(U)Sikkerhet og (u)kjente feil

UiBs IT-forum
17. april 2008

Per Arne Enstad og Morten Knutsen
UNINETT CERT

Introduksjon

- Hvem er vi og hva gjør vi?
- Hva observerer vi av uhumskheter?
- Trender
- Trusselbildet
- Et lite dykk ned i ”Drive-by infections”

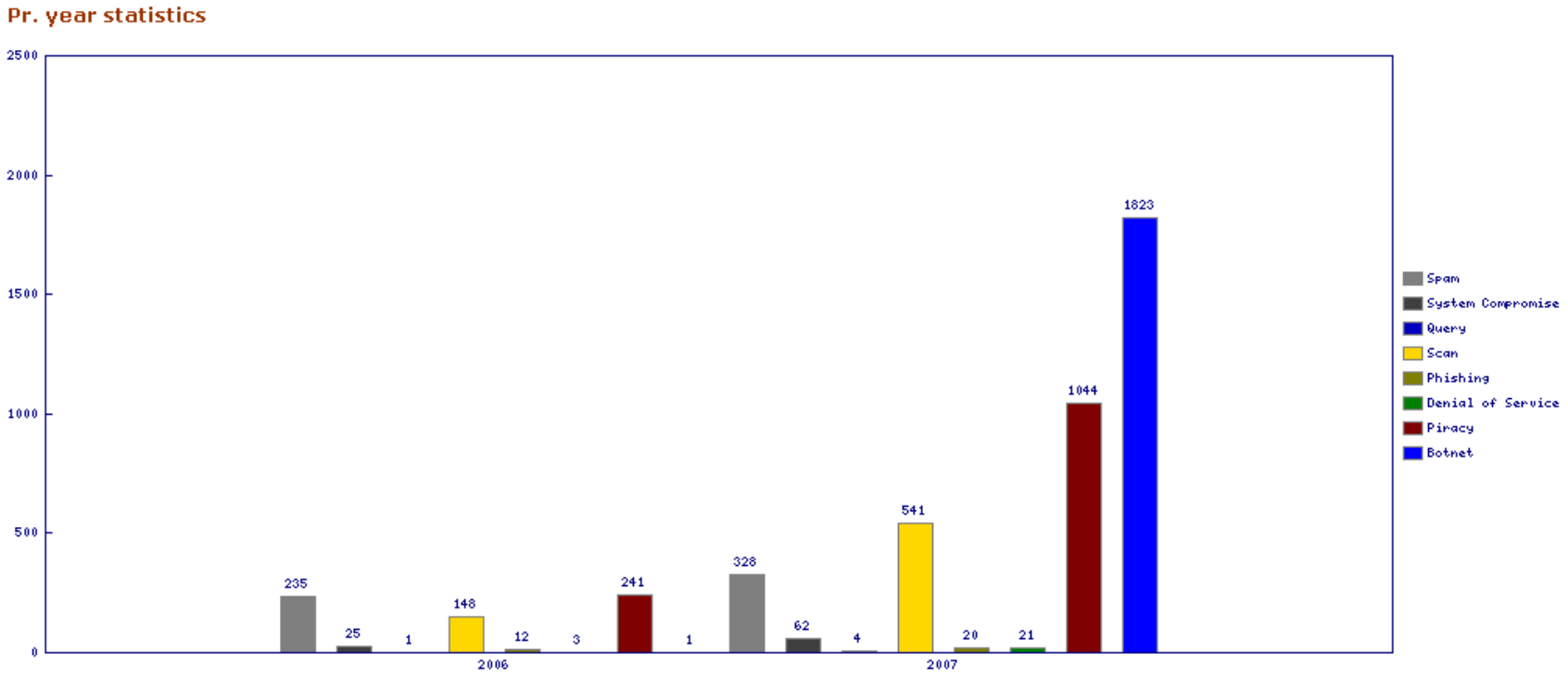
UNINETT

UNINETT CERT

- Etablert 1995
  - ”Core Team”: 4 personer fra sikkerhetsgruppen
- Tilbyr:
  - Fokuspunkt for håndtering av sikkerhetshendelser
  - Koordinering
  - Bistand
  - Restsikring
  - Rådgiving
- Har et stort internasjonalt kontaktnett til disposisjon
  - Samarbeid er essensielt i denne typen virksomhet!
- Håndterer årlig ca 5000 sikkerhetshendelser

UNINETT

Hvilken type hendelser observerer vi?



Hva er truslene mot våre IT-systemer i dag?

