




# MISP Expansion CIRCL Internship



Tuteurs  
Université : Mme Herrmann  
Entreprise : Mr Dulaunoy

Morisot Anselme  
2021



# Introduction

**SECURITY**  
**MADEIN.LU** —



**circl.lu**



**cases.lu**



**c-3.lu**



*Computer Incident  
Response Center  
Luxembourg*

# Plan

- I) MISP
- II) Contenu d'une extension
- III) Contenu de MISP Expansion
- IV) La Sécurité de l'extension





# MISP

## Threat Sharing

*Malware Information Sharing Platform*

# MISP

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions API

★ MISP Anselme Morisot Log out




























Welcome! Last login was on Mon, 16 Aug 21 13:25:01 +0000

## Local organisations, both local and remote

« previous 1 2 3 4 5 6 7 next » last »

Local organisations Known remote organisations All organisations

Enter value to search Filter ✕

ID	Name	UUID	Description	Nationality	Sector	Type	Contacts	Added by	Local	Users	Restrictions	Actions
515		582ae291-250c-4107-9a24-4cf9950d210f							✓	7		  
57		55f6ea60-ed28-4ae5-a52e-42fd950d210f							✓	1		  
288		56b35512-11ec-46d2-b530-c9af950d210f							✓	1		  
1818		fb7b0ebb-c205-4096-9ab3-f8c1637cbdd			Software	Private			✓	5		  
311		56dd31dc-e278-46ac-b3ad-42c2950d210f							✓	2		  
1694		af4e6695-00d7-4fe1-a4b4-d89cd286f8dd			Security	Private			✓	1		  
1258		5d2c12ba-0744-4ca2-9d2f-4695950d210f			Security	Private			✓	1		  
702		590b1f41-f270-43fd-8bed-bd3d950d210f							✓	2		  
97		55f6ea62-9a0c-453b-88f4-4825950d210f							✓	1		  

# MISP

## REST client

Bookmarked queries

Query History

HTTP method to use

POST

Relative path to query

/attributes/restSearch

☐ Bookmark query

☒ Show result ☐ Skip SSL validation

HTTP headers

Authorization:

Accept: application/json

Content-type: application/json

HTTP body

```
1 {
2   "returnFormat": "mandatory",
3   "page": "optional",
4   "limit": "optional",
5   "value": "optional"
6 }
```

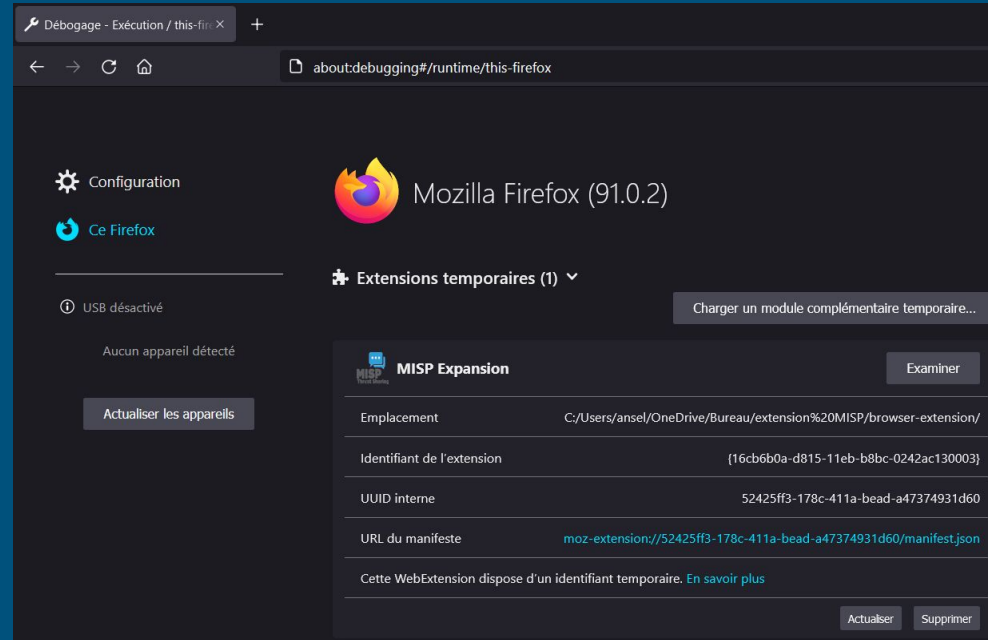
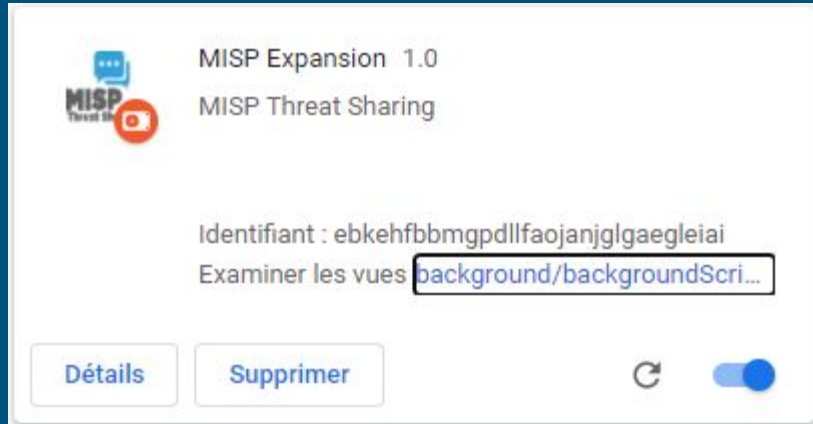
Fill out the JSON template above, make sure to replace all placeholder values. Fields with the value "optional" can be removed.

