



SKJULTE HEMMELIGHETER

Har du sjekket filområdene dine før hackerne gjør det?

Finn sensitive data på egne filområder med Snaffler – før angriperne gjør det



Esben Jørgensen

IKT-sikkerhetsrådgiver, Horten kommune · leder for fagnettverket for informasjonssikkerhet og personvern i Digi-TV

Hva skjuler seg på filserveren?



Et regneark med passord

...fra 2016. Fortsatt på fellesområdet.



En gammel NAV-eksport

Personopplysninger som aldri ble ryddet.



Et dokument ingen har åpnet

På fire år – men fortsatt lesbart for hele organisasjonen.

De fleste virksomheter har mer skjult på filserverne sine enn de tror – og det er nettopp dette angripere leter etter så snart de er inne. Vi kan lete på nøyaktig samme måte, i vårt eget miljø, og rydde opp *før* de kommer.

Et redteam-verktøy, brukt defensivt



Dobbeltbruk

Funksjonaliteten som finner deres hemmeligheter kan en angriper bruke like godt til å finne veien videre inn i nettverket.



Lovlig kun med mandat

Uautorisert bruk mot systemer du ikke eier eller har fullmakt til, kan rammes av straffeloven § 204 – uberettiget tilgang til datasystem.



Skriftlig godkjenning først

Avtal omfang, varighet og ansvarlig leder før du kjører – akkurat som ved en pentest.



Del aldri ukritisk

Egne regelsett og funn er sensitive i seg selv. Ikke del dem åpent, og vis aldri ekte hemmeligheter på skjermen.

Angriperens perspektiv

Etter et første fotfeste er fildelinger et av de mest lønnsomme stedene å lete. Det du finner, finner de også:



Legitimasjon

Passord i klartekst, service-kontoer, nøkler og tokens gir veien videre i nettet.



Personopplysninger

Sensitive opplysninger



Privilegie-eskalering

Backup, config og scripts avslører hvordan miljøet henger sammen.

Snur vi verktøyet mot oss selv, ser vi miljøet slik angriperen ville sett det.

Hva er Snaffler?



Et åpent verktøy som gjennom søker Windows-/AD-fildelinger og bruker regler og regex-mønstre til å skille ut filer som kan inneholde hemmeligheter – fra fjellet av uinteressante filer.



Hvordan

Bruker regler og SMB for å skanne miljøet – kombinasjoner av regler, ordlister og regex som samarbeider.



Finner

Passord, nøkler (id_rsa, .ppk), .kdbx, config-filer, backup, VMDK m.m.



Vår vinkling

Brukt defensivt: skann eget miljø, rydd opp, gjør det til fast rutine.

Opprinnelig laget for pentest/red team (l0ss & Sh3r4, SnaffCon) – like nyttig for den som forsvarer.

Hvordan det fungerer



1 · AD-oppslag

Henter liste over
domenemaskiner via LDAP



2 · Finn filområder

Kobler til SMB og ser hvilke
shares som er lesbare



3 · Enumerer filer

Går gjennom filer og mapper i
delingene



4 · Klassifiser

Regler avgjør hva som er
sensitivt vs. støy

Defensivt: du kjører med en konto du kontrollerer, mot dine egne delinger. Da ser du akkurat det angriperen ville sett – uten å måtte gjette hvor de sensitive filene ligger.

Bruk din egen config-fil

Med **-z** samler du alle valgene i én **.toml**-fil – dokumentert, gjenbrukbart og likt hver gang.

```
# 1) Generer config fra dine vanlige valg
PS> snaffler.exe -s -o srv.log \
    -i \\filserver\felles \
    -p C:\mine-regler -z generate
# -> lager .\default.toml til redigering

# 2) Kjør skann rett fra config senere
PS> snaffler.exe \
    -z C:\snaffler\config.toml
```

PathTargets

Hvilke stier / shares som skannes

RuleDir

Mappe med dine egne .toml-regler

LogType / LogFilePath

Plain eller JSON – og hvor loggen havner

InterestLevel

Hvor mye støy du tar med (0–3)

MaxSizeToGrep / ...Snaffle

Grenser for søk i og kopi av filer

MaxThreads

Tråder: fart vs. belastning

Fordelen: skannet blir reproduserbart, kan versjonshåndteres og deles – hele teamet kjører likt, hver gang.

Kjør det trygt og ryddig



Forankring

Ha godkjenning fra ledelsen. Verktøyet er laget for angrep – behandle det deretter.



Det er støyende

Standardmodus ligner SharpHound/BloodHound. Varsle SOC/drift så det ikke tolkes som et reelt angrep.



Håndter funnene som sensitive

Loggen peker rett på hemmeligheter. Lagre den beskyttet og slett når du er ferdig.



Velg tidspunkt

Store skann belaster filservere og nett – kjør utenom topplast.

