

# Vedlegg G – Test CanaryTokens

## Innhold

|  |   |
|--|---|
| Enkel testing .....                                | 1 |
| Test ved Google Drive og andre teksteditorer ..... | 2 |
| Detektering av CanaryToken .....                   | 3 |

## Enkel testing

### 1. Åpner CanaryToken Filen og får varsel

### Canarytoken triggered

ALERT

An MS Word Canarytoken has been triggered by the Source IP 85.19.195.178

**Basic Details:**

|                |  |
|----------------|--|
| Channel        | HTTP   |
| Time           | 2024-02-27 08:47:25.154452                       |
| Canarytoken    | h64ina251j6aon46jsmz8j1x                         |
| Token reminder | Honeydocument - passord, åpnet                   |
| Token type     | MS Word  |
| Source IP      | 85.19.195.178                                    |
| User-agent     | Mozilla/4.0 (compatible; ms-office; MSOffice 16) |

**Canarytoken Management Details:**

Manage this Canarytoken [here](#)

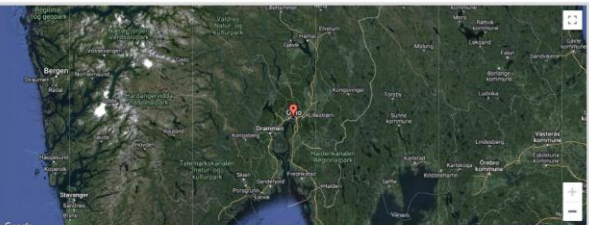
More info on this token [here](#)

### 2. Ser på «Manage» på CanaryToken nettsiden

History for Canarytoken:  
h64ina251j6aon46jsmz8j1x

Heads Up! Click the incident items for more info.

Incident Map



Incident List

Export

|       |                            |     |               |          |      |
|-------|----------------------------|-----|---------------|----------|------|
| Date: | 2024-02-27 08:47:25.149732 | IP: | 85.19.195.178 | Channel: | HTTP |
| Date: | 2024-02-27 08:40:30.126569 | IP: | 85.19.195.178 | Channel: | HTTP |
| Date: | 2024-02-27 08:40:29.903799 | IP: | 85.19.195.178 | Channel: | HTTP |
| Date: | 2024-02-27 08:36:28.826112 | IP: | 85.19.195.178 | Channel: | HTTP |

### 3. Annen informasjon en kan se:

| Geo Info  |  |
|---|--|
| Country   | NO 🇳🇴  |
| City  | Oslo   |
| Region  | Oslo   |
| Organisation  | AS25400 Telia Norge AS                           |
| Hostname  | 85-19-195-178.telia-isp.no                       |
|  |  |
| Known Exit Node   | False  |
| Basic Info  |  |
| Memo  | Honeydocument - passord, åpnet                   |
| useragent   | Mozilla/4.0 (compatible; ms-office; MSOffice 16) |

## Test ved Google Drive og andre teksteditorer

### 1. Forsøk på å laste opp til Google Drive for så å laste ned

"passord\_praksis.docx" er infisert med et virus. ×

Denne filen kan skade datamaskinen din. Du må bare laste ned denne filen hvis du forstår risikoen.

[Last ned den infiserte filen](#) [Avbryt](#)

- a. Ved åpning etter nedlastning alarmerer fortsatt CanaryToken til mail.

### 2. Ved åpning i andre program enn Microsoft Office vil den fortsatt gi alarmer

| Basic Info |   |
|------------|---|
| Memo       | Honeydocument - passord, åpnet                                |
| useragent  | LibreOffice 24.2.0.3 denylistedbackend/8.6.0<br>OpenSSL/3.2.1 |

# Detektering av CanaryToken

## 1. For å laste ned CanaryTokenDetector:

```
git clone https://github.com/referefref/canarytokendetector.git

cd canarytokendetector/

sudo apt install pdftk-java python3 python3-pip -y

sudo pip3 install pefile

sudo apt install zsh

wget
https://raw.githubusercontent.com/DidierStevens/DidierStevensSuite/master/disitool.py

chmod +x canarytest.sh
```







## 2. Starter programmet og viser hjelpe-siden

```
Released under GPL-3.0 license
Description: Tool that allows for the location and nullification of some types of canary tokens.

Currently Supported Canary Tokens:
Type          Detect  Nullify
-----
Microsoft Word  ✓      ✓
Microsoft Excel ✓      ✓
Wireguard VPN Config ✓      ✓
Sensitive Command Token ✓      ✓
Windows Folder  ✓      ✓
MySQL Dump      ✓      ✓
PDF Token       ✓      ✓
Azure Login Certificate ✓      ✓
Kubeconfig Token ✓      ✓
Custom Executable (.exe, .dll) ✓      ✓

Arguments and Options:
Flag  Option  Description  Argument  Default Value
-----
-h    help    Show this dialogue
-v    verbose  Verbose output
-t    test-mode  Check for presence only, do not nullify tokens
-d    directory  Check entire directory contents
-r    recursive  Scan recursively from directory or current path
-f    location  File or Folder location
-o    output_file  Report output file
```

