Malwareanalyse - Trender

Christophe Birkeland, Dr.Ing.
NorCERT - Norwegian Computer Emergency Response Team

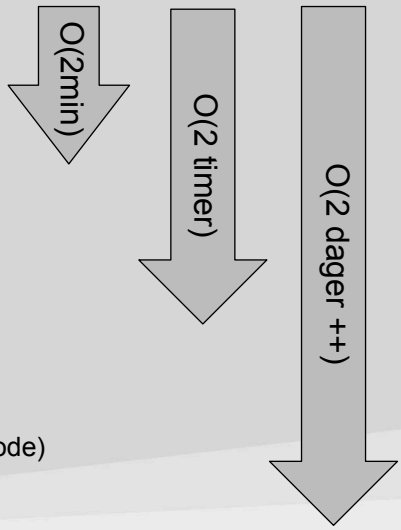
MALWARE ANALYSE | HVA ER UTFORDRINGEN?

Hva skjer når vi kommer over kode vi mistenker er malware?

- Mål: effektiv analyse – ulike fremgangsmåter:
  - Avhengig av "sak" og omfang/alvorlighet
  - Tidskritisk?
- Spørsmål:
  - Er det malware?
  - Hva er funksjonaliteten? Kapasiteten?

Malware-analyse i 3 steg

- Surface Analysis
- Dynamic Analysis
- Static Analysis (Analyse av kode)



NSM NorCERT

11

MALWARE ANALYSE | SURFACE ANALYSIS

- **Formål:**
  - Best mulig oversikt koden på under 2 minutter
  - Stake ut riktig fremgangsmåte for videre analyse
  - Meget godt egnet til automatisering
- **Inngår i analysen, bl.a.:**
- Sjekksummer
- Strings
- Identifisere filtype
- Antivirus skann

NSM NorCERT

4

MALWARE ANALYSE | DYNAMIC ANALYSIS

- Kjøring av kode i isolert miljø
  - Må ligne mest mulig på et reelt system
  - De fleste labmiljø kan detekteres
- Analysere oppførsel – Logging av API-kall
  - Opprettelse av filer
  - Nye prosesser
  - Identifisere de viktigste filene / delprosessene
- Dump av nettverkstrafikk
  - Hvem snakkes det med, og hvordan?
  - All malware er på nett
  - Kryptering benyttes i økende grad

NSM NorCERT

5

MALWARE ANALYSE | DYNAMIC ANALYSIS – UTFORDRINGER

- Man drukner i informasjon
  - Det er mye som skjer på et OS når et program kjører
  - Alt er ikke interessant
- Rootkits skjuler informasjon / hindrer analyse
- Malware oppdager at det kjører i labmiljø
  - Koden kjører ikke
  - Koden kjører annen funksjonalitet
- Analysen blir sjeldent tilstrekkelig detaljert
- Dynamisk analyse har stor verdi i forkant av statisk analyse (identifisere delkode for analyse)

NSM NorCERT

6

MALWARE ANALYSE | STATIC ANALYSIS

- "Kodeanalyse"
- Binærkode tolkes --- disassembleres--- og koden studeres
- Funksjonalitet kan bestemmes veldig eksakt og presist
  - Enormt potensiale for detaljert analyse

- Stor utfordring knyttet til bruk av pakkere
  - Disse må omgås for å få innsyn i koden
  - Ikke trivielt !

Trend:
Malware blir større og mer kompleks
--> store mengder kode å analysere

7

Christophe Birkeland
e-mail: **cbi@nsm.stat.no**
Hendelser: **norcert@cert.no**
Tlf (24/7): **02497**