Session Number C22
Introduction to Advanced Security Threats

Bryan Kissinger, PhD

ISACA SF Fall Conference
November 8th, 2011

Discussion Points

- Traditional Security Threats
- The Evolving Threat Landscape
- Securing the Future

Traditional Security Threats

Terminology

- Malware – Malicious software that consists of programming (code, scripts, active content and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. [1]
- Virus – A computer program that can copy itself and infect a computer. A true virus can spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as CD, DVD, or USB drive. [2] [3]
- Worm – A self-replicating malware computer program, which uses a computer network to send copies of itself to other nodes and may do so without any user intervention. This is due to security shortcomings on the target computer. Unlike a virus, it does not need to attach itself to an existing program. Almost always, worms cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

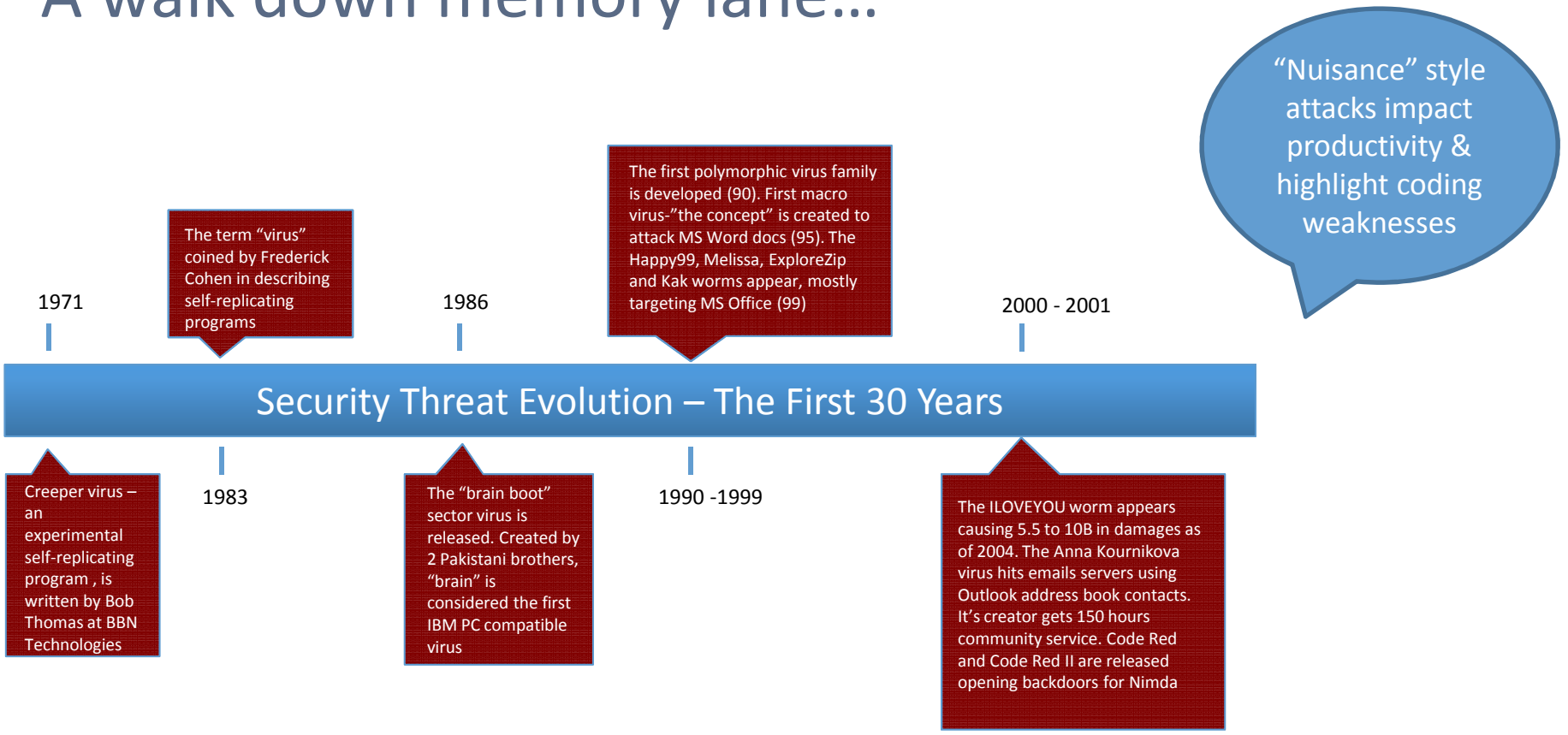
Traditional Security Threats

Terminology

- Adware/Spyware – Adware is typically not destructive by intention, but rather automatically plays, displays or downloads advertisements to a computer. Spyware is software that can be installed on computers with the intention of collecting small pieces of information about users without their knowledge.
- Bot or Botnet – A computer becomes a bot when it downloads a file (e.g., an email attachment) that has bot software embedded in it. A botnet is a collection of infected computers or bots that have been taken over by hackers and are used to perform malicious tasks or functions. A botnet is considered a botnet if it is taking action on the client itself via IRC channels without hackers having to log in to the client's computer. The typical botnet consists of a bot server (usually an IRC server) and one or more bot clients. [4]

Traditional Security Threats

A walk down memory lane…



Traditional Security Threats

General premise of operation:

1. Exploit known vulnerabilities in O/S and Application code
2. Generally, damage was denial of service and/or defacement with recognition sought by hacker
3. Countermeasures by patching vulnerabilities or updating anti-virus signatures and firewall rule sets usually remediated the breach

