

【Honeypot】canarytokens

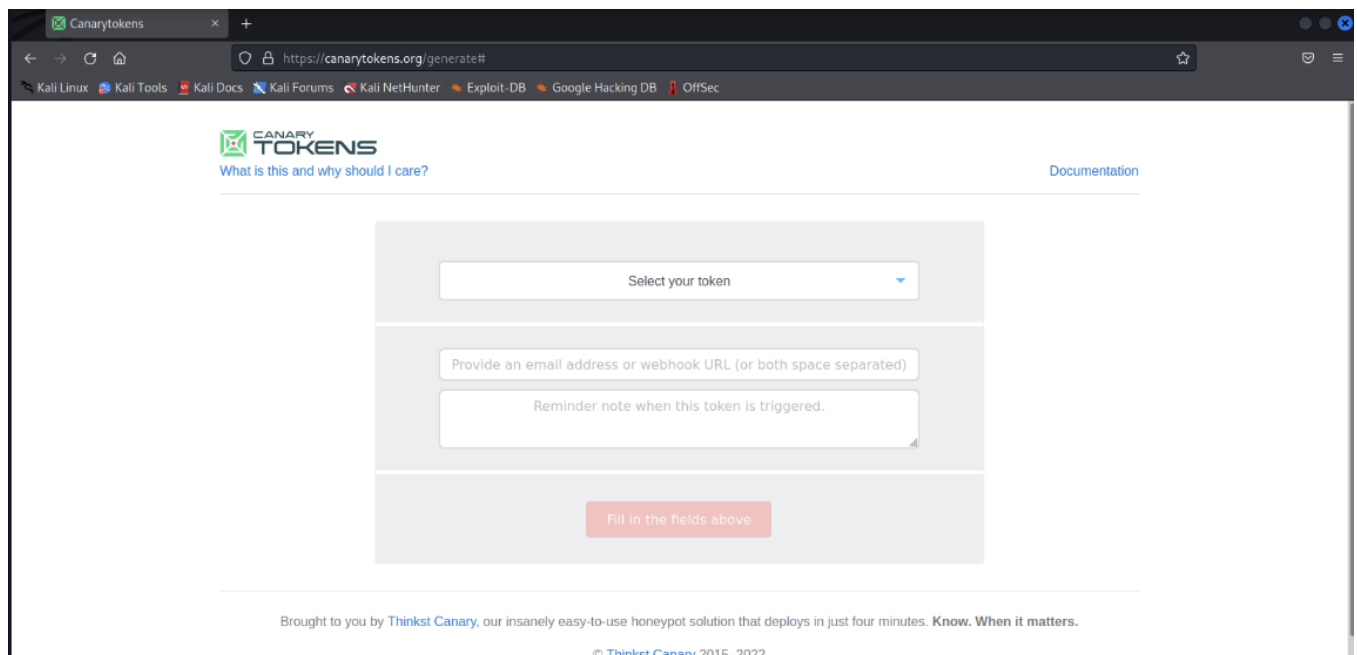
<https://canarytokens.org/generate>

我們將使用Canarytokens，這是一個免費的網絡服務，生成帶有嵌入式令牌的鏈接，我們將其發送給目標。當目標在瀏覽器中打開鏈接時，我們將獲得有關其瀏覽器、IP地址和操作系統的信息。有了這些信息，我們可以確認目標正在運行Windows，並確定我們應該嘗試進行HTA客戶端攻擊。

在創建我們的追蹤鏈接之前，讓我們簡要討論在這種情況下我們可以使用的前設。前設以特定的方式框定一種情況。在大多數情況下，我們不能要求目標（一個陌生人）在任意電子郵件中點擊鏈接。因此，我們應該嘗試創建上下文，可能是利用目標的工作角色。

例如，假設我們的目標在財務部門工作。在這種情況下，我們可以說我們收到了一張發票，但其中包含了財務錯誤。然後，我們提供一個鏈接，我們說這個鏈接打開了一張突出顯示錯誤的發票的截圖。這當然就是Canarytoken鏈接。當目標點擊鏈接時，IP日誌記錄器會創建目標的指紋，為我們提供準備客戶端攻擊所需的信息。目標在點擊鏈接時將總是收到一個空白頁面。

