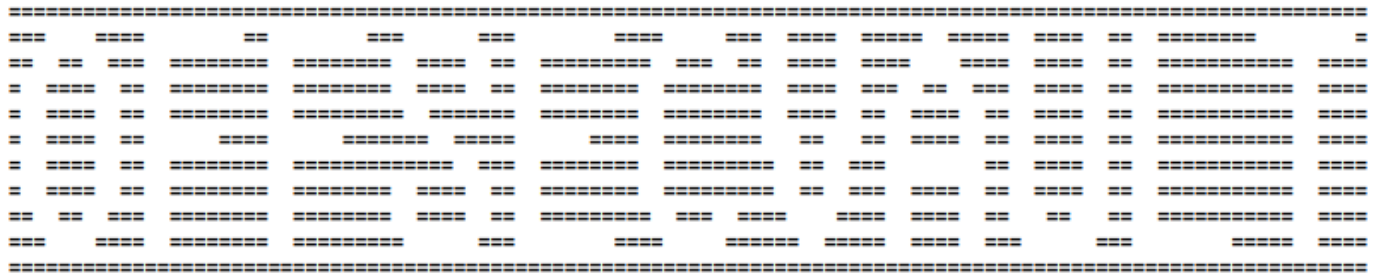


how_to_create_honey_tokens_?_CanaryTokens



[offsecvault](#) - Since 2021

Honey tokens are basically known as “traps or decoys“, are different artifacts that helps to track activity in case of a breach. It can be used on files, images, databases, API keys, and more.

As part of an “Active Defense & Cyber Deception” mindset, the use of honey tokens to track valuable data can be a good technique to track as much information as possible from any attack activity. Canary Tokens is a project that can be used for this, it is free and available online, also, you can set up your own server (preferable) to avoid easy detection and get better results.

Track activity ? but how ?

First: Token

“It is a unique value created to identify something”

For example,

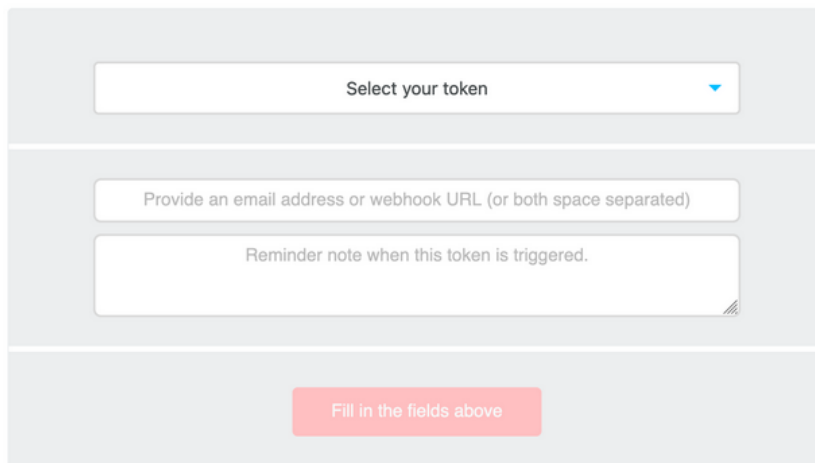
Recently your company approved a new security policy to store the financial reports in .pdf file format on a specific network location. “C:\vault” So, based on the request the network location from now will be a high risk data value and monitor it will be a must. Canary Tokens contains a token type “adobe_pdf” that basically can create a simple trap, “a new blank file named as you want that will trigger an alert once the file is open” also, for this specific scenario you can set a new token to monitor in case the network share is accessed.

Let’s create the .pdf file trap, (Canary Tokens – online version)

#createdecoy

Step.1 Visit the Website (site)

You will see a interface like the following,



The screenshot shows a configuration form for a Canary Token. It consists of three input fields stacked vertically, followed by a red button. The first field is a dropdown menu labeled "Select your token". The second field is a text input labeled "Provide an email address or webhook URL (or both space separated)". The third field is a larger text input labeled "Reminder note when this token is triggered." The button is labeled "Fill in the fields above".

