

Kapittel 2:

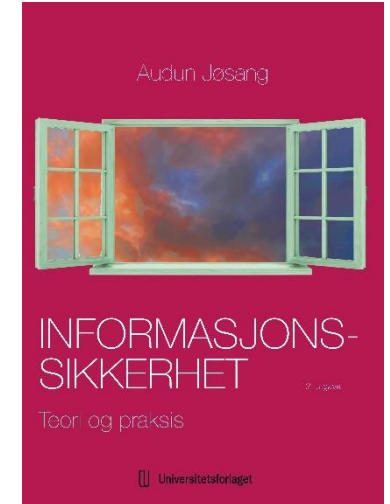
Angrepsvektorer og skadevare

Informasjonssikkerhet: Teori og praksis

Audun Jøsang

2. utg. 2023

Universitetsforlaget



Oversikt

- Angrepsvektorer
- Skadevare

Angrepsvektorer

Ulovlig sporing og avlytting, f.eks. av mobiltelefoner, og ulovlig kartlegging av brukere gjennom apper og nettsteder.



12



Phishing-e-post, -SMS og -meldinger med skadevare og lenker til skadelige nettsider.



2

11 Overlastangrep mot nettsteder slik at legitim trafikk blokkeres.



1

Drive-by-angrep fra kriminelle eller infiserte nettsider.

Innsideangrep fra utro tjenere i virksomheten.



10

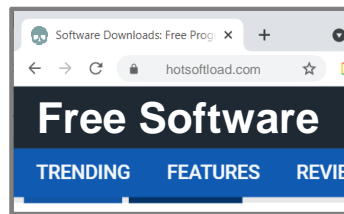


3



Falske nettsider som stjeler bruker-ID og passord.

Skadelige programmer fra internett og andre lagringsmedier.



9



4

Deepfake lyd og video for å spooft identitet i online møter og samtaler.

8 Hacking av upatchede sårbare IoT-enheter.



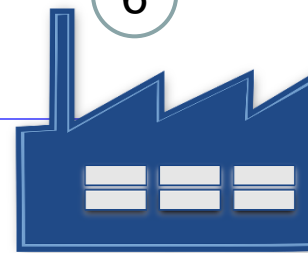
7

Skadelige eksterne enheter.



6

Infisering og angrep gjennom leveransejeden.



5



Direkte angrep mot sårbare systemer og applikasjoner.

Phishing-angrep



- *Phishing* er en type sosial manipulering.
- Kan sendes som e-post, SMS eller andre meldinger.
- En phishing-e-post er f.eks. designet for å lure mottageren til å oppgi sensitiv informasjon, til å besøke en falsk nettside eller til å installere skadevare.
- Fra omtrent år 2020 er phishing den desidert vanligste angrepsvektoren for cyberangrep og datakriminalitet på internett.
- Sikkerhetskultur, kunnskap og bevissthet rundt phishing er viktig for å forhindre denne typen angrep.

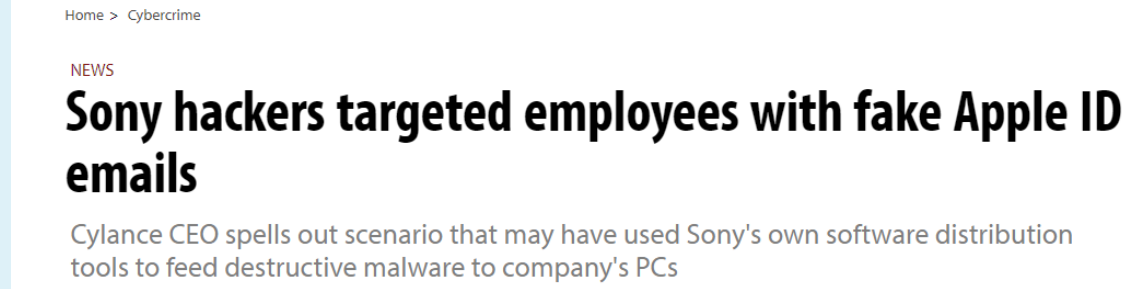
Phishingeksempler



PHISHING-KAMPANJE – ET EKSEMPEL FRA FORSKNINGS- OG UTDANNINGSSEKTOREN

Forsknings- og utdanningssektoren har gjennom 2020 vært mål for en avansert, utenlandsk aktør. Angrepene bruker e-post og falske nettsider tilpasset den enkelte virksomhet, og har som mål å «høste» brukernavn og passord som gir tilgang til interne ressurser. Aktøren retter seg mot universiteter og forskningsmiljø i flere vestlige land, og samarbeid mellom sikkerhetsmiljø på tvers av landegrensene har vært avgjørende for å forstå framgangsmåten i Norge. Som sektorens responsmiljø, har Uninett CERT jobbet tett med sektoren og internasjonale samarbeidspartnere for å oppdage, forhindre og ikke minst bedre forstå kampanjene. Dette har gjort det mulig å flere ganger sette i gang forebyggende tiltak før angrepene kommer.

[Kilde: NSMs «Helhetlig digitalt risikobilde 2020»]



skadevare

Kategorier av phishing-angrep

- *Masse-phishing*
 - Stort volum som er ment å nå flest mulig
- *Spyd-phishing*
 - Målrettet mot bestemte personer eller virksomheter
- *Direktørsvindel (hval-phishing)*
 - Spyd-phishing rettet mot «store fisker» (f.eks. rike, høyprofilerte, tilgang til mye penger,...)
- *Klone-phishing*
 - Kopi av legitim melding/epost hvor lenker/vedlegg er erstattet av skadelige versjoner

Andre former for sosial manipulering

- Spør pent
 - Folk er generelt hjelpsomme og gir fra seg mye informasjon
- Lur folk til å gi deg tilgang
 - «Hi, I`m calling from Microsoft»
 - Få tak i «hemmeligheter» til å resette glemte passord
- Falske adgangskort
 - Gir en følelse av fellesskap – «du og jeg har noe felles, og derfor stoler jeg på deg»
- Bruk av stjalne/falske kontoer på sosiale nettverk
 - Du tror du får melding fra en venn, men egentlig er det en angriper som har stjålet din venns identitet
 - Hvis det skjer, kontakt din venn gjennom annen «sikker» kanal, f.eks. vanlig telefon