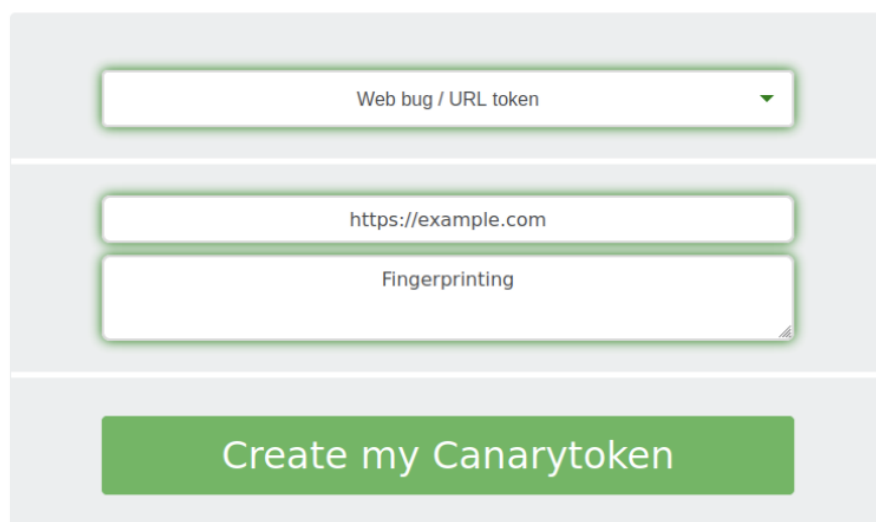
有了我們的前設，讓我們在Canarytokens中創建我們的鏈接，通過在瀏覽器中加載令牌生成頁面。圖3顯示了該站點的首頁。



網頁表單為我們提供了一個下拉菜單，以選擇我們要創建的追蹤令牌的類型。我們必須輸入一個電子郵件地址，以獲得有關追蹤令牌的警報，或者提供一個Webhook URL。在這個例子中，我們將從下拉菜單中選擇Web bug / URL令牌，輸入https://example.com作為Webhook URL，然後輸入Fingerprinting作為評論。輸入完這些信息後，我們將點擊"Create my Canarytoken"。

 **CANARY
TOKENS**
[What is this and why should I care?](#)

[Documentation](#)



一個新的頁面出現，上面有一個藍色的窗口，顯示我們的網絡令牌現在已經啟動：



Your Web token is active!

Copy this URL to your clipboard and use as you wish:

`http://canarytokens.com/tags/articles/static/7u3`



Remember, it gets triggered whenever someone requests the URL.

If the URL is requested as an image (e.g. ``) then a 1x1 image is served. If the URL is surfed in a browser than a blank page is served with fingerprinting Javascript.

Ideas for use:

- In an email with a juicy subject line.
- Embedded in documents.
- Inserted into canary webpages that are only found through brute-force.
- This URL is just an example. Apart from the hostname and the actual token (the random string), you can change all other parts of the URL.

這個頁面包含我們可以用來指紋識別目標的追蹤鏈接。它還提供了如何讓目標點擊該鏈接的想法。

接下來，讓我們點擊頁面右上角的"Manage this token"，這將帶我們進入令牌設置頁面。

Token settings

Webhook reporting
https://example.com

ON

Browser scanner

Runs Javascript fingerprinting when the token is browsed

ON

Here's your Web token:

`http://canarytokens.com/tags/articles/static/7u3`

This token has not been triggered yet

We hope you are enjoying the free version of Canarytokens!

For more (non-public) tokens, support, mass-deployment-tools and better management of your deployed tokens, check out our commercial Canarytoken offering at <https://canary.tools/canarytokens>.

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

該令牌尚未觸發，但這是預期的，因為我們剛創建它。在這個例子中，我們將保持默認設置，因為我們只是對目標進行指紋識別，而不是將令牌嵌入到Web應用程序或網頁中。

接下來，讓我們點擊右上角的"History"。歷史頁面會顯示所有點擊我們Canarytoken鏈接的訪問者以及有關受害者系統的信息。截至目前，列表是空的。

History for Canarytoken:
7u303y650trp4891zfnwrpszl

Heads Up! Click the incident items for more info.