Brought to you by [Thinkst Canary](#), our insanely easy-to-use honeypot solution that deploys in just four minutes. **Know. When it matters.**

© [Thinkst Applied Research](#) 2015–2021

Step.2 Create the .pdf file token

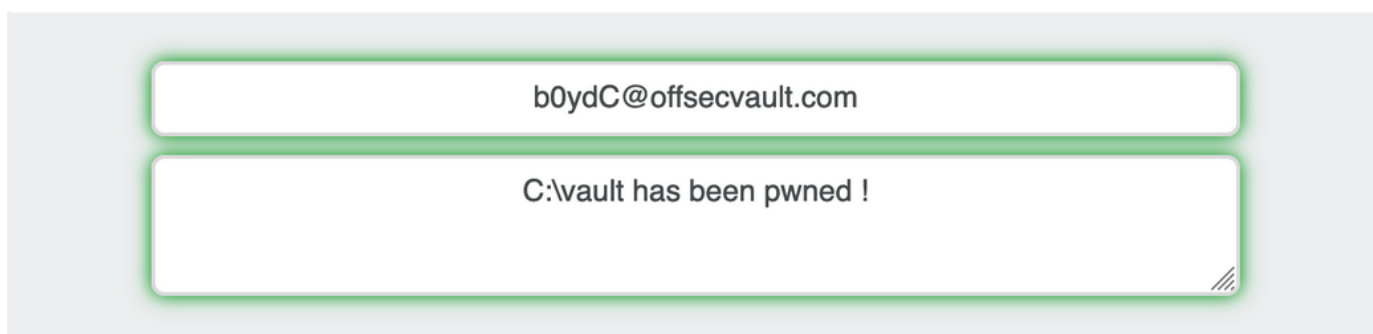
2.1 Select your token from the drop-down menu:



Acrobat Reader PDF Document

Get alerted when a PDF document is opened in Acrobat Reader

2.2 Insert the email address or web-hook URL and brief description as reminder for this alert notification:



The screenshot shows the configuration form with example values. The first field contains the email address "b0ydC@offsecvault.com". The second field contains the reminder note "C:\vault has been pwned !".

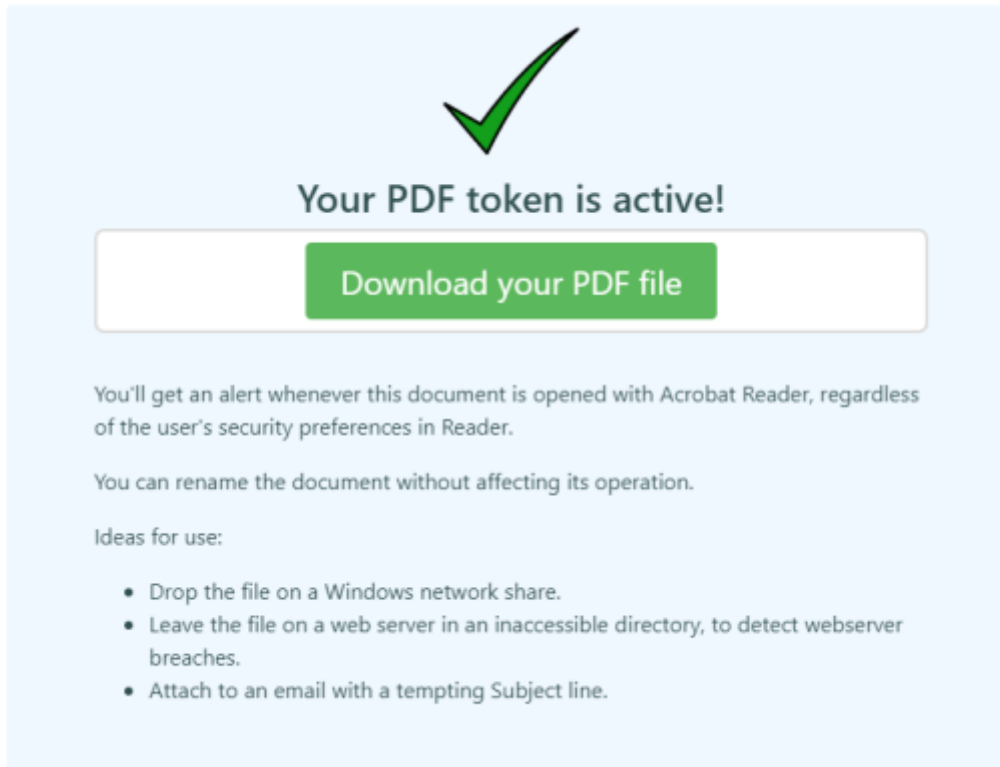
2.3 Click "Create my Canarytoken"



Create my Canarytoken

Note: The token creation process is the same for the different token types, it will change on behavior, for example for .pdf or word token type you will download a file and a remote request will be created when the file is open, however, the “Web bug /URL Token” does not create a file, instead it creates a URL and it triggers when the URL is visited.

2.4 Token active, now, let's download the token



Your PDF token is active!