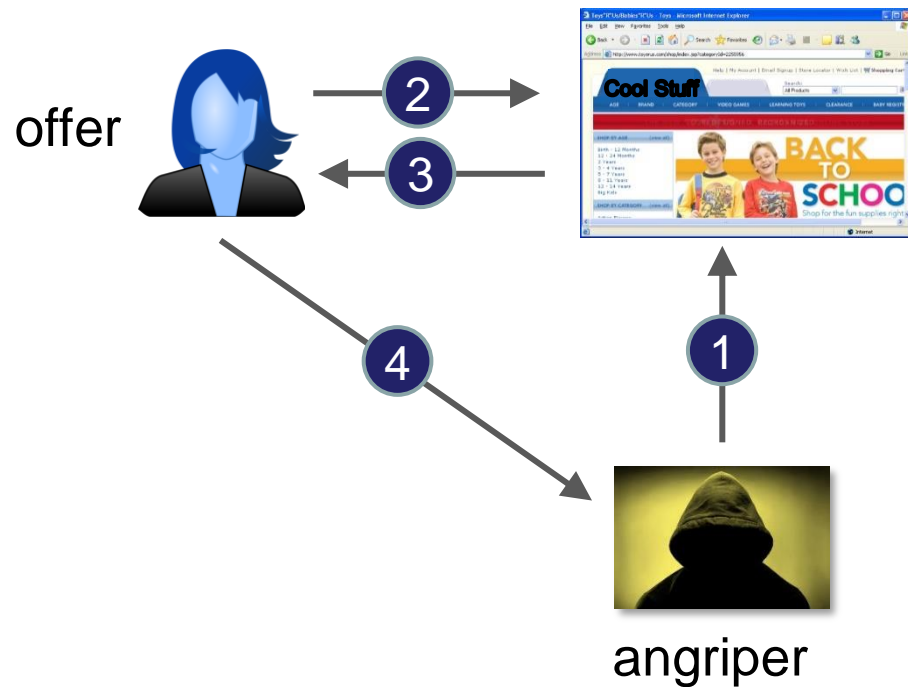
Drive-by-angrep



- Mange ulike scenarier for drive-by-angrep.
- Generelt skjer drive-by-angrep uten at brukeren trenger å klikke på noe, eksplisitt laste ned noe eller åpne noe vedlegg for at klienten skal bli infisert. Brukeren trenger bare å besøke nettsiden for å bli angrepet.
- Kan være en vanlig nettside infisert av trusselaktør, eller en falsk nettside kontrollert av trusselaktør.
- Mulige scenarier er:
 - Direkte nedlasting av skadelige JavaScript
 - Videre sending til falsk nettside

Drive-by-angrep - eksempelscenario

XSS (Cross Site Scripting) er et angrep hvor et ondsinnet skript er injisert i en nettside (som ellers er godartet).

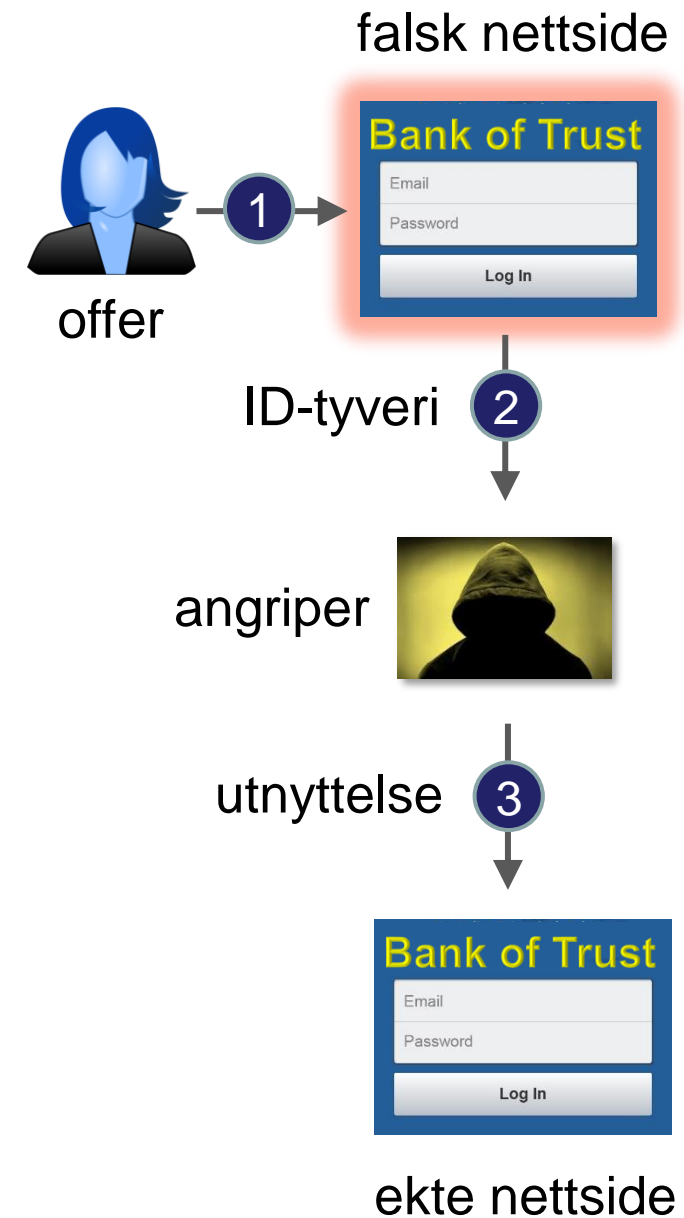


Scenario med direkte nedlasting av skadelig JavaScript, f.eks. som følge av en XSS-sårbarhet på en nettside.

1. Angriper injiserer skadelig skript
2. Offer besøker nettsiden
3. Skadeskript sendes til nettleser
4. Nettleser stjeler og sender sensitive data til angriper

Falske nettsider

- *Falske nettsider* kan være nesten umulig å skille fra ekte nettsider.
- Brukere kan bli villedet til å besøke en falsk nettside f.eks. gjennom phishing-e-post, gjennom andre falske eller infiserte nettsider eller gjennom skadereklame.
- En bruker som har havnet på en falsk nettside kan bli lurt til å oppgi bruker-ID og passord eller annen sensitiv informasjon.
- Angriperen kan så bruke stjålet bruker-ID til å besøke den ekte nettsiden og logge seg inn som brukeren.
- Måter å unngå falske nettsider er å ikke klikke på lenker i meldinger, eller å sjekke nøye nettsidens URL og sertifikat.