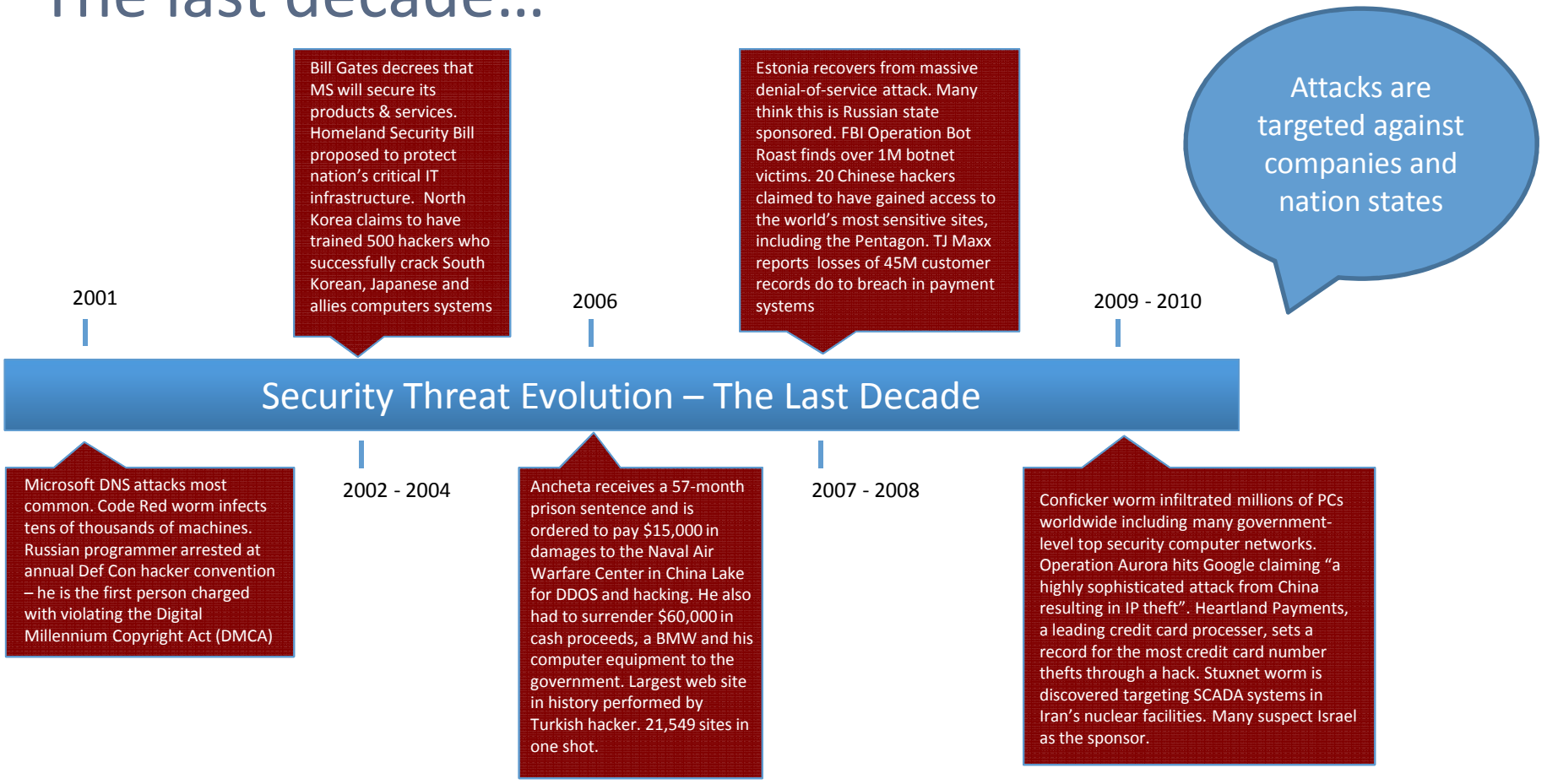
Traditional Security Threats

Observations on threat activity:

- Hacking actors range from bored teenagers to disgruntled IT employees
- Hacking activities are not monetized
- Many companies did not report or underreported these incidents making catching the hacker a low or non-priority
- Law enforcement mechanisms are weak or non-existent