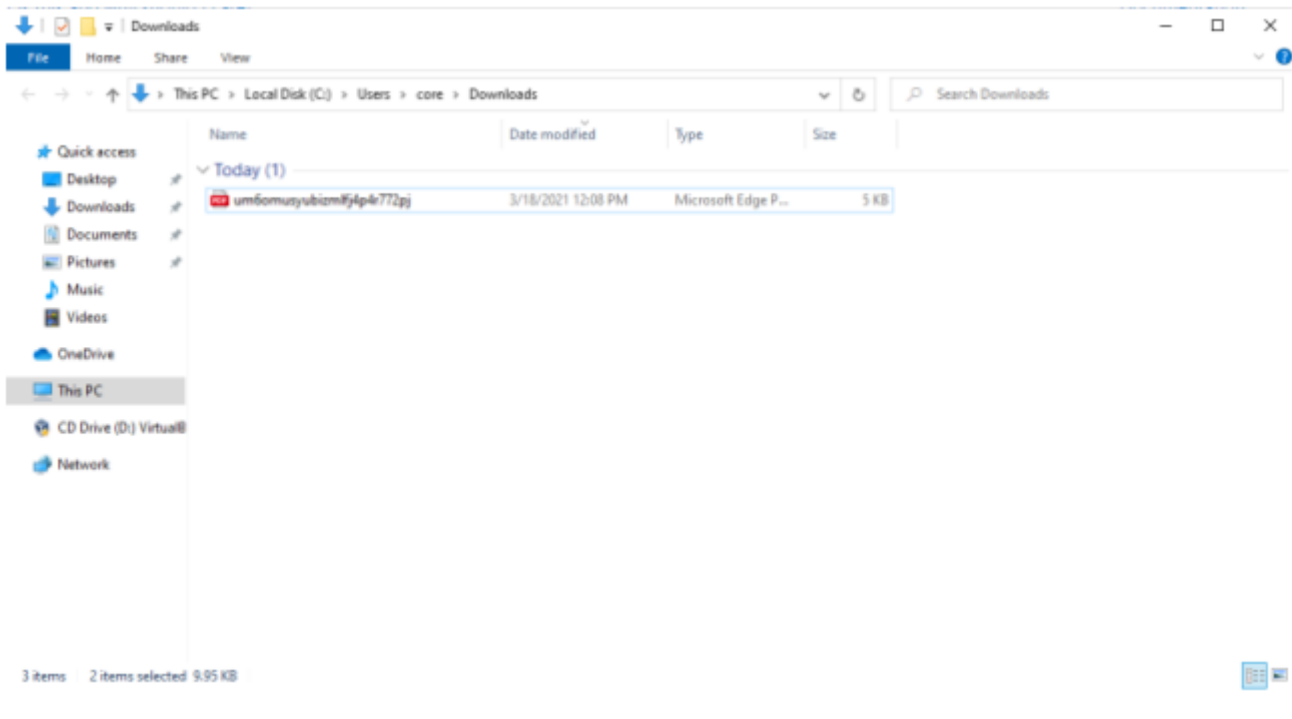
[Download your PDF file](#)

You'll get an alert whenever this document is opened with Acrobat Reader, regardless of the user's security preferences in Reader.