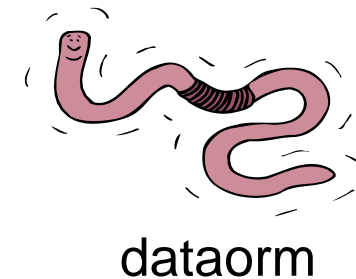
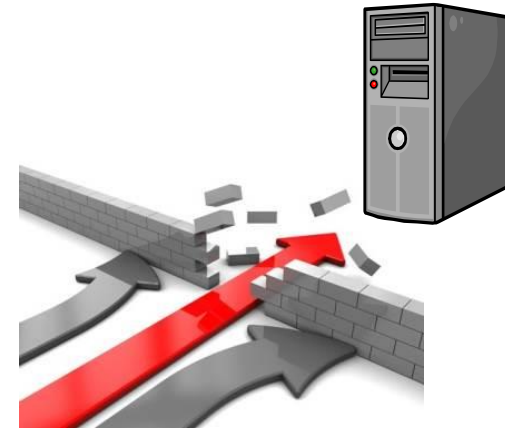
Deepfake



- Verktøy basert på maskinlæring gjør det mulig for en angriper å snakke på en måte som høres ut som deg, eller opptre i et videomøte med ansikt og stemme som deg.
- Deepfake refererer til at falsk lyd og bilde genereres av teknologi basert på dype nevraltnettverk (DNN).
- En angriper kan f.eks. spoofe identiteten til virksomhetens direktør under et online-møte, og gi en ansatt med høye autorisasjoner instruks om å overføre en stor pengesum til en konto kontrollert av angriperen.
- Alternativt kan angriperen spoofe identiteten til en ansatt i en bedrift under et videomøte, og sende en chattemelding med en link til en skadelig nettside. Fordi kollegaer kjenner og stoler på den ansatte, vil de typisk klikke på lenken.
- Deepfake kan også brukes til å forfalske biometri.

Direkte nettverksangrep

- Typiske angrep mot sårbare web-applikasjoner er f.eks. SQL-injeksjon og XSS (Cross-Site Scripting).
- Svake passord kan crackes med passordspraying, som betyr å automatisk forsøke typiske passord mot mange ulike brukerkontoer.
- *Automatisk spredning av skadevare* kan skje f.eks. gjennom en dataorm som automatisk sprer seg til andre computere gjennom datanett og internett.
- En dataorm utnytter ukjente eller upatchede sårbarheter for å infisere en computer, og bruker denne som vert for å skanne og infisere andre computere. Dette utløser en kjedereaksjon som kan gi eksponentiell spredning på kort tid.
- Foruten å beslaglegge betydelig båndbredde gjennom spredningen, kan dataormer ha alvorlige tilsiktede skadevirkninger.

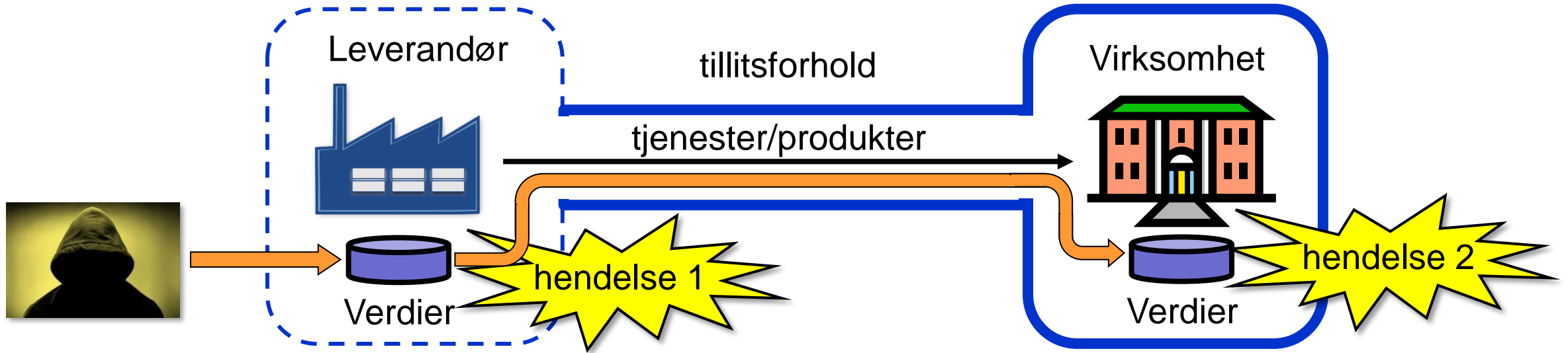


Leveransekjedeangrep



- *Leveransekjedeangrep* betyr at angripere kan infiltrere systemer og nettverk gjennom en ekstern partner eller leverandør som har tilgang eller leverer komponenter med tilgang til systemer og data.
- Fra et sikkerhetsperspektiv representerer leveransekjedene en del av angrepsflaten.
- Avhengigheten av lange og komplekse leveransekjeder har ført til en dramatisk forstørrelse av angrepsflaten til virksomheter i de senere år.
- Enhver entitet som bidrar i en leveransekjede, har mulighet til å påvirke sikkerheten lenger opp i leveransekjeden.
- Jo lenger og mer kompleks leveransekjeden er, desto vanskeligere er det å få oversikt over trusler og sårbarheter, og desto vanskeligere er det å håndtere sikkerhetshendelser.

Illustrasjon av leveransekjedeangrep



- Virksomheter har ofte relativt god sikkerhet, mens leverandører kan ha relativt dårlig sikkerhet
- Angriper velger det svakeste led i kjeden
- Leveransekjedeangrep skjer flere trinn
 1. Leverandør blir angrepet for å kompromittere produkter eller tjenester
 2. Virksomheter som bruker kompromittert produkt/tjeneste fra leverandør blir sårbare
 3. Sårbare virksomheter blir angrepet

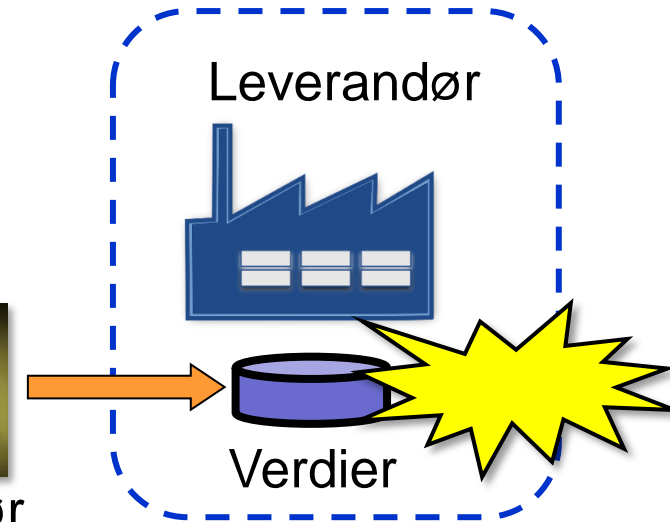
Trusselaktørens angrepsmål hos leverandør

