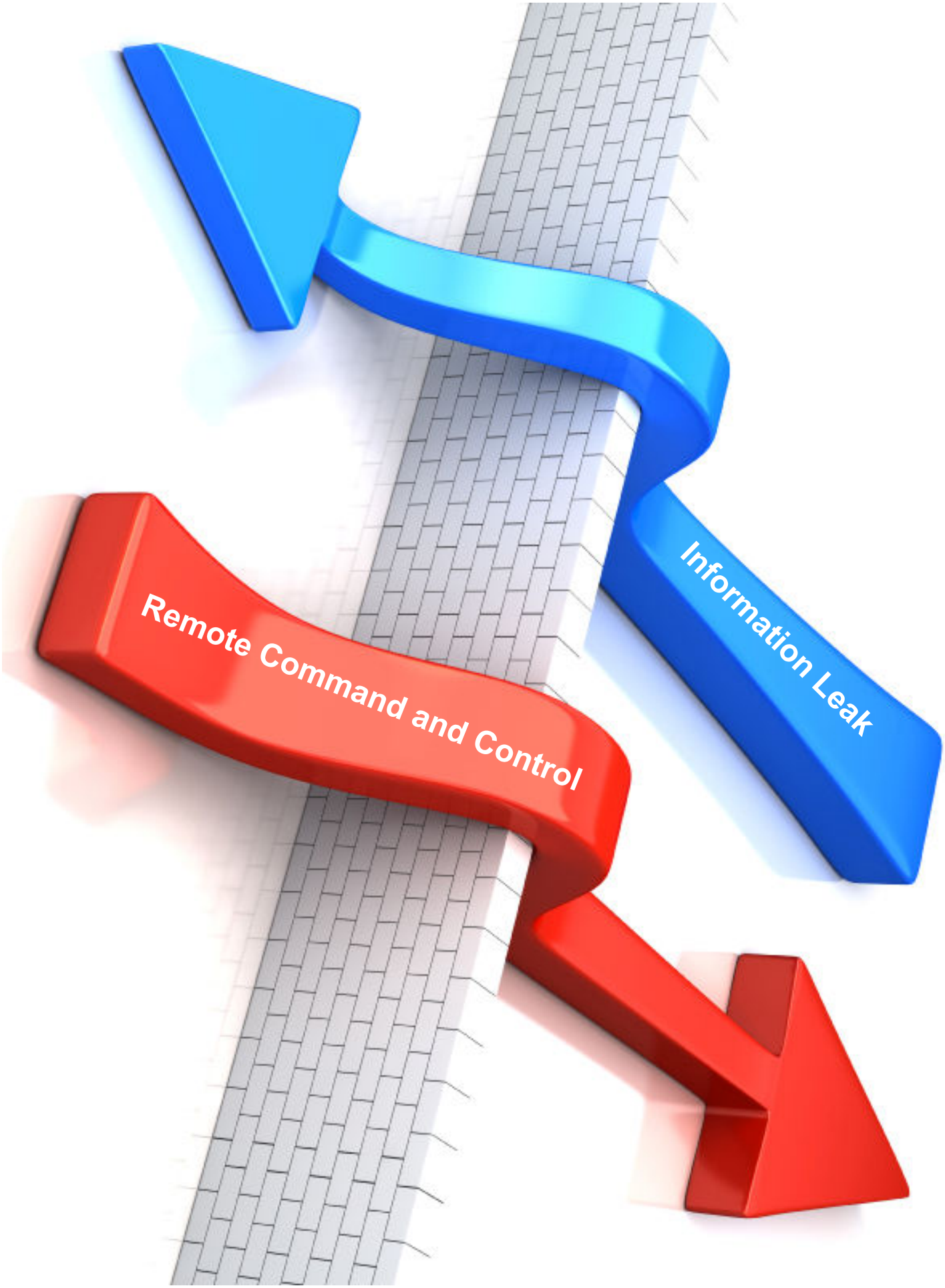
By Joshua Davis 08.21.07 | 2:00 AM

Source: NY Times and Washington Post




Facebook
MySpace
Bebo
FaceParty
Twitter
Blip


Phish
Spam
Socialize
Infect
Evade
Command
&
Control
Leverage
Exploit
Harm
Destroy