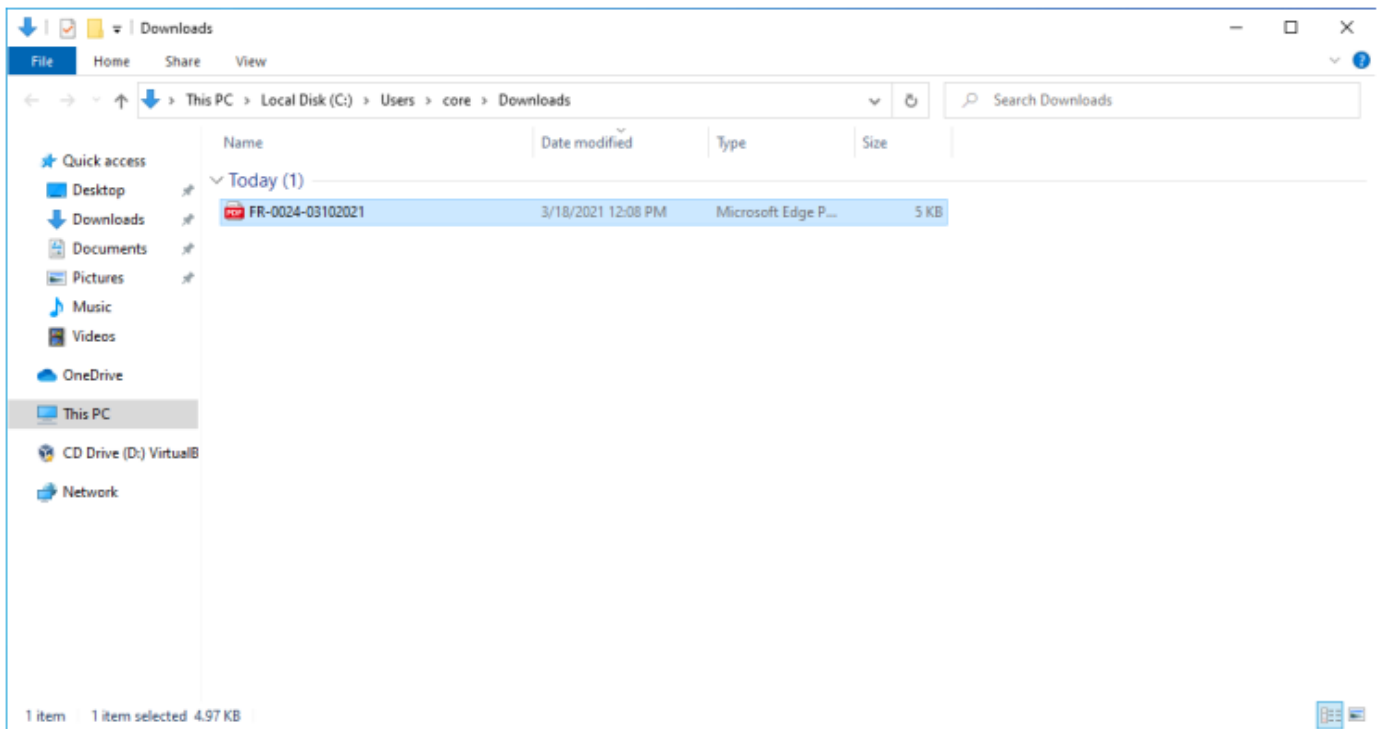
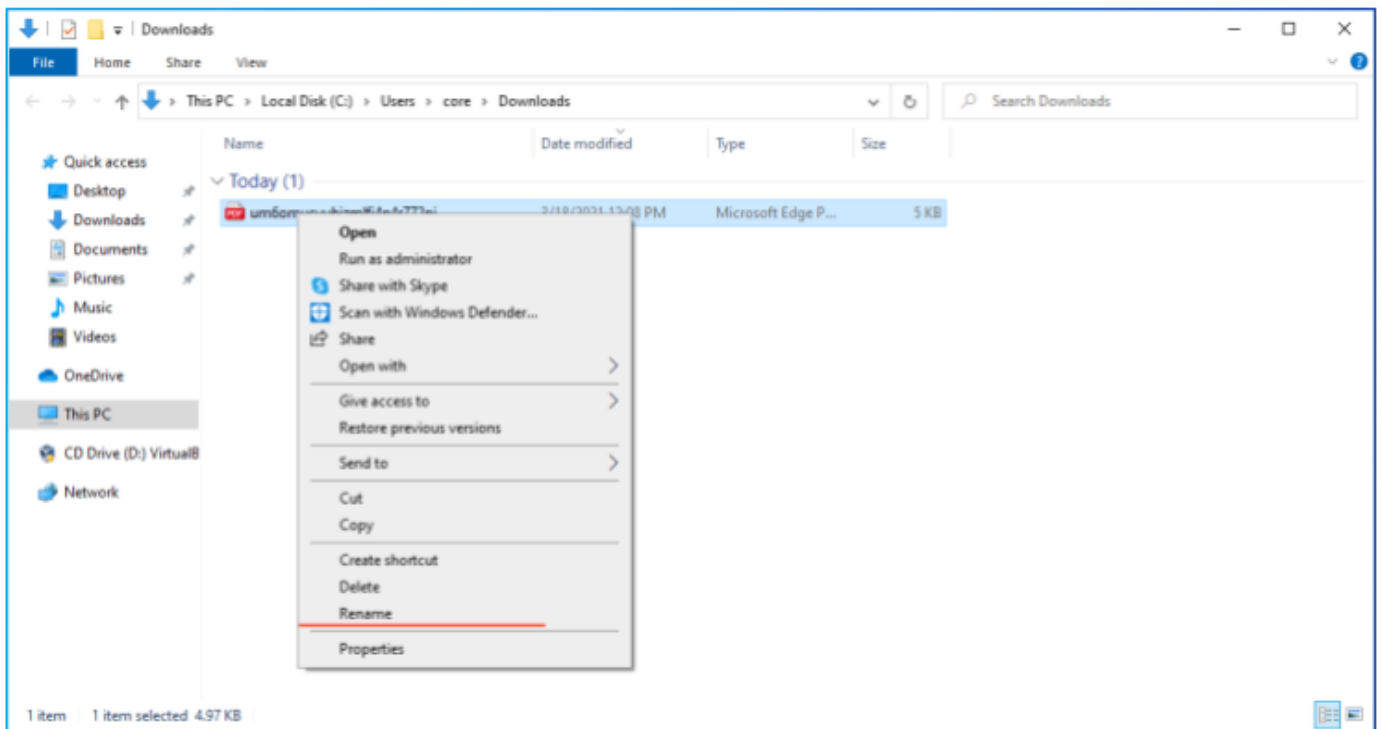
You can rename the document without affecting its operation.