Trusselaktører vil typisk angrepe:

- Programvare utviklet av leverandøren
- Konfigurasjoner
 - f.eks. passord, API-nøkler, brannmurregler, URL-er
- Data
 - f.eks. konfidensiell informasjon, kryptografiske nøkler, sertifikater, CRM-data, personopplysninger om leverandørpersonale eller kundeansatte
- Prosesser
 - f.eks. oppdateringsprosesser, backup-prosesser, digitale signaturprosesser
- Maskinvare produsert av leverandøren
- Personer med privilegert tilgang til data og infrastruktur



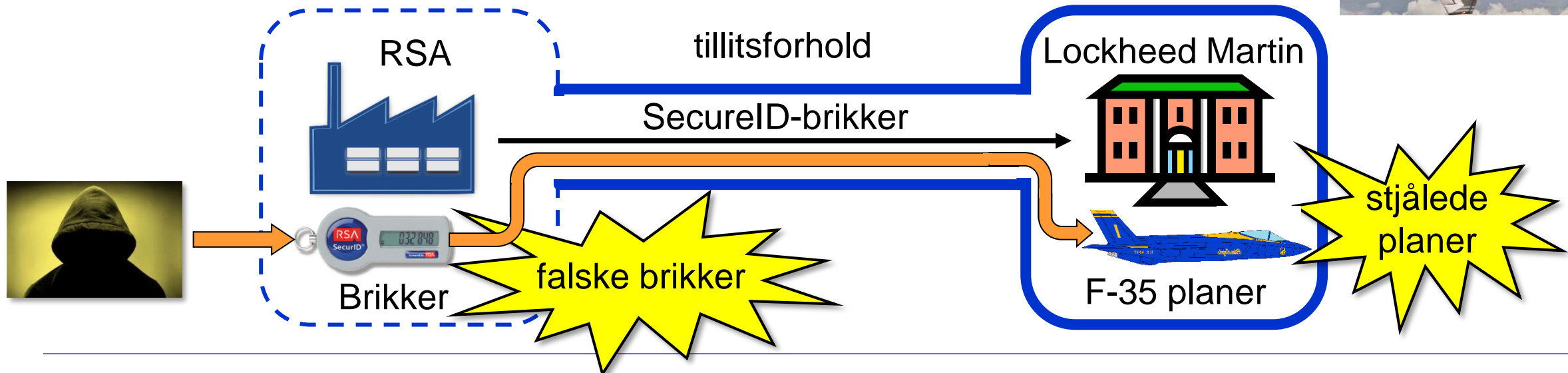
Trusselaktør



Falske SecureID-brikker for spoofet innlogging

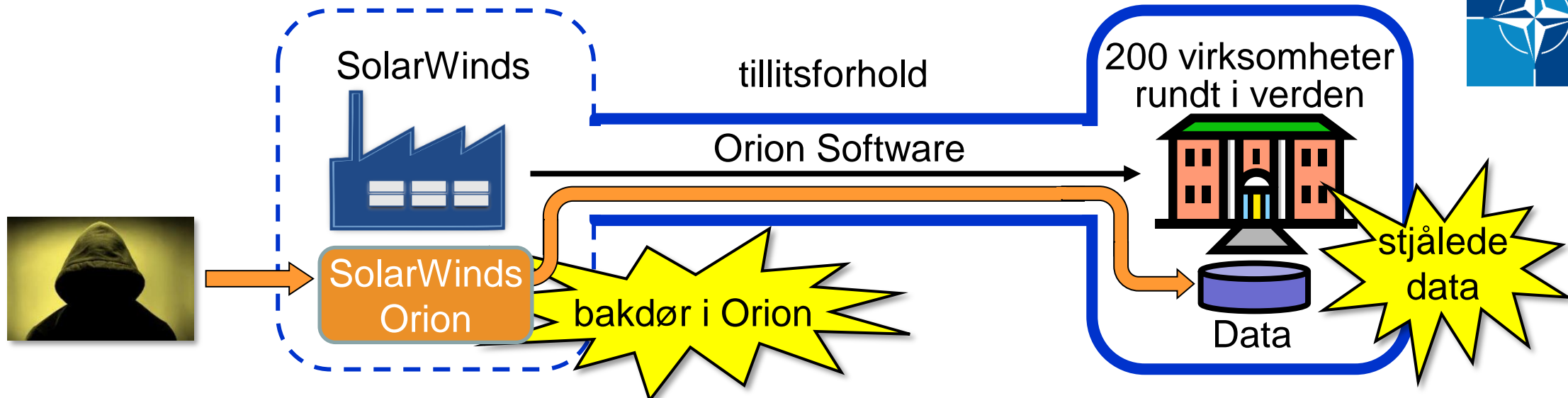


- RSA ble hacket i 2007, mistet sensitive data for SecureID-brikker
- Hackere laget falske SecureID-brikker for å spoofe 2FA innlogging
- Selskaper som brukte 2FA med SecureID var sårbare
- Lockheed Martin brukte SecureID for 2FA (2-Faktor Autentisering)
- Kinesiske angripere spoofet Lockheed Martin-ansatte
- Stjal planer for F-35 jagerfly