- Ikke helt liketil å komme med et entydig svar på dette ☹
- Avhengig av flere ting:
  - Type virksomhet
  - Sikkerhetskultur
    - Eller eventuelt mangel på sådan
  - Kvalitet på beredskap
    - Forebyggende virksomhet
    - Reaksjonsmønster når uhellet så likevel er ute
- Vi har imidlertid en brukbar oversikt over hva vi i *UH-sektoren* utsettes for av ulike uhumskheter →

UNINETT

Vår fortolkning av grafene

- Vi har et jevnt sig av ”tradisjonell” cracking, men aktiviteten viser en nedadgående tendens
- Portscanning av ulike slag er fortsatt populært
  - SSH bruteforce scanning
  - Ulike typer malware som forsøker å formere seg
  - ..og en sjelden gang et ærlig, manuelt NMAP-scan
- Antall klager på brudd på opphavsrett er svakt nedadgående
  - Men er dette egenlig et sikkerhetsproblem?
- Maskiner som sannsynligvis er rekruttert som botnet-klienter er bekymringsverdig høy

UNINETT

Trender

- Gammeldags, *manuell* cracking er ikke så vanlig lenger
- Vi merker en tydelig dreiing bort fra rampestreker (ønsker å bli lagt merke til) til mer sofistikerte typer aktiviteter hvor man *ikke* ønsker å bli lagt merke til
- Aktivitet som stammer fra malware er observerbar til alle døgnets tider