Ideas for use:

- Drop the file on a Windows network share.
- Leave the file on a web server in an inaccessible directory, to detect webserver breaches.
- Attach to an email with a tempting Subject line.

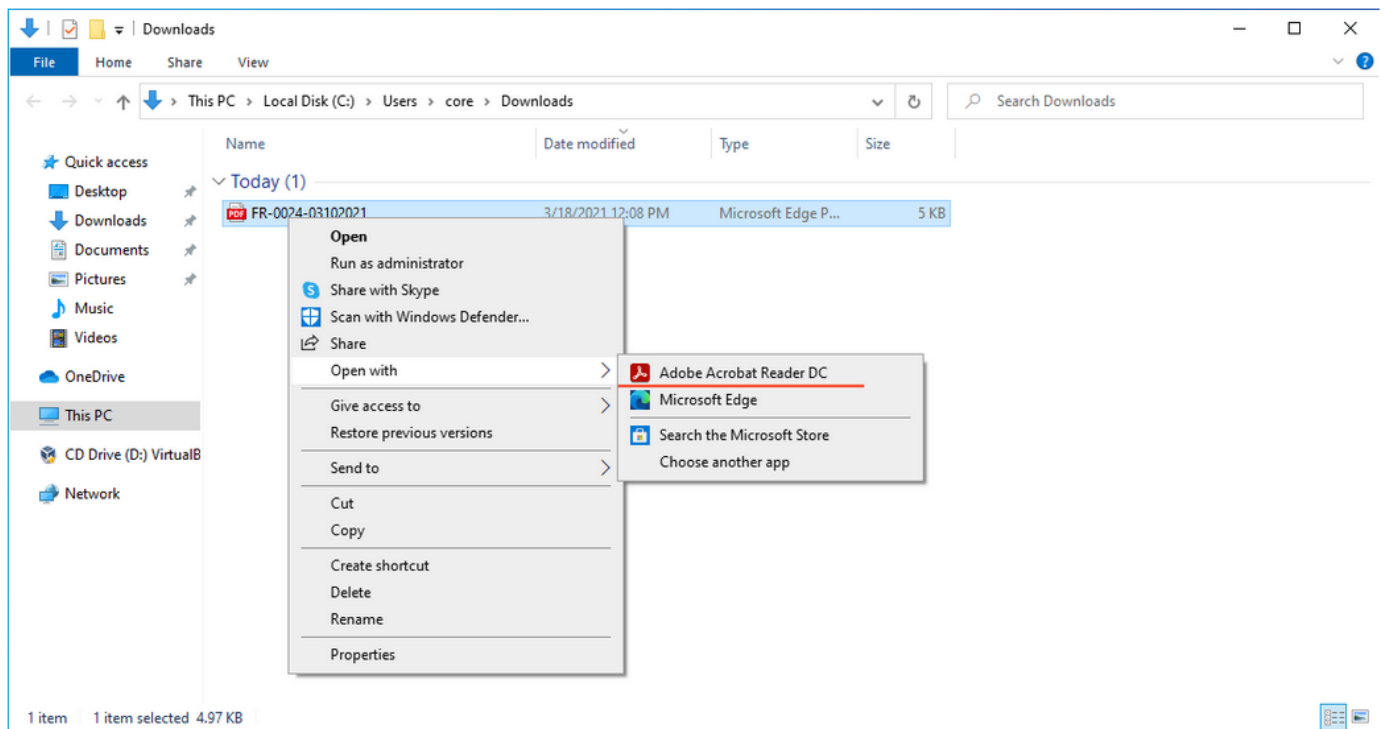


2.5 Rename the file so it looks like a normal report

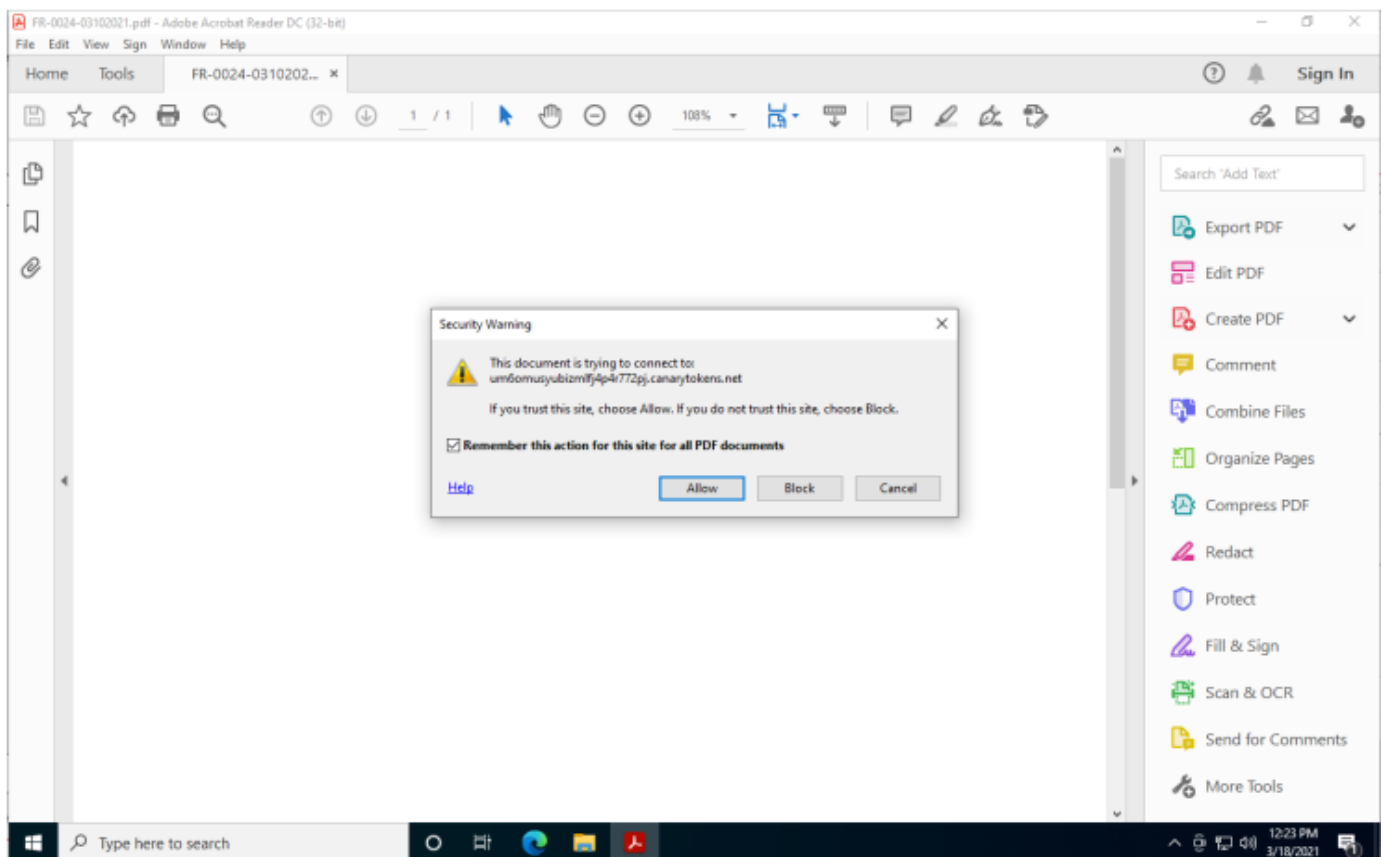


#attack

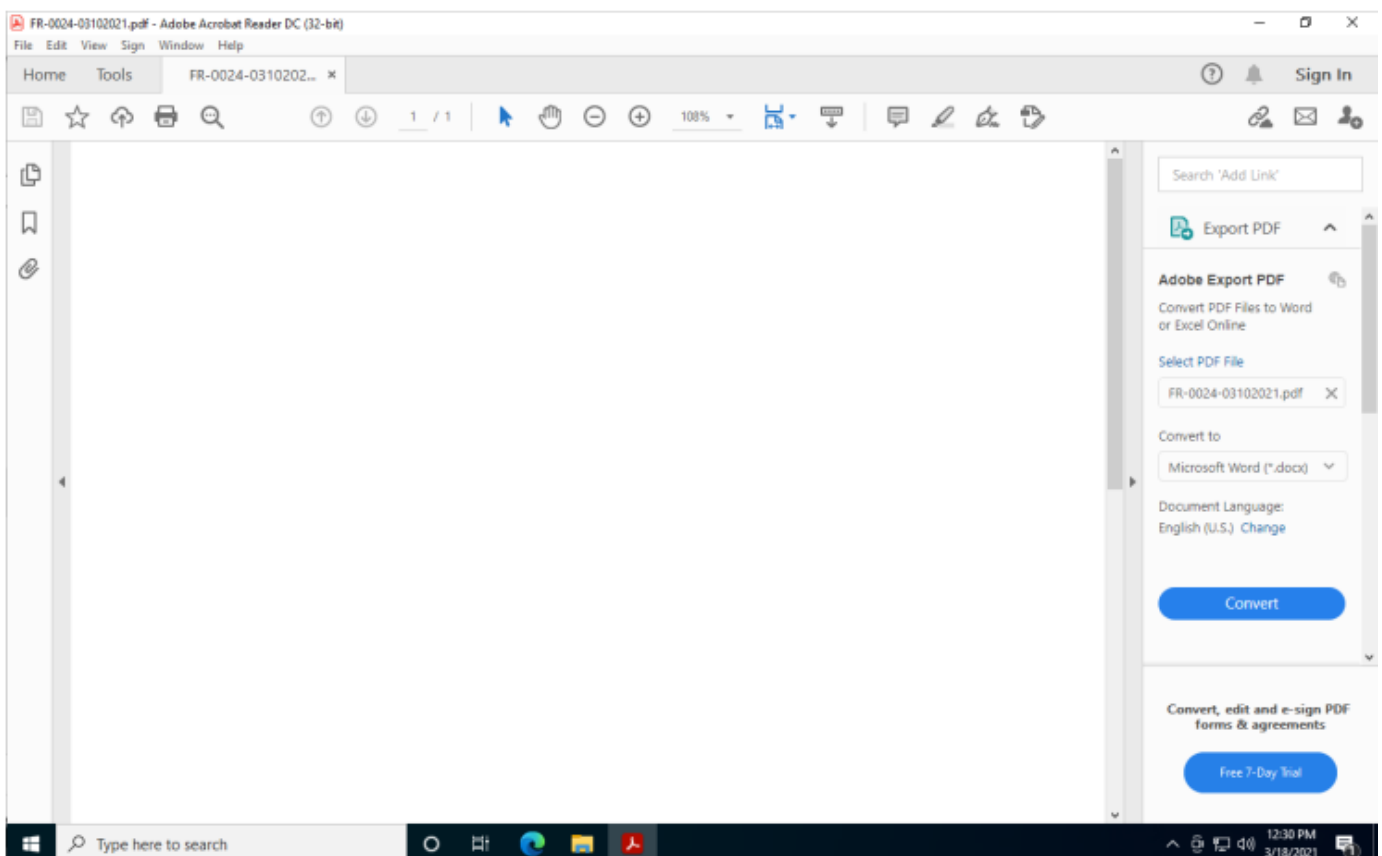