The Evolving Threat Landscape

The last decade…

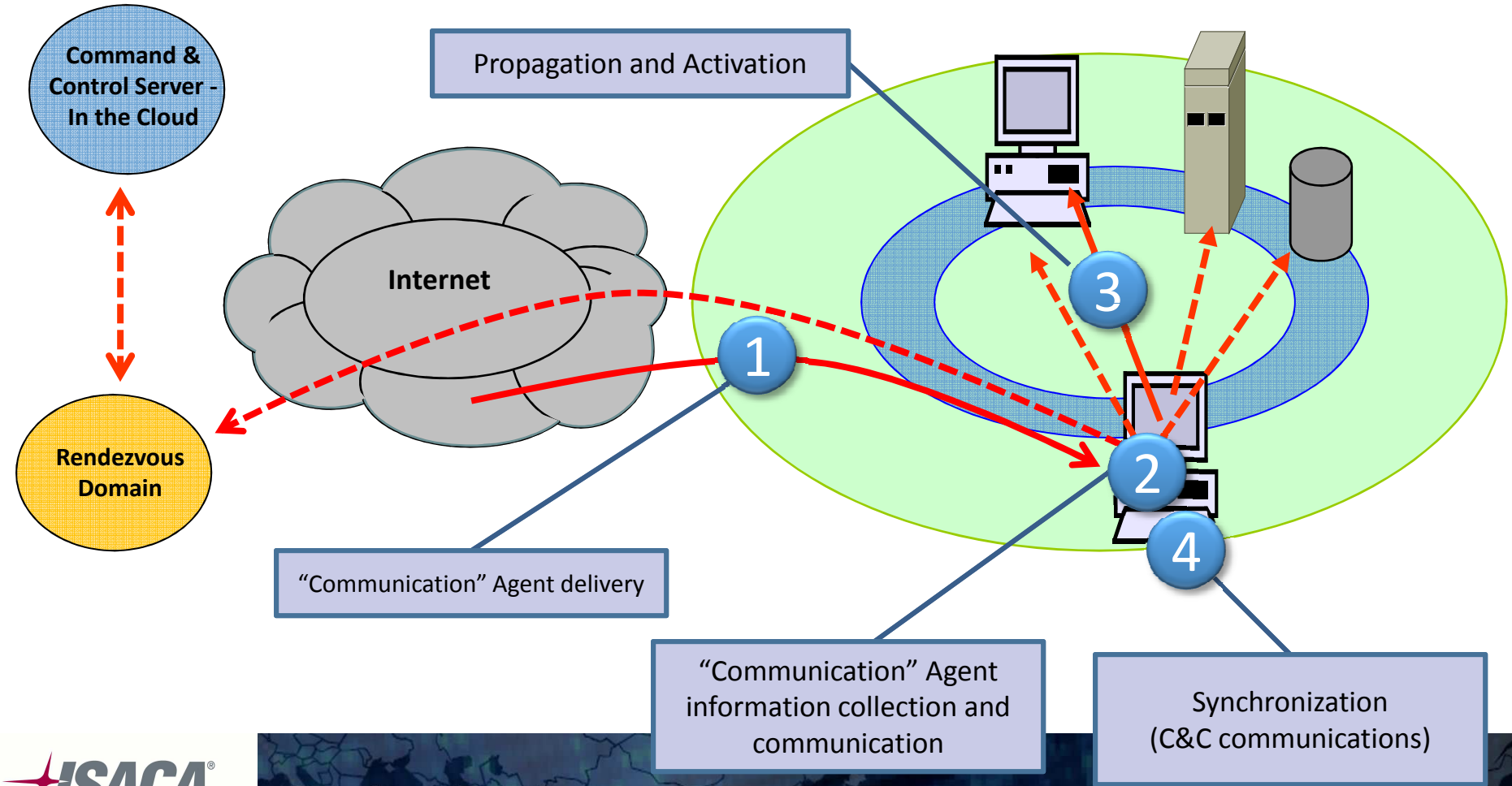


The Evolving Threat Landscape

2011, so far:

- Hacker group Lulz security is established
- U.S. Senate systems are attacked by hacker group Lulz Security
- In mid-March, Boston-based cryptography firm RSA suffered a massive network intrusion that resulted in the theft of information related to its SecurID tokens. 40M people use the tokens to access the internal computer networks of 25,000 corporations, government organizations and financial institutions. A month later, defense contractor Lockheed Martin had its own networks penetrated by attackers who used "cloned" RSA tokens made with data taken in the original breach. Unconfirmed reports named defense contractors Northrop Grumman and L-3 Communications as other victims.
- In early April, hackers penetrated the internal networks of Epsilon, a Texas-based firm that handles email communications for more than 2,500 clients worldwide. The companies affected by the Epsilon hack included Ameriprise Financial, BestBuy, Capital One Bank, Citi, JPMorgan Chase, TiVo, U.S. Bank and dozens more.
- April 17: Sony experiences an “external intrusion” that sends the PlayStation network offline and comprises sensitive information of it’s members, possibly including credit card numbers (cited as one of the 5 largest data breaches ever)

Conficker High-level Overview



The Evolving Threat Landscape

So what's happening now?

The Evolving Threat Landscape

General premise of operation:

1. Goal is to compromise an internal networked system to use it for synchronization and command & control communications
2. Once an internal system is “owned”, an external user can:
   - Access sensitive data and extract it
   - Upload code or programs that lie dormant and wait to be triggered
   - Take over hundreds or even thousands of network resources to capture bandwidth for other hacking activities
3. Escape without the target ever knowing a hacker was there