Manipulert SolarWinds Orion programvare

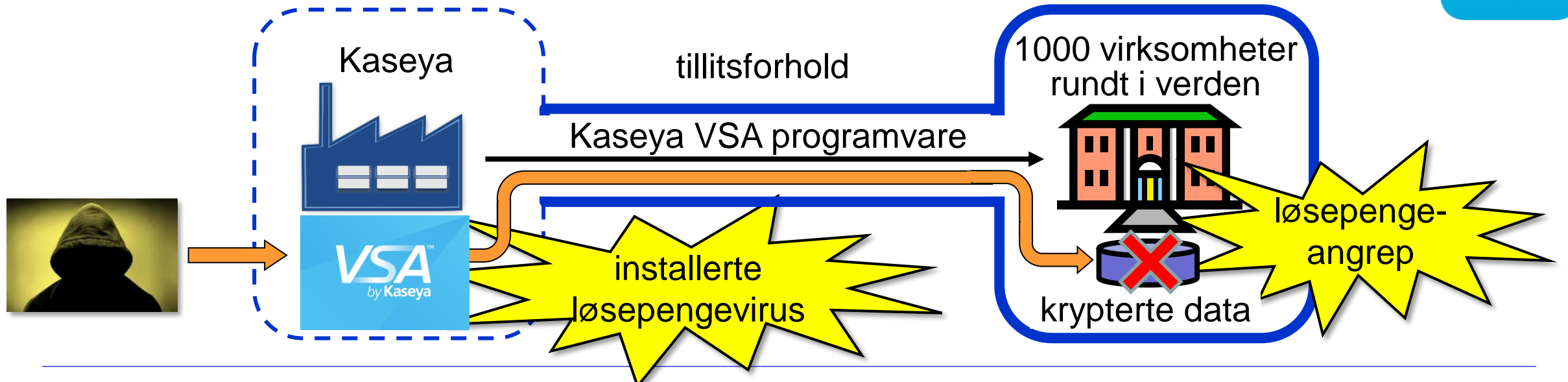
- SolarWinds ble hacket i 2020
- Hackere installerte bakdør i Orion programvare for nettverksadministrasjon
- Tusenvis av virksomheter rundt i verden bruker Orion-programvaren, og var sårbare
- 18000 virksomheter som brukte SolarWinds Orion programvare var sårbare
- Minst 200 virksomheter over hele verden ble utsatt for angrep, inkludert NATO
- Angrepet er antatt å komme fra russisk APT-gruppe



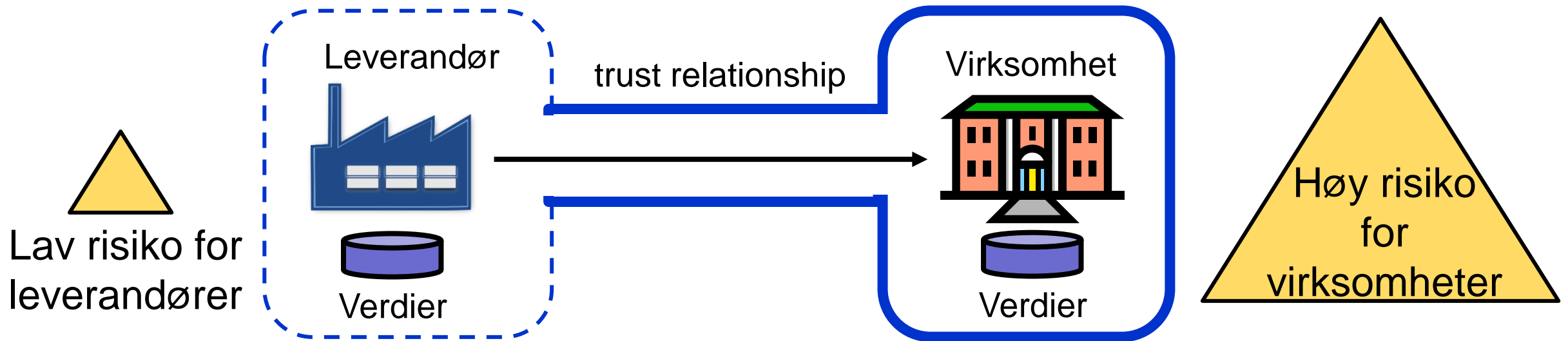
Manipulert Kaseya VSA programvare



- Autentiseringssårbarhet i Kaseya VSA (Virtual System Administrator) programvare
- Hackere installerte løsepengevirus i Kaseya VSA-programvaren
- Tusenvis av organisasjoner over hele verden bruker Kaseya VSA
- Minst 1000 selskaper over hele verden ble ofre for løsepengeangrep, inkl. coop
- Coop Sverige måtte stenge 800 butikker i 1 uke
- Tilskrevet den russiske REvil APT-gruppen



Markedssvikt for risikostyring av leveransekjeder



- Leverandører kan ha lav risiko og dermed lite insentiv til å implementere sterke (og dyre) sikkerhetstiltak
- Virksomheter kan ha høy risiko, men få muligheter til å implementere effektive sikkerhetstiltak mot sårbarheter i leveransekjeden

Skadelige eksterne enheter

skadevare



- *Skadelige eksterne enheter* kan f.eks. kobles til USB-kontakten og brukes i angrep.
 - Enheten kan f.eks. inneholde skadevare som brukeren kanskje installerer av nysgjerrighet.
 - En USB-minnepinne konfigureres som en HID-enhet (Human Interface Device), som lurer computeren til å tro at den er et tastatur og sender en strøm av tastetrykk som utgjør skadelige kommandoer.
 - USB-ladekontakter på offentlige steder kan ha blitt manipulert til å sende skadelige kommandoer til enheter.
 - Et *drop-angrep* er når angriperen legger igjen skadelige USB-minnepinner f.eks. på kafeer, og venter på at noen finner dem og plugges dem inn i en computer.

Stuxnet

- Dataorm/rootkit
Flere nulldagssårbarheter
- Angrep en av Irans atomreaktorer i 2010
- Krysset «air-gap» gjennom overføring over USB
- USA og Israel (trolig) bak

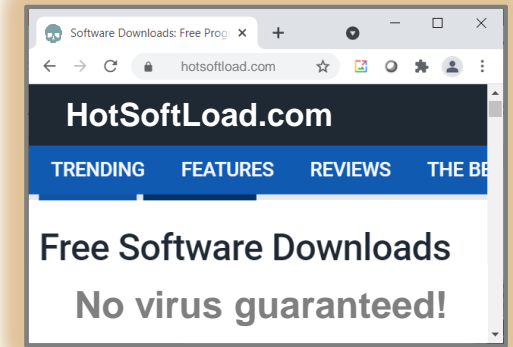
Uvitende innstallering av skadevare

- Å lure brukere til å installere skadelige programmer gjennom nettsteder eller andre lagringsmedier kan brukes som del av angrep.
- Brukeren kan bli lurt til å installere skadevare i den tro at programvaren er legitim.
- Det fins en rekke ulike typer skadevare
- Trojaner (trojansk hest) er en type skadevare som faktisk har en nyttig funksjon, men som samtidig har skjulte skadelige funksjoner.
- Unngå skadevare ved å kun laste ned fra anerkjente nettsteder, og sjekke digital signatur.

nettside med skadevare



angriper



Installerer skadevare uten å vite det



offer



Innsideangrep fra utro tjener



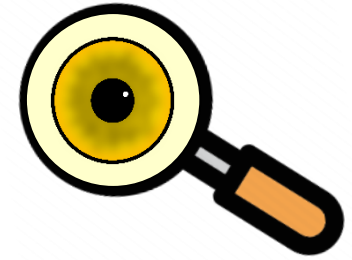
- Innsideangrep er angrep som begås av en ansatt eller annen person som er autorisert for tilgang til virksomhetens systemer og data.
- Begrepet *utro tjener* benyttes typisk om slike personer.
- Innsideangrep kan være svært skadelige fordi angriperen har kjennskap og tilgangsrettigheter til systemer og verdier slik at typiske sikkerhetstiltak har begrenset nytte.
- I tillegg kan innsideangrep være svært vanskelig å oppdage fordi angriperen ofte vet hvordan spor kan skjules.