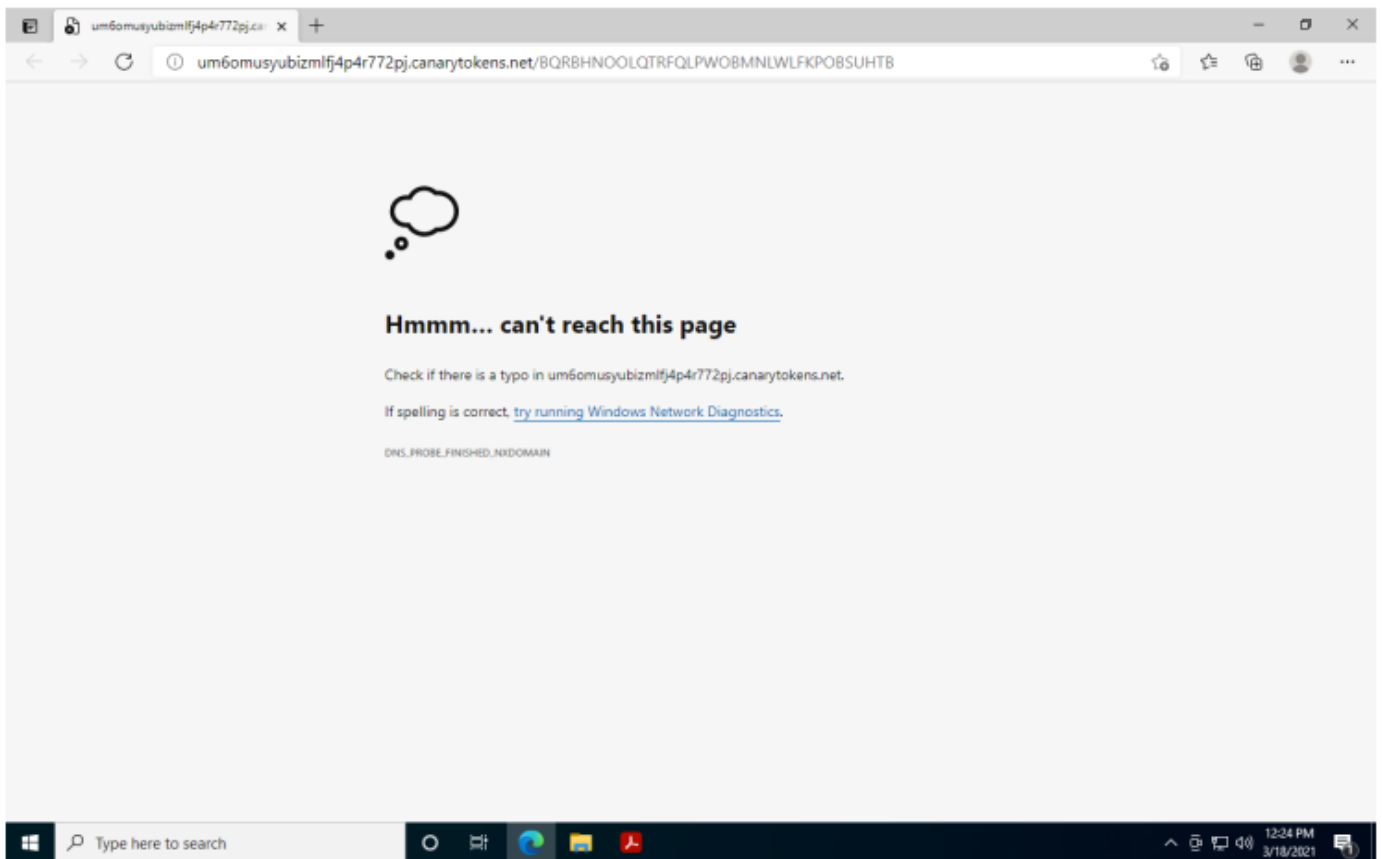
Now, assume an attacker got access to the folder and the attacker will open the file looking for PII, PCI, etc, information,