The Evolving Threat Landscape

Observations on threat activity:

- Hacking actors have become more sophisticated and funded
- State sponsorship and the use of “cyber warfare” seems to be increasing
- Intent has shifted from “fun” and “recognition” to specific outcomes or monetary gain

The Evolving Threat Landscape

Hacking attack Video – “SSL Strip”

Content courtesy of: Security Risk Advisors, Inc.

info@securityriskadvisors.com

Securing the Future

Attackers are more creative than ever:

- Spearphishing/phishing campaigns
- USB thumb drive drops
- Mobile device man-in-the-middle attacks
- Social engineering
- Foreign country trusted networks
- “Advanced Persistent Threats” - APTs

Securing the Future

Spearphishing & Phishing Campaigns:

- Spearphishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information [5].
- Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal.

Prevention: Education & Awareness of end-users to be wary of all emails from these supposed “trusted sources”

Securing the Future

USB Thumb Drive Drops:

Images courtesy of: http://laughingsquid.com/usb-flash-drive-dead-drops-installed-in-public-locations-around-nyc/

Securing the Future

Mobile Device Man-in-the-Middle Attacks:

- A form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle).

Prevention: Strong authentication between hosts, public key infrastructures, secret keys and latency examination

Securing the Future

Social Engineering:

- The use of routine or non-suspect activities to take advantage of relaxed physical security or non-technical controls. Examples include shoulder surfing, piggy-backing, dumpster diving and “IT Customer calls”.

Prevention: Enforce physical security rules and periodically test your workforce’s adherence to policies for protecting routine activities that involve sensitive data

Securing the Future

Foreign Country Trusted Networks:

- Connections to international locations are ripe for bad actors to use a trusted network to gain entrance into the US segments.