DDoS – overlastangrep - tjenestenektangrep



- Et DDoS-angrep betyr at et nettsted blir bombardert med falsk trafikk som gjør at web-tjeneren blir overbelastet og ikke lenger kan betjene legitim trafikk.
- DDoS-trafikk genereres typisk med botnett som kan bestå av flere millioner infiserte computere som kan fjernstyres av en trusselaktør kalt *bottgjeter*.
- Det kan være vanskelig og ressurskrevende å stoppe DDoS-trafikk.
- Se presentasjon om nettverkssikkerhet for mer info om DDoS.

Ulovlig sporing og avlytting



- Det fins mange former for sporing og avlytting
 - Mobiltelefoner kan spores med IMSI-fangere, se presentasjon fra kapittel 7 om sikkerhet i trådløse nett.
 - Nettsteder og apper kan benyttes til å spore og kartlegge brukere, noe som kan være lovlig eller ulovlig (f.eks. i henhold til GDPR), avhengig av hvordan det gjøres og hvordan brukere informeres. Se presentasjon fra kapittel 10 om personvern.
 - TEMPEST er et samlebegrep for alle typer elektronisk overvåking, og tiltak mot dette. Se presentasjonen fra kapittel 3, spesifikt om sidekanaler og skjulte kanaler. For eksempel kan refleksjon av laserlys mot et vindu benyttes for å avlytte samtaler i rommet bak vinduet. Dette er mulig fordi lydbølgene får glasst til å vibrere, som kan detekteres med det reflekterte laserlyset.

Skadevare

- Datavirus



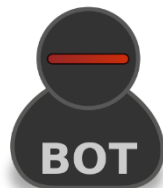
- Løsepengevirus



- Spionvare



- Bott-program



- Exploit



- Makro-virus



Office



- Trojaner



- Dataorm



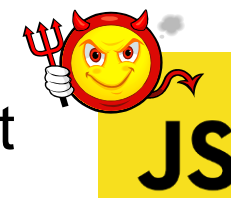
- Rootkit



- Bakdør



- Skadelig JavaScript



- Logisk bombe



Datavirus



- En datavirus infiserer andre programmer ved at skadelig kode legges til og flettes inn i et annet program.
- Viruset utføres bare når det infiserte programmet kjøres.
- At et virus er flettet inn i et annet program gjør det spesielt vanskelig å fjerne, og selv de beste antivirusprogrammene sliter med å gjøre dette riktig.
- Rene datavirus er uvanlige i dag, og utgjør mindre enn 10 % av all skadevare.
- Vær oppmerksom på at begrepet «virus» ofte brukes som et generelt navn på alle typer skadevare, noe som kan være forvirrende.

Trojaner



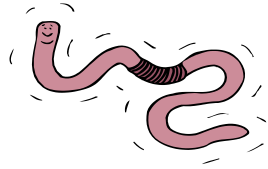
- Trojanere maskerer seg som legitime programmer som faktisk (eller tilsynelatende) har nyttige funksjoner, men som samtidig har skjulte skadelige funksjoner.
- Trojanere er populære blant hackere og har stort sett tatt over etter datavirus.
- Trojanere blir typisk lastet ned fra kriminelle eller infiserte nettsteder, eller kommer som et vedlegg til phishing-e-post.
- Brukeren blir lurt til å tro at programmet er nyttig, og velger eksplisitt å installere det.
- Det er ironisk at falske antivirusprogrammer er en utbredt type trojaner.

Løsepengevirus



- Løsepengevirus er en type skadevare som i første trinn krypterer alle, eller et utvalg, kritiske data på offerets computer, slik at data og applikasjoner blir utilgjengelige.
- Dette er en form for tjenestenektangrep som fører til brudd på *tilgjengelighet*.
- Angriperen følger opp første trinn med å foreta utpressing og kreve løsepenger for å utlevere dekrypteringsnøkkelen.
- Utpressing kan også baseres på en trussel om å offentliggjøre dataene hvis ikke løsepenger blir betalt. Dette kan være en trussel mot personvern.
- En viktig beredskap mot løsepengevirus er å ta regelmessige sikkerhetskopier (backup) av alle viktige data, og ha gode gjenopprettelsesrutiner.
- Løsepengevirus er ikke et datavirus i ordets opprinnelige forstand.

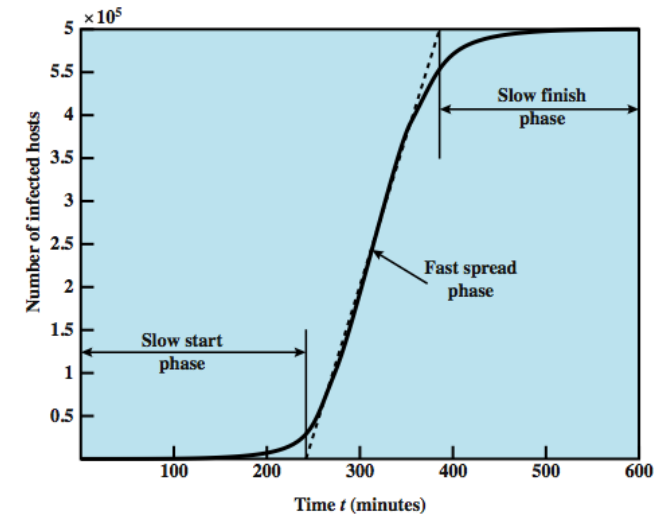
Dataorm



- Dataormer sprer seg selv til andre computere innen et datanett eller over hele internett på en automatisk måte, som regel uten brukerinteraksjon.
- Dataormer klarer dette ved at de kobler seg til andre vertsnoder og utnytter sårbarheter i programmer som er eksponert til internett.
- Kan være svært ødeleggende fordi de sprer seg uten brukerdeltagelse. Virus og trojanere krever i det minste at en bruker starter et program.

Eksempler på dataormer

- Morris-dataormen (1988) laget av en student kalt Robert Morris og er en av de første dataormene på internett
- Stuxnet
- Wannacry & NotPetya
- SQL Slammer-ormen
 - I januar 2003 infiserte ormen omkring 75 000 Microsoft SQL-tjenere på omtrent 10 minutter
 - viser dens eksponentielle spredningshastighet.