Note: Depending on the current Acrobat Reader settings, when you open the file automatically, it creates a DNS request to the server and it will show up as a pop-up window requesting you to allow or not the connection. Allowing this request will trigger the alert, however, in case you already have that setting as “allow”, it will automatically trigger the alert.



“here an attacker probably will identify that something is really strange...” however if the setting is already set, it will not pop-up any request window, so, the attacker only will see the new tab window with the request.



#analysis

Once the alert was triggered you will receive a notification depending the settings you selected, (email, SMS, etc.) for this specific scenario [.pdf file] we have two options, “email address or web-hook URL”, previously we selected “email address” so, let’s check the notification we got.

Canarytoken triggered

ALERT

A DNS Canarytoken has been triggered by the Source IP 181.193.218.●. Please note that the source IP refers to a DNS server, rather than the host that triggered the token.

Basic Details:

Channel	DNS
Time	2021-03-18 19:30:18 (UTC)
Canarytoken	um6omusyubizmlfj4p4r772pj
Token Reminder	C:\vault has been pwned !
Token Type	adobe_pdf
Source IP	181.193.218.●

Canarytoken Management Details:

Manage this Canarytoken [here](#)

More info on this token [here](#)

Powered by: [Thinkst Canary](#)

Here we have some valuable information, the first and most important! File and network share was compromised... Analyzing further the canary token alert we can conclude the following,

- Source IP that accessed the file / GEO (possible public IP, it depends based on configuration)
- Time when it was accessed
- Reminder, brief description of what was compromised
- Token type in case description does not help !

Checking, "more info on this token" section you have more information and a possible location of the attacker, let's double check

Incident Map

Incident List

Export ▾

Date: 2021 Mar 18 19:30:18.971862 (UTC) IP: 181.193.218.1 Channel: DNS

Geo Info	
Country	CR
City	San Pedro
Region	San José
Organisation	AS11830 Instituto Costarricense de Electricidad y Telecom.

Tor

Known Exit Node	False
-----------------	-------

Basic Info

Memo	C:\vault has been pwned !
------	---------------------------

Date: 2021 Mar 18 19:30:18.810682 (UTC) IP: 181.193.218.1 Channel: DNS

Date: 2021 Mar 18 19:30:18.676759 (UTC) IP: 181.193.218.1 Channel: DNS

This section adds some information related to the geolocation, ISP, if it is currently using a Tor Node or not etc.

Exist different ways to implement decoys using Canary Tokens (.pdf files, word files, networks shares, API keys, database usage, QR code) and more, it will depends the current scenario but it is a really good way to known that something bad is happening so we can take actions at same time.