



Organized Cyber-Crime : A Case Study

UNECE, Geneva

Marco Ricca, IRIS, CEO
June 20th, 2009



News

- ❑ The Conficker Worm contaminated over 15 million hosts in more than 100 countries
- ❑ A new Web site trapped for drive-by attacks is detected every 14 seconds in the world

Observations

- ❑ As of 2005, cybercrime and computer fraud have been generating more illicit revenues than drug trafficking (US Treasury)
- ❑ Malware is used nowadays for extremely precise lucrative purposes

Threats

Infected emails, dangerous downloads, trapped websites, sudden data destruction, stolen information assets, tampered data, Internet scams, webpage defacements, illegal pirated content storage, spam relays, fakemails, virus, worms, Trojan Horses, spyware, phishing, botnets, password cracking, WiFi hacking, social engineering, hoax, buffer overflows, etc...

Two categories of threats : latent or targeted

Threats



Internal Network



Demilitarized Zone



Outside World

Two categories of attacks : frontal and client-side

Internet Impunity



WiFi ubiquitousness provides a strong supply of anonymous, broadband, free connection points

Relaying a communication on the Internet is trivial, while tracking a transaction through several countries is strenuous

Information Risk

Security vs safety

Security vs usability

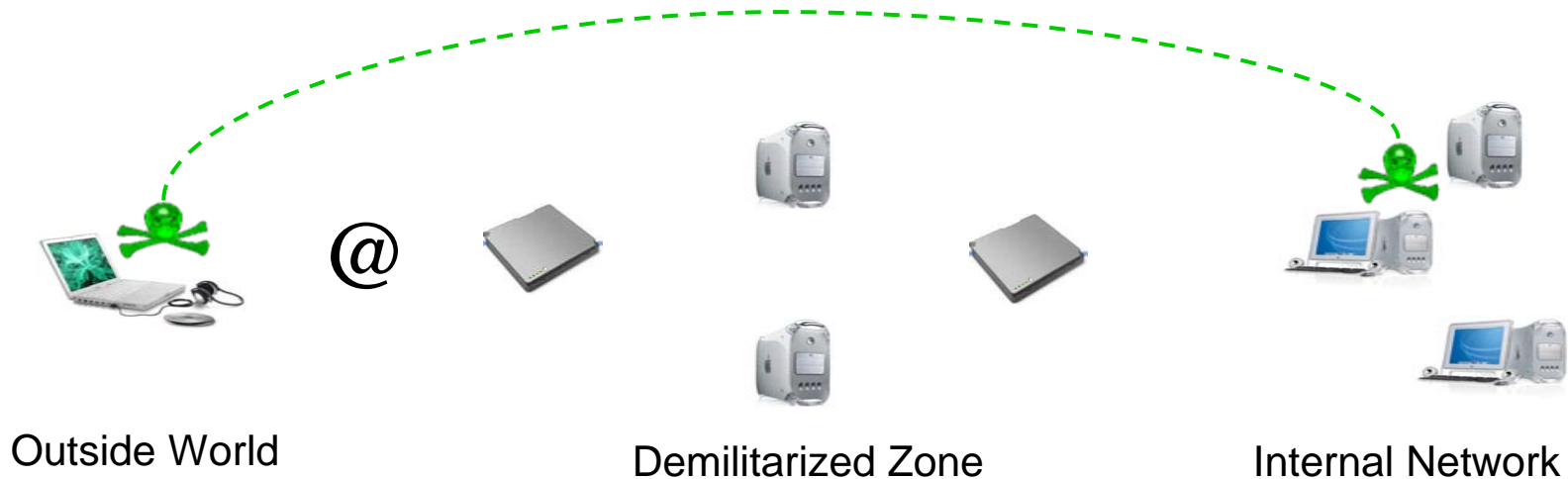
Risk transversality and volatility

Reactive vs pro-active security

Lim Prob(Intrusion) = 100 %
ressources → *infinite*

Case Study : Client-Side Attack

Criminal intention: access the internal user network (information, transactions, relay)



STEP 1 : Execute software on the user network (workstation)

STEP 2 : Communicate with the running software

Particularities

Human weakness is part of the vulnerability

Offline preparation : sudden and swift attack

Difficult to mitigate and detect

The implications can vary greatly

Information Risk

Security vs safety

Security vs usability

Risk transversality and volatility

Reactive vs pro-active security

Lim Prob(Intrusion) = 100 %
ressources → *infinite*

Why So Little Safety ?

Heterogeneous, complex security solutions

Technical bias

Ephemeral reactive security

Difficult tradeoff between usability and security

Best-effort philosophy



Solutions

Systemic and holistic security

Behavioral security

Insurance

Full disclosure



Conclusion

- ❑ Novelty and complexity of information risk
- ❑ Best practice risk management approach
- ❑ Challenge for policymakers
- ❑ Clean, “drinkable” upstream Internet

