The Economic Threat Landscape from Cyber Criminals

Guest Lecture, HiG
Sofie Nystrøm
31. May 2013
By 2020 global Internet users will nearly double
Internet traffic from 2011 increased by 4x.

Connected devices became ubiquitous by 2020.

75% of data under 3rd Party Control by 2020.

40+ countries are developing cyber security policy.

* Source: Microsoft
Global Risks

Where is the legislation heading? – EU and US perspective

Conclusion: Focus from government on cyber security issues globally has increased.
Economic Threat
Cocktail of ”The bleeding edge” and ”simple” attacks
Targeted attacks – long-term

- States and organized criminals invest large amounts of resources to harvest information
- Often targets entities with contracts, sensitive stock information, key personnel, executive employees
- Monitors and lurch around for years to find the data they are looking for

- "Advanced Persistent Threat"
Evolution Internet banking Trojans 2006 - 2011

- Customer’s PC infected by trojans
- Easier for fraudsters to target and exploit end-point than a banks infrastructure and servers
- Electronic fraud (eFraud) is on the rise
- Sophisticated and complex code
DNB targeted by DDoS attack

Norges største bank er utsatt for et tjenestetangrep. Bildet viser bankens hovedkvarter på Aker brygge i Oslo.

DNB under angrep

Distribuert tjenestetang (DDoS) skaper fortsatt problemer for kundene.

Mandag 7. mai 2012 kl. 11:40
Av Eirik Roaæen
Kripos har pågrepet to norske hackere

Kripos har pågrepet og siktet to gutter i slutten av tenårene for omfattende datahacking mot norske og utenlandske virksomheter.
Infection Vector
What WEB sides have infected Norwegian users
Norske nettsteder sprer skadevare

Stadig flere norske nettsider smitter sine besøkende med ondsinnet programvare. Det melder Norcert.

SMITTEFARE: Marie Moe i Norcert har fått økt tilfølge av varsler om infiserte, norske nettsider siste tiden. (Foto: Leif Martin Kirknes)
Trojan infrastructure overview

- Trojan Command & Control panel
- eFraud admin panel
-uples transaction
- Several proxy jumps
- Trojan C&C
- Victim PC
- Trojan C&C
- Hacker PC
Challenges for our customers

- Malvertizing – advertising that contains malware

- Awareness around measures such as habits of surfing is NOT a countermeasure anymore

- Depending on swift maintenance of the endpoint of the customer
Future

- Super "trojan"/malware - Advanced Persistent Threat (APT)
- DDoS will continue to flourish and try to jam our important infrastructure
- eFraud continues to escalate towards all groups of customers
Future

- More research and innovation around long-term cyber security problems
- Recruitment of talented security experts will continue to be scarce
- Grow public private partnerships further
- Continue close collaboration with law enforcement
- Establish mechanisms for efficient incident handling of serious attacks towards all banks in Norway
Lager A-lag mot kyberkrim

Finansnæringen oppretter eget FinansCERT.

Fredag 12. april 2013 kl. 07:27
Av Norsk Telegrambyrå

Oslo (NTB-Dag Kjarholt): Finansnæringen bretrer opp ertene og ru eller seg til kamp mot datakriminalitet.

FinansCERT skal først og fremst bidra til å verne finansnæringens IT-tjenester. Det skal søke å samarbeide med NoyCERT.
Establishing a Computer Emergency Response Team (CERT)

Security incident handling, early warning og information sharing

- In Norway the following CERT’s are established:
  - NorCERT (National CERT for critical national infrastructure)
  - Helse CSIRT
  - Justis CSIRT
  - Telenor CERT
  - Uninett CERT

- And now for bank and finance
Challenges in incident handling

- Code more advanced as we go along and analysis is extensive
- Strict control mechanisms from the criminals to avoid being detected
- Experience more "bleeding edge" attacks where nobody has previously seen code and methods
- Tools to handle new threat situations are quickly outdated
- Lack of knowledge at our vendors
- Large volume of customers that call their bank and alarms
So what is this all about?
Strategic Security Foundation

- "Security as a business enabler"
- Incident response team and counter threat 24 x 7
- Old days – eliminate vulnerabilities and monitor the "fence"/perimeter
- Today – eliminate vulnerabilities, monitor as much as possible and find abnormal traffic or behavior

Our strategic starting point: you are compromised
Summary

- Volume of data, number of Internet users and cyber security attacks grow hand in hand

- Attention on the economic threat is here

- ...but we do not have the countermeasure we need clearly in mind

- More public knowledge, attention, funding, education and research is paramount