Spionvare



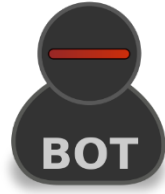
- Spionvare og reklamevare er programmer som spionerer på brukeren eller viser reklame til brukeren.
- En keylogger er en type spionvare som logger tastetrykk, slik at angriperen kan stjele passord og annen sensitiv informasjon.
- Slike programmer blir ofte installert gjennom en form for sosial manipulering kombinert med en av angrepsvektorene, og de starter som regel hver gang systemet starter.

Exploit / utnyttelseskode



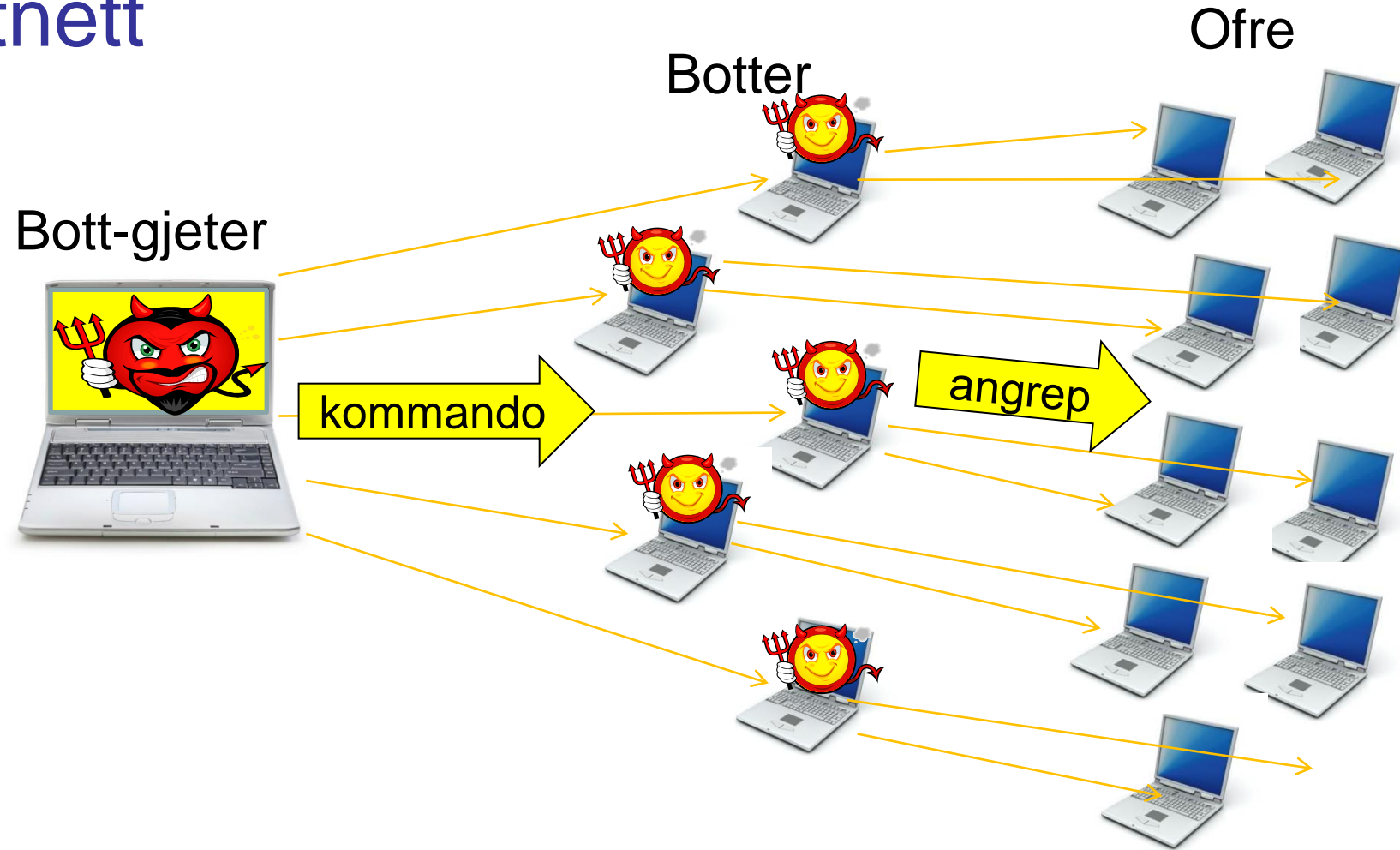
- Exploit, også kalt utnyttelseskode, er et lite program, en streng med data, en fil eller en sekvens med kommandoer som utnytter en eller flere feil eller sårbarheter i en programvare, maskinvare eller annet datautstyr for å trigge korrumpert eller unormal oppførsel.
- En exploit trigger ofte en buffer overflow (se kapitlet om systemsikkerhet)
- Angriperens hensikt med å trigge slik oppførsel kan for eksempel være å få kontroll over et system, laste ned bakdører, få uautorisert tilgang eller å utføre et tjenestenektangrep.

Bott-programvare



- En computer med bott-programvare kalles en bott (eng.: bot), fra «robot», altså noe som går automatisk.
- Bott-programvare kan brukes til legitime formål
 - f.eks. søkemotorer for å utføre indeksering.
 - Dessverre brukes bott-programvare ofte som skadevare av angripere.
- Bott-skadevare er typisk selvreplikerende, og er i stand til å motta kommandoer fra en sentralisert eller distribuert bott-gjeter. Angripere infiserer computere i stort antall for å lage et bottnett som kan utføre forskjellige typer angrep.
 - F.eks. DDoS-angrep eller utvinning av kryptovaluta med ofrenes elektrisitet og beregningsressurser.

Bottnett



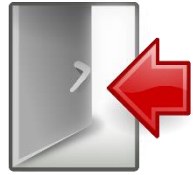
Mirai er (en dataorm som) er et eksempel på botnett, med fokus på IoT-enheter og DDoS-angrep.

Rootkit



- Rootkit er en type programvare som angriperen installerer for å skjule at angriperen, eller skadevaren er i systemet
 - Navnet kommer av «root»
- Typisk vil et rootkit endre prosesslisten for å skjule skadevaren
 - eller det skjuler bakdører
 - eller det skjuler falske brukere som er opprettet av angriperen

Bakdør



- En bakdør er en skjult metode for å omgå normal autentisering og tilgangskontroll i et system.
- Bakdører har legitime bruksområder, som å gi produsenten av systemer og programvare en måte å foreta vedlikehold og service på.
- En bakdør kan også brukes av angripere for å få uautorisert tilgang til systemer.
- En bakdør kan være en skjult del av et program, et eget program, kode i fastvaren til maskinvaren eller en del av operativsystemet.
- En skadebakdør kan f.eks. bli installert av en trojaner eller av et exploit.