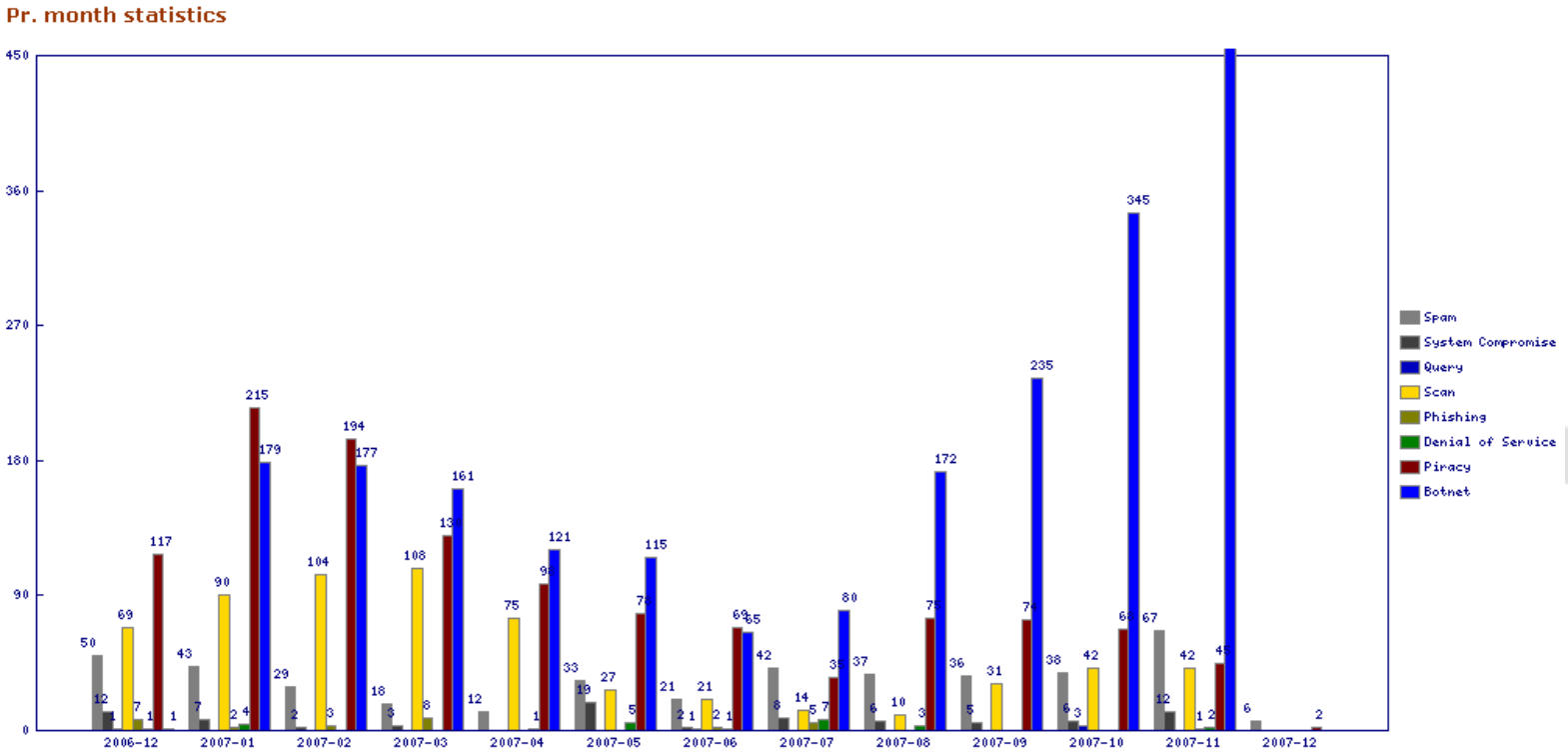
UNINETT

Trusselbildet - hovedtrekk

- Økning i økonomisk motivert ondsinnet aktivitet
  - Nettsvindel
    - ”Nigeria scam”
    - Ulike typer social engineering
  - Tjenestenekt-angrep
    - Betaltjeneste – lei et botnet
    - Vi har problemer med å detektere dem fordi:
      - De har blitt mer målrettet
      - For offeret er de imidlertid vel så destruktive som før
    - Angrepene er blitt vanskeligere å observere av alle som *ikke* er berørt
      - Vi har en kraftig infrastruktur som tåler en støyt
      - Pakkerate er tilpasset tiltenkt mål
  - Søppelpost i bøtter og spann

UNINETT

Hvilken type hendelser var det vi observerte nå igjen?



IMHO - største trussel i UH-land for øyeblikket er:

Botnets

- Vi som bor i UH-land er attraktive for bot-herdere fordi vi har:
  - Høy nettkapasitet
  - God konnektivitet
  - Mange potensielle zombier
  - Plenty lagringsplass

UNINETT

Botnets - bruksområder

- Pakkekanoner i tjenestenekt-angrep
- Masseutsendelse av SPAM
- Distribusjon av ulovlig/opphavsrettslig beskyttet materiale
- Phishing (aktiv)
- Identitetstyveri (passiv)
- … for å nevne noen.
  - Datamaskiner er svært anvendelige…

UNINETT

Botnets – hva skjer på dette området?

- Sikkerhetsmiljøet *tror* at man har oversikt over knapt 1/3 av eksisterende botnets
  - Bruk av IRC som kommunikasjonkanal, samt det at CC-trafikk går ukyptert, gir innsikt i virkemåte og struktur, samt at man kan infiltrere
  - Vi klarer å avskjære en del zombier fra CC-serverne
  - Vi klarer også å ta ut enkelte CC-servere
- Dreiing fra åpen til kryptert CC-trafikk
- Dreiing fra bruk av IRC mot HTTP
- Dreiing fra bruk av IRC til P2P type struktur ☹

UNINETT

HTTP-baserte BOTnets

- Infiserte maskiner instrueres til å kople seg opp mot http-tjenere som er kontrollert av bot-herdere
  - Effektiv unngåelse av pakkefiltere, ”alle” trenger tilgang til web
- Fra ”push” til ”pull” teknologi:
  - Dynamiske web-sider
  - Klientene poller webserverne med jevne mellomrom for å hente nye arbeidsordrer

UNINETT

P2P Botnets

- Kjennetegn:
  - Skift fra hierarkisk struktur til maskestruktur
  - Hvert individ i nettet kan være både klient *og* tjener på samme tid
    - Eliminerer behovet for en sentral C&C
    - Uttak av enkeltindivider har minimale konsekvenser for BOTnettet som et hele
  - Benytter både kjente P2P protokoller og spesialutviklede protokoller
    - Gjerne kryptert

Hvordan skjer rekrutteringen til botnets?

- Ved hjelp av ulike typer av ondsinnet programvare (malware)
- Spredevektorer:
  - Vedlegg til e-post
  - Websider
  - MSN/pratekanaler
  - ”Smarte” gratisprogrammer som man kan laste ned
  - Utnyttelse av sikkerhetshull

UNINETT

Spredning av malware

- Pakkefiltrering har antakelig nådd sitt potensiale
  - Baserer seg på en ”vennlig” innside og ”uvennlig(e)” utside(r)
  - Ofte konstruert slik at det er begrensinger på inngående trafikk, mens utgående trafikk slippes igjennom ufiltrert
    - Bummer!
- Paradigmeskifte:
  - ”Får vi ikke levere varene til deg, så får du komme og hente dem selv!”

UNINETT