## 3. Lager 6 CanaryTokens i henhold til Vedlegg B i ulike format

|   |                               |                  |                         |       |
|---|-------------------------------|------------------|-------------------------|-------|
|  | 1 - passord_praksis.docx      | 12.03.2024 09:17 | Microsoft Word-dok...   | 0 kB  |
|  | 1 - økonomi-2024_praksis.xlsx | 12.03.2024 09:04 | Microsoft Excel-regn... | 0 kB  |
|  | 1 - kubeconfig_praksis        | 12.03.2024 08:44 | Fil                     | 10 kB |
|  | 1 - kontrakt_praksis.pdf      | 12.03.2024 08:59 | Chrome HTML Docu...     | 5 kB  |
|  | 1 - ja.docx                   | 12.03.2024 09:04 | Microsoft Word-dok...   | 0 kB  |
|  | 1 - directory-token_praksis   | 12.03.2024 08:47 | Filmappe                |       |




4. Kjører programmet med -dtf, som vil si at en KUN detekterer hvis filene er CanaryTokens.

```
joachim@Håversens-LAB:~/FILER_LINK/CanaryTOKENS/canarytokendetector$ ./canarytest.sh -dtf .  
  
CanaryTokenDetector Version 1.0  
James Brine : https://github.com/referefref/canarytokendetector  
cp: cannot create regular file 'tmp/.1 - directory-token_praksis/My Documents/desktop.ini': No such file or directory  
grep: tmp/.1 - directory-token_praksis/My Documents/desktop.ini: No such file or directory  
Canary token detected in file: ./1 - ja.docx  
Canary token detected in file: ./1 - kontrakt_praksis.pdf  
Canary token detected in file: ./1 - okonomi-2024_praksis.xlsx  
Canary token detected in file: ./1 - passord_praksis.docx
```

5. Kjører programmet med -vdf, som vil si at en detekterer og eventuelt fjerner varslingsmekanismen hvis en detekterer at filen er en CanaryToken.

```
joachim@Håversens-LAB:~/FILER_LINK/CanaryTOKENS/canarytokendetector$ ./canarytest.sh -vdf .  
  
CanaryTokenDetector Version 1.0  
James Brine : https://github.com/referefref/canarytokendetector  
Running in directory mode  
RUNNING IN NULLIFY MODE... MAKE SURE DATA IS BACKED UP BEFORE PROCEEDING  
Searching . for potential canary files  
Discovered 6 potential canary tokens...  
./git/config  
./1 - directory-token_praksis/My Documents/desktop.ini  
./1 - ja.docx  
./1 - kontrakt_praksis.pdf  
./1 - okonomi-2024_praksis.xlsx  
./1 - passord_praksis.docx  
Checking if canary token is present in ./git/config  
No canary token detected  
Checking if canary token is present in ./1 - directory-token_praksis/My Documents/desktop.ini  
cp: cannot create regular file 'tmp/.1 - directory-token_praksis/My Documents/desktop.ini': No such file or directory  
grep: tmp/.1 - directory-token_praksis/My Documents/desktop.ini: No such file or directory  
No canary token detected  
Checking if canary token is present in ./1 - ja.docx  
Extracting file...  
Canary token detected in file: ./1 - ja.docx  
Removing token...  
sed: can't read s/canarytokens.com//g: No such file or directory  
sed: can't read s/canarytokens.com//g: No such file or directory  
Compressing files...  
ms_office:20: command not found: zip  
Replacing original file  
mv: cannot stat './.1 - ja.docx.tmp': No such file or directory  
Done  
Checking if canary token is present in ./1 - kontrakt_praksis.pdf  
Unpacking PDF  
Canary token detected in file: ./1 - kontrakt_praksis.pdf  
Removing token...  
Replacing original file  
Done  
Checking if canary token is present in ./1 - okonomi-2024_praksis.xlsx  
Extracting file...  
Canary token detected in file: ./1 - okonomi-2024_praksis.xlsx  
Removing token...  
sed: can't read s/canarytokens.com//g: No such file or directory  
Compressing files...  
ms_office:20: command not found: zip  
Replacing original file  
mv: cannot stat './.1 - okonomi-2024_praksis.xlsx.tmp': No such file or directory  
Done  
Checking if canary token is present in ./1 - passord_praksis.docx
```

6. Filene som det ikke ble detektert som CanaryTokens:

|   |                  |                     |       |
|---|------------------|---------------------|-------|
|  1 - kubeconfig_praksis      | 12.03.2024 08:44 | Fil                 | 10 kB |
|  1 - kontrakt_praksis.pdf    | 12.03.2024 08:59 | Chrome HTML Docu... | 5 kB  |
|  1 - directory-token_praksis | 12.03.2024 08:47 | Filmappe            |       |