Skadelig JavaScript



- De fleste nettsider inneholder JavaScript som automatisk lastes ned og kjører i nettleseren når en bruker besøker nettsiden.
- Vanligvis er JavaScript helt legitimt, og brukes til avanserte funksjoner på en nettside, men det kan også utføre skadelige funksjoner, f.eks. å laste ned et exploit fra et nettsted kontrollert av angriperen.
- JavaScript kan også misbrukes til å få nettleseren til å utvinne kryptovaluta for angriperen eller til å stjele sensitiv informasjon som sendes til angriperen.
- Skadelige JavaScript kan bli injisert i nettsider gjennom XSS-angrep.
- Ettersom JavaScript utføres automatisk og helt uten interaksjon når brukeren besøker en nettside, er JavaScript typisk brukt til drive-by-angrep.

Macro-virus



- Makroer brukes for å automatisere funksjoner i Office-dokumenter.
- Imidlertid kan angripere gjemme skadelige Office-makroer i Office-filer som f.eks. sendes som vedlegg til phishing-e-post.
- Disse filene har ofte navn som er ment å lokke eller skremme folk til å åpne dem, og ser typisk ut som fakturaer, kvitteringer, juridiske dokumenter osv.
- Tidligere kjørte Office-makroer automatisk, men ikke nå lenger. Nå må angriperen lure brukere til å aktivere makroer for at de skal kunne kjøre.

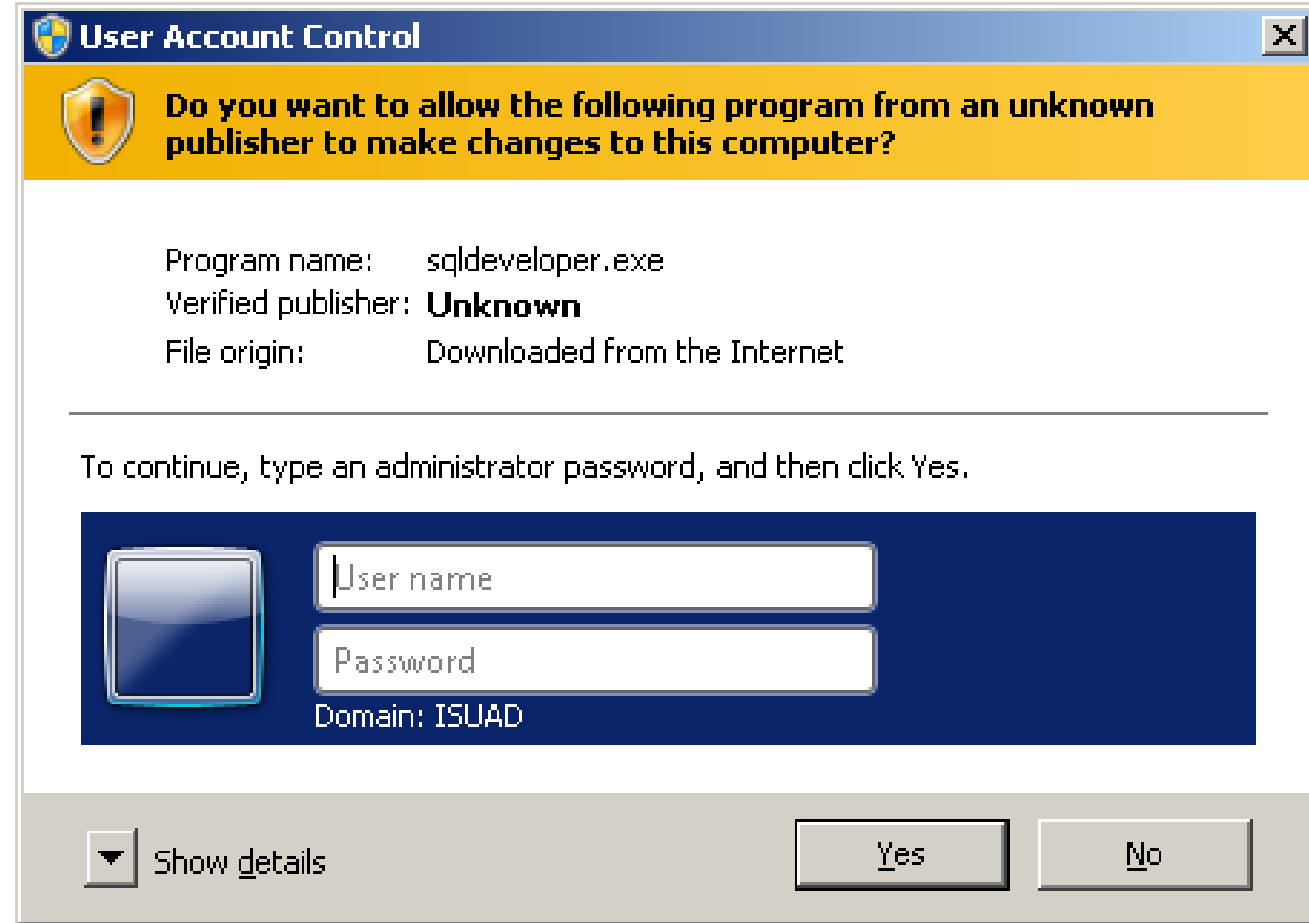
Logisk bombe



- Logiske bomber er en av de eldste typer skadevare
- Logiske bomber er kode innebygd i et legitimt program, eller et program som går i bakgrunnen.
- Skadelige funksjonalitet aktiveres når bestemte betingelser er oppfylt, f.eks.
 - tilstedeværelse/fravær av en fil
 - bestemt dato/klokkeslett
 - bestemt bruker
- Logiske bomber forårsaker skade når den utløses:
 - endre/slette filer/disker, stoppe maskinen osv.
- Logiske bomber lages typisk av en innsidetrussel

Hvilke tilgangsrettigheter har skadevaren?

- Exploits og annen skadevare får samme tilgang som bruker / tjeneste som angripes
 - Dvs: Kjører man skadevare som bruker, får skadevaren brukertilgang.
 - Kjører man skadevare som administrator, får skadevaren administratortilgang.
 - Derfor benyttes sikkerhetsmekanismer som UAC (User Account Control).



Slutt på presentasjonen

