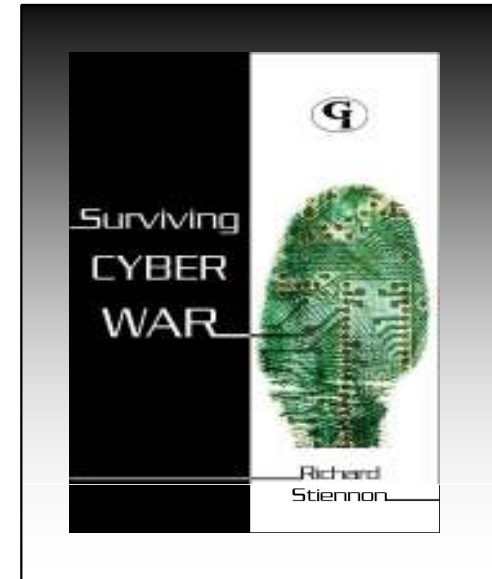


Cyber Scenarios

Richard Stiennon
Chief Research Analyst
IT-Harvest

Blog: ThreatChaos.com
twitter.com/stiennon





Blog: www.ThreatChaos.com

twitter.com/cyberwar



Scenario 1.

Collateral damage from cyberwar

- Wide spread state sponsored DDoS attack
- Communication outages
- Official web sites taken down



The reality

- August 8, 2008 Russia invades Georgia
- DDoS against Georgia
 president.gov.ge
 rustavi2.com
- Tulip Systems Atlanta
- 68,000 requests/sec





Scenario 2. Political protesters enlist social media to target attacks

Facebook or Twitter used to call protesters to arms

DDoS tools distributed along with instructions

Websites disabled



Twitter as tool of riot creation

Post Iranian election Twitter was used to support virtual riots via DDoS



Twitter escalation

Phase 1. Hacking instructions sites.

Phase 2. Links to pagereload.com

Phase 3. Links to a specially crafted site that opens 15 frames on pagereload.com



Scenario 3. An insider uses privileged access to steal customer data

- Despite strong authentication, encryption, and DLP, a trusted employee steals customer data
- Sells it to a third party



Countrywide data loss



Countrywide



- Rebollo estimated he downloaded about 20,000 customer profiles a week in excel spreadsheets onto the flash drives



Scenario 4. Malicious Software Updates

- A software vendor issues software updates that are malicious in nature
- Software is back-doored
- Systems compromised.



Athens 2004



A series of software updates turns on Lawful intercept function

104 diplomats and Olympic officials spied on

Engineer mysteriously commits suicide

Ericsson SPT 2700



Scenario 5. Hardware backdoors

- Hardware vendor builds backdoors into critical equipment
- Uses backdoor to steal confidential information
- Gains control of network



Hardware backdoors

- [REDACTED]
- [REDACTED]
- [REDACTED]



Scenario 6. Insider abuse

Insider uses knowledge of business
Systems and back office to get
around internal controls.

Loss of millions



Trading losses



January 2008, Jerome Kerviel covers up trading losses,
Largest trading fraud in history to be carried out by a single person.

\$7.14 Billion

5 year sentence reduced to 3



Scenario 7. State sponsored spying

- A nation state infiltrates dozens of computers belonging to key personnel
- Reads emails
- Steals information
- Uses information to impact diplomatic mission



Ghostnet

- Office of the Dalai Lama infiltrated through malware installed on computers
- Email servers completely owned
- Emails modified in transit
- Email read and acted on
- Over 1,200 infected computers globally



Sound familiar?

- Pentagon 2007
- Rio Tinto 2009
- Google Aurora 2010



Proposed change to your security organization

- Create a Cyber intelligence team

- Aurora

- Myrtle



Blog: www.threatchaos.com

email: richard@it-harvest.com

Twitter: twitter.com/cyberwar