Information Leak
Remote Command and Control

Critical eCrime Technology Evolution

- Critical Emerging Threats
  - Broadband expansion in China and India
  - Attacks on Social Networks
  - Stealthware and AntiForensics
  - Zero Day Exploits on Applications

Broadband expansion in China and India

- Predictions
  - China and India will reach approximately 30 percent of broadband adoption to the home by 2011

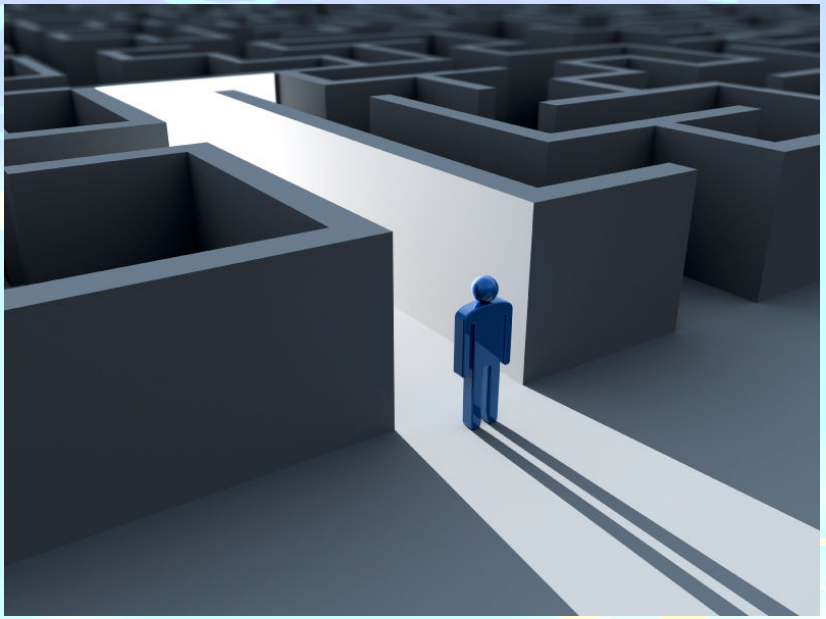
  - Infections and Botnet creation is already growing with an estimate of 50-100 million zombies operational there by 2012

Attacks on Social Networks

- Predictions
  - By 2011 Over 70% of exploitations will originate from social networks
  - The exploits will cross contaminate between and among social networks
- Proof
  - The Koobface worm which has in the past attack Facebook is affecting users at MySpace and Bebo
  - The worm is now infecting friends not only the original duped user

Stealthware and AntiForensics

- Predictions
  - Worms, Bots, Keyloggers and Rootkits are employing countermeasures
    - Poly and Metamorphism
    - API hooks are adding stealth
  - The latest threats can sense their environment
  - Exploits are memory resident and temporal
  - Bot controls are smarter, riding on top of allowed protocols (http, rtp, udp)
  - Most can avoid AV detection
  - When detection occurs they aggressively cause destruction



Zero Day Exploits on Applications

- Predictions
  - Crimeware inventors are targeting high value application beyond e-mail and web
  - User's inherently trust these applications and believe they are safe

- Proof
  - An exploit was recently discovered for a previously unknown bug in Adobe Acrobat one of the most widely used and trusted user applications
  - Adobe hopes to have a fix out within a month allowing a windows of opportunity millions of infections and zombie deployments

Mitigating the Threat

Keys to Threat Mitigation

- Top 10
  1. Investment in research like we mean it
  2. Investment in training at all levels
  3. Clearly define operational policies
  4. Consistently audit and measure against these policies
  5. Aggressively prosecute/sentence the spammers, phishers and bot operators
  6. Globally collaborate with regards to eCrime
  7. Make it as cool for young people to catch and expose hackers as it is to be one
  8. Define better standards for internet protocols that consider security as a primary objective
  9. Hold software companies accountable
  10. Develop new software development tools that evaluate security and safety as as an integral part of the process

Chet Hosmer
chet@wetstonetech.com