Klassifiserere – motoren

Snaffler bruker et system av **klassifiserere** som sender objekter nedstrøms eller forkaster dem. Hver klassifiserer jobber i én fase:



Kraften ligger i å kjede regler: en rimelig regel (matcher .config) sender treff videre til en dyrere regel (regex mot innholdet). Slik blir dype søk mulig uten å bremse alt.

Hvordan en regel er bygd opp

```
[[ClassifierRules]]
EnumerationScope = "FileEnumeration"
RuleName        = "KeepExtExactBlack"
MatchAction     = "Snaffle"
MatchLocation   = "FileExtension"
WordListType    = "Exact"
WordList        = [".kdbx", ".ppk",
                  ".vmdk", ".ovpn"]
Triage          = "Black"
```

EnumerationScope

Hvilken fase regelen gjelder

MatchAction

Snaffle · Discard · Relay · CheckForKeys

MatchLocation

ShareName · FilePath · FileName · FileExtension · FileContent...

WordListType

Exact · Contains · StartsWith · EndsWith · Regex

WordList

Strengene / regex-mønstrene det matches mot

Triage

Alvorsgrad: Black · Red · Yellow · Green

Regeleksempler: behold vs. forkast



Behold interessant (Snaffle)

```
[[ClassifierRules]]
EnumerationScope="FileEnumeration"
RuleName="KeepFilenameExactBlack"
MatchAction="Snaffle"
MatchLocation="FileName"
WordListType="Exact"
WordList=["id_rsa", "shadow",
          "NTDS.DIT", "passwd"]
Triage="Black"
```



Forkast irrelevant (Discard)

```
[[ClassifierRules]]
EnumerationScope="FileEnumeration"
RuleName="DiscardExtExact"
MatchAction="Discard"
MatchLocation="FileExtension"
WordListType="Exact"
WordList=[".png", ".gif", ".css",
          ".ttf", ".ico", ".svg"]
# Triage ignoreres ved Discard
```

Discard fjerner støy: kast bilder, fonter og CSS på utvidelse, eller hele stier (node_modules, gamle programmapper) på FilePath.

Regelkjeder og spesialsjekker

Med **Relay** sender en billig regel treff videre til en (eller flere) navngitte regler – slik bygger du forgrenede kjeder.

```
[[ClassifierRules]]                                # 1) billig: sjekk utvidelse
RuleName="ConfigGrepExtExact"
MatchLocation="FileExtension"    WordList=[".config", ".xml", ".ini"]
MatchAction="Relay"    RelayTargets=["KeepConfigGrepContainsRed"]

[[ClassifierRules]]                                # 2) dyr: grep i innholdet
RuleName="KeepConfigGrepContainsRed"    EnumerationScope="ContentsEnumeration"
MatchLocation="FileContentAsString"
WordList=["password=", "connectionString=", "validationKey="]
MatchAction="Snaffle"    Triage="Red"
```



CheckForKeys: parser .der/.pfx-filer som x509-sertifikater og varsler bare hvis de faktisk inneholder en privat nøkkel – langt bedre signal-til-støy enn å rapportere alle sertifikater.

Egne regler tilpasset dine data

Standardreglene er laget for generiske miljøer. **Den store gevinsten ligger i regler skreddersydd for norske forhold og nettopp din organisasjon:**

```
[[ClassifierRules]]                # 1) filsti - egen Black-varsel
RuleName = "BarnevernFileNames"
MatchLocation = "FilePath"    WordListType = "Contains"
WordList = ["barnevern", "fosterhjem", "omsorgsovertak", ...]
MatchAction = "Snaffle"      Triage = "Black"

[[ClassifierRules]]                # 2) NY: kobler på innholdssøket
RuleName = "BarnevernContentTrigger"
MatchLocation = "FileExtension"    WordListType = "Contains"
WordList = [".txt", ".csv", ".xml", ".log", ...]
MatchAction = "Relay"      RelayTargets = ["BarnevernFileContents"]
```



Barnevern

barnevern, fosterhjem, bekymringsmelding – Black på filsti.



Helseopplysninger

pasientjournal, diagnose, sykemelding – Red-triage.



Skole & elev

utrygt skolemiljø, klage på vedtak – Yellow-triage.



Kjente støykilder

Discard på deres egne store, kjedelige mapper.

Legg reglene i en mappe og kjør med -p. Test regex på et lite område først – dårlige mønstre gir mye støy og treg kjøring.

Å lese loggen



Black

Mest alvorlig



Red

Svært interessant



Yellow

Verdt et blikk



Green

Lav interesse

Prioriter opprydding etter farge – ta Black og Red først.

