Det elektroniska samhället som en arena för internationell brottslighet

Jaak Akker

Varför?

- ”Där det finns pengar finns det brott.”

  Leif G.W.Persson

Internationell

- Internationell = mellan flera nationer
- Internet känner inga nationsgränser

Det vi alla vet

- Spamming
- Phishing – spam som utger sig för att vara från penningsinstitutioner (banker, kreditkortsföretag etc.)
- Trojaner som stjäl login till banker, certifikat
- Hacking med kreditkortsnummerstölder ”spear phishing”
- Handel med stulna kreditkortsnummer (även manuellt stulna)

Den småttiga kriminaliteten

- PWSteal.Ragnarok
  - Trojansk häst som stjäl information om onlinespel
- vissa Onlinespel innehåller symboler värda pengar

Industrispionage

- Israeler som planterade in trojaner riktade mot ett visst företag arresterades efter tillslag av UKs National High Tech Crime Unit

"It is hard to say what forms the organised crime will take in the future, but the reality is not very far from some science fiction movies."

- http://www.jolt.unc.edu/Vol4_I1/Web/Brenner-V4I1.htm
- **North Carolina Journal of Law & Technology (2002)**
- Även brottslighet är numera nätverk i stället för hierarkiska gäng (jmfr. Handeln med rånplaner i Sverige)
- På Internet kan identifieras
  - Kodare – skriver program i kriminellt syfte
  - Eventuellt förmedlare, handlar med kriminella program
  - Brottslingar som utför brottet

Vad är ett program i kriminellt syfte?

- Syfte: lösenords/id-stölder, dDoS, spam
- Teknik: kriminalprogram är ofta små system med flera komponenter
  - Lokalt
  - På Internetsiter
- Möjliggör:
  - Lätt att infektera med små filer
  - Lätt att uppgradera till andra syften

Ett typexempel: Bots

- Om ett företag har 100% av sin omsättning via Internetsidor, hur stor del är då sårbar för attacker via Internet?
- Pokerföretag, Pay-Pal (betalningsförmedling), onlinespel

Spybot

- Attackerar via sårbarheten MS05-39, publicerad 9. Augusti 2005
- Ca 400 varianter en månad senare
- Syfte: bakdörr till datorn samt kan styras för att utföra dDoS (stänger av brandvägg) eller sända spam

Affärsnytta

- Utpressningsbrev sänds till offret
- Om de inte betalar startas en dDoS med hjälp av 10.000-tals datorer

Förslag till vidare läsning http://staff.washington.edu/dittrich/misc/ddos/

- Innehåller ”allt” teknik, historia, motmedel, juridik
- (obs! Mycket historiska data, läs gärna om Stacheldracht, ett av de första dDoS-verktygen, mycket gulligt)