Prevention: Work with your network architects to understand how high risk network segments connect to US segments. Separate networks with limited connections are the best protection. Segmentation with special monitoring will help to mitigate risk. Thoroughly vet foreign employees through background checks

Securing the Future - Advanced Persistent Threats

Highly Sophisticated Next Gen Attacks

Targeted, custom, encrypted, morphing, multiple “agents”
Reconnaissance, “zero-day” and distributed attacks over many months

Well Funded: Crime, Terrorism & Cyber Warfare

$5.4B lost in cyber theft of data and funds in 2010 (CNET stats)
Citibank, Google, Intel, NY Power Grid and many others were attacked

Existing Security Infrastructure considered **Inadequate**

Signature and heuristic based approaches obsolete
Distributed deployment renders current behavioral analysis ineffective

Industry Leaders Agree - **New Solution Required**

Securing the Future - Neutralizing APTs

- A need for “accelerated analysis”
  - Concept akin to “virus culture” in medical field
- Ability to predict outcomes before they happen
  - Analysis of application interactions to detect abnormal traffic
- Ability to take broader looks at traffic
  - Analysis of decentralized communications
- Capability to “learn”
  - Develop “personalities” for each network

Securing the Future – APT Market Analysis

- Advanced Persistent Threat (APT) Protection Spend
  - New spending by Global 2000 companies to prevent APT: $790M (Source: Global Consulting Firm)
  - US Government planning $1.3B spending on APT in 2011 (Source: Market Research Media)
  - Augments $1.5B Intrusion detection & prevention (IDS/IPS) market (Gartner)
  - Shift in security spending from compliance to data protection (Forrester)

Securing the Future – Oldies, but Goodies

- Protections that are always in style
  - Security awareness training and educational campaigns
    - Consider special training for super users and in-house developers
  - Device and media controls
    - Locking down USB ports and controlling how portable media are utilized
  - Monitoring
    - Use of Data Loss Prevention tools, alerting systems and other active defenses
  - Robust incident management program
    - Impacts of incidents can be mitigated if caught early and lessons learned employed

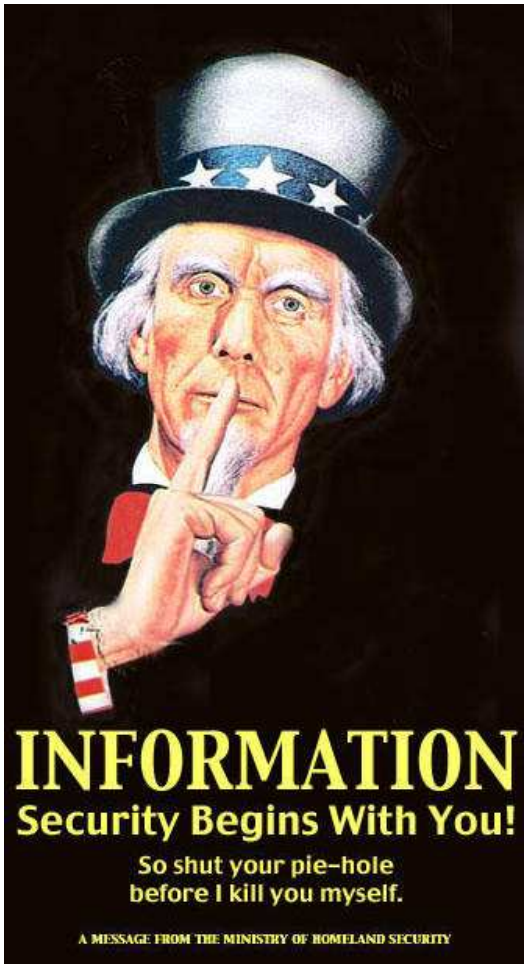


Image courtesy of: The Propaganda Remix Project

References

1. http://www.us-cert.gov/control_systems/pdf/undirected_attack0905.pdf
2. Dr. Solomon's Virus Encyclopedia, 1995, ISBN 1897661002, Abstract at http://vx.netlux.org/lib/aas10.html
3. Jussi Parikka (2007) "Digital Contagions. A Media Archaeology of Computer Viruses", Peter Lang: New York. Digital Formations-series. ISBN 978-0-8204-8837-0, p. 19
4. Craig A. Schiller ... [et (2007). "2". Botnets the killer web app ([Online-Ausg.] ed.). Rockland, MA: Syngress Publishing. p. 30. ISBN 9781597491358
5. http://searchsecurity.techtarget.com/definition/spear-phishing

Presenter: Bryan Kissinger, bryan.c.kissinger@kp.org