T-02

**MALWARE**

Notater:

* Infeksjonstyper :
* (overskriving(ødelegger opprinnelig kode))
* Prepending beholder opprinnelig kode og kan komprimere den.
* Biblioteksinfeksjon som tillater virus å være minne resistente
* DLL er et dynamisk bibliotek som kunne endres av et virus program
* Teknikker for virus å gjemme seg er å skjule signaturen eller gjøre det vanskelig å generere (krypterte virus ofte komplekst)
* Krypterte virus har dekrypteringmotor og genererer tilfeldig krypteringsnøkkel , antivirus søker etter dekrypteringsmotor
* Ofte bare for å skjule koden , men kan gi: Polymorfe virus
* Virus legger tilfeldige variasjoner i koden sin før den spres videre. En polimorfic engine trengs for å dekode viruset før den kan kjøre og kan detekteres med en CPU-emulator.
* Malware er den egentlig årsaken til hackeangrep media definerer kan ha skjedd ved at it-admin trakk på et vedlegg i epost og systemet ble infisert.
* Adware var en annen skadeprogram som viser popup reklamer etter at den infiserte maskinen eks facebook.

1. **Hva står «malware» for? Hva betyr «malware»?**

Det står for malatious sofware og er en skadevare utviklet av svindlere. De er ofte programmerere

Fellesbetegnelse på “Ondsinnet

programvare” som utfører

uautoriserte og (oftest) skadlige

handlinger

1. **Hvilke ulike klassifikasjoner av malware har vi?**

• Virus: Virus endrer eksisterende filer eller systemer, koden kan

ikke leve eller spre seg alene

• Orm: automatisk spredning fra maskin til maskin over nettet

• Skjuler seg

• Rootkit: endrer OS for skjule nærvær

• Trojaner: Nytteprogram som skjuler ondsinnede operasjoner

(f.eks. keylogger)

• «Nyttelast» (payload)

• Alt fra humor/irritasjon til ran av maskinkraft og identitetstyveri

1. **Hva menes med «innside-angrep»?**

Skyldes av noen som er en del av en organisasjon som kontrollerer eller bygger tjenesten som skulle vært beskyttet (utro programvare) eks malware som utnytter sikkerhetshull er lagt inn med vilje av en programmerer og er mest aktuelt for bedrifter og deres kunder

1. **Hva menes med «backdoor»?**

En skjult metode eller kommando i et program som typisk tillater en bruker å utføre handlinger han /hun ikke normalt har tillatelse til .

Programmer oppfører seg vanligvis normalt og når den aktiveres gjør programmet noe uforventet f.eks. hever privilegier

Vennlig utgave easter eggs:

Eks på det er google :Do a barrel roll er en skjult kommando i søkefeltet etter tasting.

1. **Hva er «Easter Egg» i forhold til Malware?**

1. **Hva menes med Logikkbomber**

Det utfører en handling først når en betingelse inntreffer

Det er eks en programmerer legger inn en betingelse om programmet skal kræsje alt slettes dersom man ikke er med i to lønnsutbetalinger på rad.

1. **Hva er et virus?**

Virus er program som kan replisere seg selv (Dette er ganske facinerende)

Ved å endre andre filer/program og ved å infisere andre dataprogram med kode

Som kan forme seg videre.

Det er evnene til å forme seg lokalt som skiller virus fra malware

Virus krever innledende brukermedvirkning for å spre seg.

Eksempler på virus er : Å klikke på en link og godta installasjon, åpne epost vedlegg. Eller dele en minnepinne, eller annet USB-utsyr

1. **Hvordan spredde «Brain»-viruset seg?**

Dette er verdens første virus og kom i 1986, dette viruset klarte å infisere exe filer med Suriv-02 infiserte en bootsektor og erstattet den med et virus (Brain viruset) i datamaskinen som ikke kunne piratkopiere programvaren deres. Ble utviklet av to brødre i Pakistan som var redde for at folk skulle piratkopiere programvaren deres.

1. **Hva er en orm («Worm»)?**

Det er en malware som sprer kopier av seg selv uten å infisere andre program og vanligvis uten menneskelig medvirkning .

Det som skiller ormen fra virus er at de ikke infiserer eller endrer LOKALT

(filer eller bootsektorer)

• men begge deler spres ved selv-replisering

• I de fleste tilfeller vil ormen ha en ondsinnet nyttelast

(payload)

• Installere bakdør

• Slette filer

1. **Skriv en kort sammendrag av hva «ILOVEYOU»-ormen var**

ILOVEYOU ormen er en malware som spredde seg via epost og infiserte 50 millioner PCer ila 9 dager og kom på 2000 . Den var ikke skadelig, men bare spredde seg og gikk ut på at brukeren måtte manuelt åpne en fil i epost . Dette er en type massmail malware.

1. **Hva er en «Trojaner»**

Trojaner er en malware som utfører en nyttig jobb , men som i tillegg gjør noe . ondsinnet. F.eks en tastaturavlytter Trojanere installeres ofte som en del av en nyttelast til en malware.

Eksempler på det er AIDS trojanere. Falsk antivirus

Trojanere kan også installeres av bruker/administrator med overlegg eller ved uhell.

1. **Hva er et Rootkit?**

Rootkits er en samling av software som brukes til å få tilgang til områder personen ikke er autorisert til. Rootkits kan manipulere data på root-nivå og dermed endre/fjerne filer. Siden rootkit kan endre filer så kan den også skjule seg for antivirus programmer.

Rootkits modifiserer OS og skjuler sin eksistens f.eks modifiserer filsystemer som gir muligheter til å se en fil. Den er vanskelig å oppdage med programvare som er avhengig av OS-et selv.

Dette er egentlig ikke en egen type malware, men

en teknikk brukt av malware for å skjule sine

spor og gjøre seg selv usynlig på maskinen som

er infisert.

1. **Hva er «botnet»?**

Botnet kalles også for malware zombier er det som gjør maskinen om til en zombie. Som er en eksternt kontrollert maskin som benyttes i ondsinnet angrep

Det er ofte en person som sender et angreps kommando til botene sine for å angripe et offer. Botnet går ut på at mange datamaskiner kan sende masse data til en maskin som gjør det vanskelig for den å prosessere all dataen. Botnet styres av en person som eier alle botnet og kan spre seg til mange maskiner.

1. **Hvordan bruker antivirusprogrammer signaturen til å flagge programmer?**

1. **Hva er en Heuristisk analyse?**

Brukes for å identifisere nye og <<Zero day>> malware , antivirus bestemmer om det er en malware ut ifra av f.eks. forsøker å endre eller slette system-filer.

Den kjører koden i en isolert miljø , den overvåker atferden til maskinen og ved mistanke markeres det programmet som en malware etter systemskanning. Dette kan automatiseres , men utløse false alarmer.