Incident List is Currently Empty

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

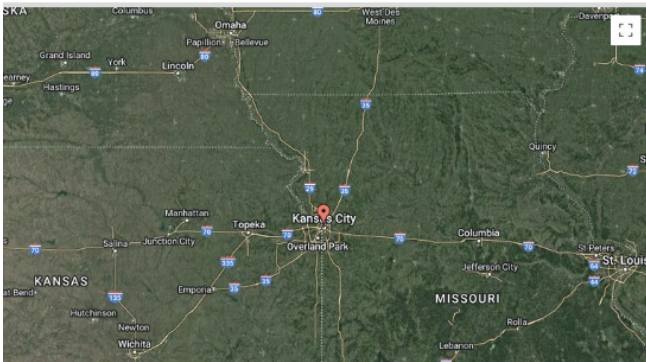
© Thinkst Canary 2015–2022

讓我們假設我們已經在我們的前設背景下說服了我們的受害者，讓他們通過電子郵件訪問Canarytoken鏈接。當受害者點擊我們的鏈接時，他們的瀏覽器中將顯示一個空白頁面。同時，我們的歷史列表中出現了一條新的項目：

History for Canarytoken: 7u303y650trp4891zfnwrpszl

Heads Up! Click the incident items for more info.

Incident Map

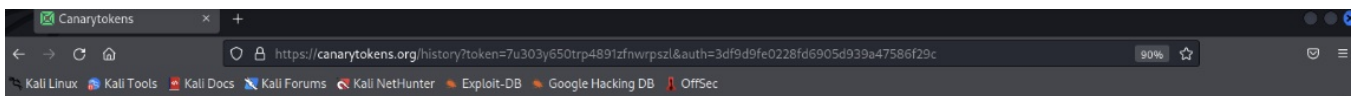


Incident List

Export

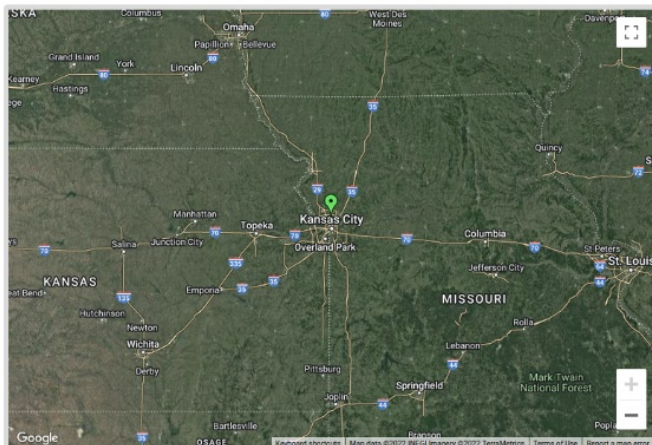
Date: 2022 Apr 29 17:47:01.239633 (UTC) IP: 38.146.5.222 Channel: HTTP

左側的地圖顯示了受害者的地理位置。我們可以點擊條目以獲取更多信息。



Heads Up! Click the incident items for more info.

Incident Map



Incident List

Export

Geo Info

Country	US 🇺🇸
City	Kansas City
Region	Missouri
Organisation	AS13737 INCX Global, LLC



Known Exit Node False

Basic Info

Memo	Fingerprinting
useragent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36

詳細視圖的上半部分提供了有關受害者位置的信息，並嘗試確定組織名稱。還顯示了受害者瀏覽器發送的用户代理。從用户代理本身，我們可以推斷目標的操作系統和瀏覽器。但是，用户代理可以被修改，並且並非始終可靠的信息來源。

在這個例子中，受害者的用户代理暗示他們在64位的Windows 10系統上使用Chrome瀏覽器。我們還可以使用在線用户代理解析器，解釋用户代理並為我們提供更易讀的結果。