Slik leses en loggrad (fra venstre mot høyre):

```
[host\bruker] 15:37 [Red] <KeepConfigRegexRed|R|...|208kB|2020-01-10> \\srv\felles\web.config (...utdrag...)
```



Tidspunkt



Triage-nivå



Regelnavn som traff



R = lese, W = skrive



Regex/streng som matchet



Størrelse + sist endret



Full sti til filen



Kontekstutdrag

Etterbehandling med Snaffler Log Viewer

100 % lokalt: loggen lastes og bearbeides i nettleseren din. Ingenting sendes opp noe sted – avgjørende når funnene er passord, personopplysninger eller andre hemmeligheter.

Fra rå logg til noe du kan handle på – og dele med de som eier områdene:

`snaffler.log` (JSON) → Snaffler Log Viewer → sortert, filtrerbar oversikt i nettleseren



Filtrér & sortér

Klikk en kolonneoverskrift for å sortere
– triage, størrelse, dato, sti



Ekskluder støy

Høyreklikk en rad: ekskluder sti,
mappe, regel eller bruker på ett klikk



Bruker-kolonne

Viser hvem/hvilken vert hvert treff
kom fra, pluss en oppsummeringslinje
øverst



Dedupliker & siste kjøring

Fjern gjentatte treff, eller vis kun siste
scan med ett klikk

Tips: kjør med «-t JSON» – det er formatet Log Viewer leser direkte, uten konvertering.

Snaffler Log Viewer

Loads a Snaffler log (JSON or plain text) entirely in your browser — nothing is uploaded anywhere.

Choose File snaffler6.json

Loaded snaffler6.json — 1214 entries.

▼ What this reads

Støtter to formater: Snaffler JSON-logg (`{ "entries": [ ... ] }`) og ren tekstlogg (én melding per linje). Meldingsteksten parseres direkte for å hente ut rating, regel, treffet ord, størrelse, modifisert dato og sti. "Modified" er filens egen sist-skrevet-tid; "Snaffled" er tidspunktet Snaffler logget funnet (fra JSON-feltets `time` tom ved tekstmodus). `[Share]`-linjer vises også, med rating og sti.

Any column filter box accepts multiple terms (all must match), and a term can be excluded by prefixing it with `not` or `-`; quote phrases with spaces, e.g. `not "bilder til id-kort"` hides every row whose Path contains that phrase, and `not "bilder til id-kort" not thumbs.db` excludes both at once.

Rows: 946 Rating: Black ▼ Type: All ▼ Modified: Any year ▼ – Any year ▼ Snaffled from: mm/dd/yyyy 📅 to: mm/dd/yyyy 📅 Latest scan only ☐ Deduplicate (keep newest per file/share) Clear filters

👤 Snaffler kjørt som: (fra:)

Rating	Type	User	Rule / Match	Size	Modified	Snaffled	Path
	filter		filter	filter	filter	filter	filter, or not "phrase"
Black	File		BarnevernFileNames — barnevern	12679	2024-12-10 06:48:37Z	2026-09-10 15:19:38	\Remitteringsfiler Barnevern Modulus\avregninger (2).xml

UltraSnaffler – å se inni dokumenter

Standard-Snaffler leser *ikke* inni Office-dokumenter og PDF-er. UltraSnaffler gjør det.

Hva det er

- Egen byggevariant – bygg UltraSnaffler.sln i stedet for Snaffler.sln
- Ser inni ikke-flate formater: Word, Excel, PDF, .eml m.m.
- Biblioteket gjør .exe-en ~12× større – tyngre å kjøre in-memory

a

Prisen du betaler

- Standardreglene ser IKKE inni Office/PDF – for tunge å skrive
- Å lese inni dokumenter er mye tregere enn ren tekst
- Typisk miljø har enorme mengder lav-verdi Office/PDF = mye støy

For deg som forsvarer: persondata ligger ofte nettopp i Word/Excel/PDF. Kjør UltraSnaffler målrettet på utvalgte områder, ikke hele domenet. Så fanger du det ren Snaffler går glipp av, uten å drukne i tid og støy.

Fra funn til handling

Et skann uten oppfølging er bare en liste. Verdien ligger i det du gjør etterpå:



1 · Prioritér

Sortér på triage. Ta Black/Red først – aktive passord og persondata.



2 · Rydd & sikre

Slett, flytt eller lås ned. Roter passord og nøkler som har ligget eksponert.



3 · Rett tilgangene

Stram inn hvem som kan lese området. Færrest mulig, etter behov.



4 · Gjenta jevnlig

Gjør skann til fast rutine – nye sensitive filer dukker opp hele tiden.

Involver de som eier områdene. De vet ofte hvorfor en fil ligger der – og må være med for at oppryddingen skal vare.



Finn dem før hackerne gjør det.

https://github.com/EsbenSec/Snaffler_Regler



Takk – spørsmål?



Esben Jørgensen · IKT-sikkerhetsrådgiver, Horten kommune

Fagnettverket for informasjonssikkerhet og personvern, Digi-TV · github.com/SnaffCon/Snaffler