Virus och skadlig kod

Nätverkssäkerhet 1DV425

Marcus Wilhelmsson

Läsanvisningar

- Kapitel 4 - Malicious Software

Typer av skadlig kod

- Insiderattacker
- Virus
- Elak kod
- Adware/spyware
- Skydd

Insiderattacker

- Bakdörrar
- Logiska bomber

Historia - virus

- Andra halvan av 1980-talet
- De flesta virus har aldrig haft någon egentlig spridning
- Trojaner för fjärrstyrning
- Maskar

Är det verkligen farligt?

- Massmedia?
- Okunnighet

Varför ska jag skydda mig?

- Ditt eget skydd
- Andras skydd
- Övertagande av dator

Hur skyddar man sig?

- Antivirus
- Personlig brandvägg
- Sunt förnuft

Mer än säkerhetsprogram?

- Uppdateringar
- Att vara kritisk mot källan

Vilka skador kan ske?

- Fjärrstyrning
- Från hemmet till arbetet via VPN
- Keylogger
- Antivirus och brandväggar slås ut

Virusskydd

- Virusskydd bör finnas med i säkerhetspolicyn
- Utvärdering?

Virustyper

- Parasitvirus
- Minnesresistenta virus
- Bootsector-virus
- Stealth-virus
- Polymorfiskt virus
- Alla ovanstående kan kombineras

Makrovirus

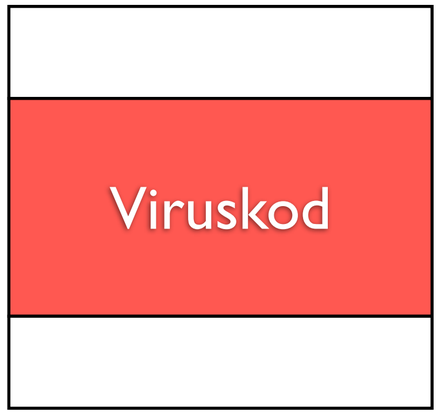
- Plattformsoberoende
- Infekterar dokument
- Sprids lätt

E-postvirus

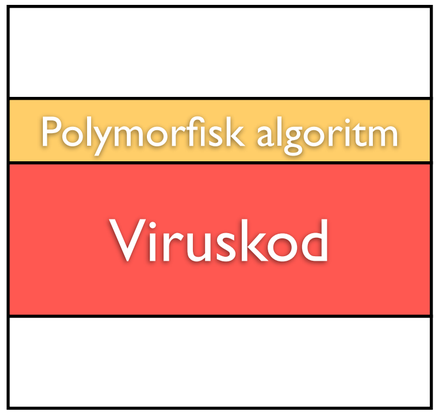
- Använder ofta svagheter i makrosystem
- Skickar en kopia av sig själv till alla i adressboken

Polymorfa virus

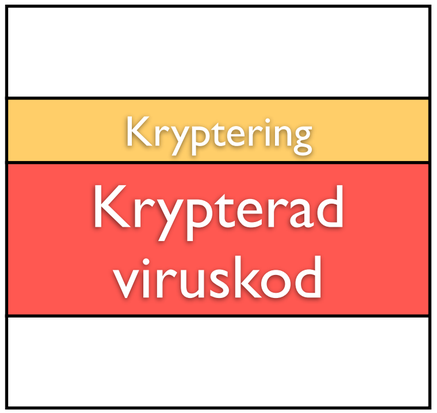
1a gen

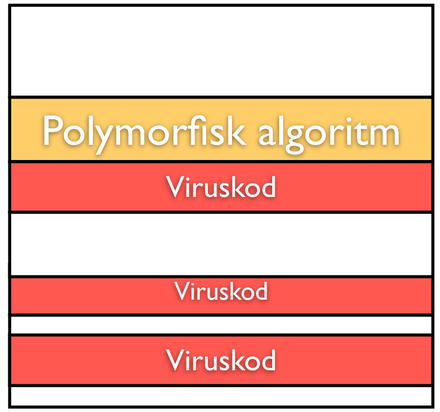


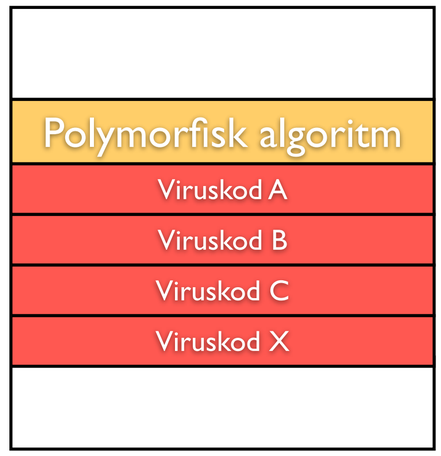
2a gen



3e gen







Patchning

- Säkerhetspatch
- Varför är det viktigt med en bra dialog mellan utvecklare och användare när säkerhetspatcher släpps?
- Varför är det otillräckligt att bara täppa till hål efter att de upptäckts?

Antivirusprogram

- Programvara
- Signaturscanning
- Virussignatur
- Polymorfa virus
- Heuristisk scanning
- Realtidsscanning

Borttagning

- Virus - förhållandevis lätta att ta bort
- Låsta filer
- Gömda processer

Malware

- Trojanska hästar
- Maskar
- Rootkits
- Botnät

Adware/spyware

- Hur fungerar de?
- Keylogger
- Skärmdumpar
- Datainsamling