讓我們滾動到瀏覽器區域。

Browser	
mimetypes	Portable Document Format;pdf,application/pdf Portable Document Format;pdf;text/pdf
vendor	Google Inc.
language	en-US
enabled	True
installed	True
platform	Win32
version	101.0.4951.41
os	Windows
browser	Chrome

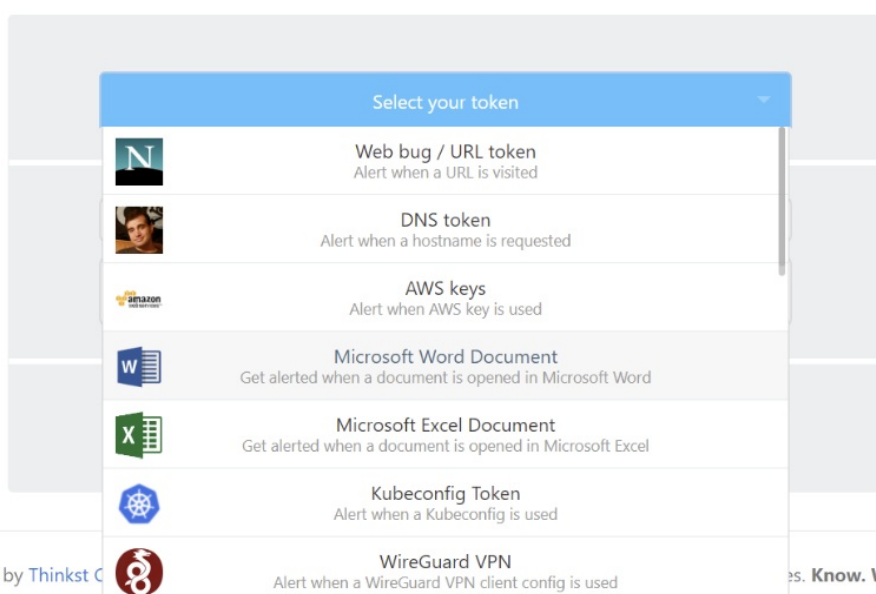
圖10向我們顯示了有關受害者瀏覽器的其他信息。這些信息不來自用戶代理，而是來自嵌入在Canarytoken網頁中的JavaScript指紋識別代碼。這些信息比用戶代理的信息更精確可靠。這再次表明目標正在Windows上運行Chrome。

Canarytoken服務還提供其他指紋識別技術。讓我們返回到Canarytokens的主頁，討論這些技術。



What is this and why should I care?

[Documentation](#)



下拉菜單提供了在Word文檔或PDF文件中嵌入Canarytoken的選項，這將使我們在受害者打開文件時獲得信息。此外，我們還可以將其嵌入到圖像中，這將在圖像被查看時通知我們。

我們還可以使用像Grabify這樣的在線IP日誌記錄器，或者使用JavaScript指紋識別庫，如fingerprint.js。

在這一節中，我們展示了一種有效的指紋識別技術，揭示了有關目標系統的關鍵信息。這是客戶端攻擊的關鍵第一步。雖然我們的目標是確定目標是否運行Windows，並啟用了Internet Explorer或Microsoft Edge，但我們只能確定受害者在Windows上運行Chrome。在這種情況下，我們應該使用不同的客戶端攻擊向量，或者更改我們的前設，例如建議該截圖只能在Internet Explorer或Microsoft Edge中查看。

參考:

<https://bookstack.treemanou.com/books/treemanoscp/page/ch11-client-side-attacks#bkmrk-11.1.2-client-finger>

[Day 12] 30天蜜罐品嘗：蜜罐非罐之四 Canarytoken

若是想設置自己的canarytoken伺服器，可以參考以下github連結

<https://github.com/thinkst/canarytokens>

他們也有自己開源的模組化honeypot，安裝後只需要改變設定便可以在同一台honeypot上模擬Linux Web Server, Windows Server MySQL Server 和MSSQL Server，可以參考以下連結

<https://github.com/thinkst/opencanary>

🕒修訂版本 #3

★由 treeman 建立於 11 🎮🎮🎮🎮 2023 01:26:12

🔪由 treeman 更新於 7 🎮@🎮🎮 2024 19:30:26