Run query

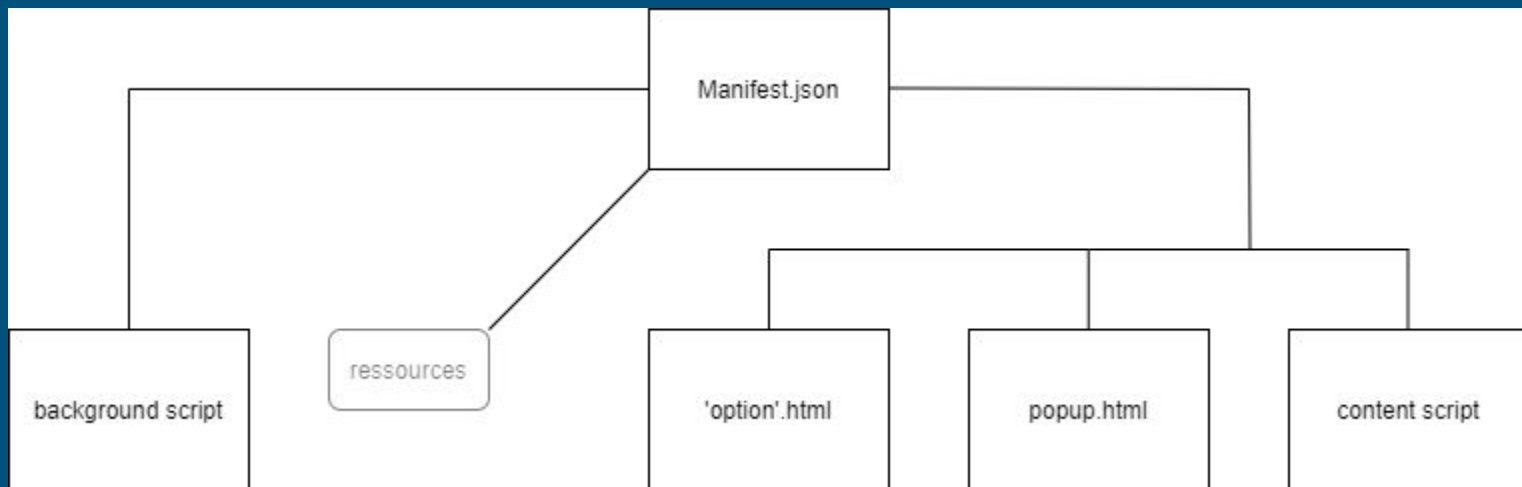
Raw JSON HTML Download

```
{
  "response": {
    "Attribute": [
      {
        "id": "1819446",
        "event_id": "13983",
        "category": "Network activity",
        "type": "hostname",
        "to_ids": false,
        "uid": "94242d73-488f-4947-a76e-ece0556436bf",
        "timestamp": "1551476939",
        "distribution": "5",
        "comment": "",
        "sharing_group_id": "0",
        "deleted": false,
        "disable_correlation": false,
        "object_id": "23858",
        "object_relation": "hostname",
        "first_seen": null,
        "last_seen": null,
        "value": "www.facebook.com",
        "Event": {
          "org_id": "2",
          "distribution": "3",
          "id": "13983",
          "info": "Processed phishtank list",
          "orgc_id": "2",
          "uuid": "5c73eba9-6fac-424c-9ceb-446a950d210f"
        },
        "Object": {
          "id": "23858",
          "distribution": "5",
          "sharing_group_id": "0"
        }
      }
    ]
  }
}
```

# Les extensions



# Les extensions





# Les extensions

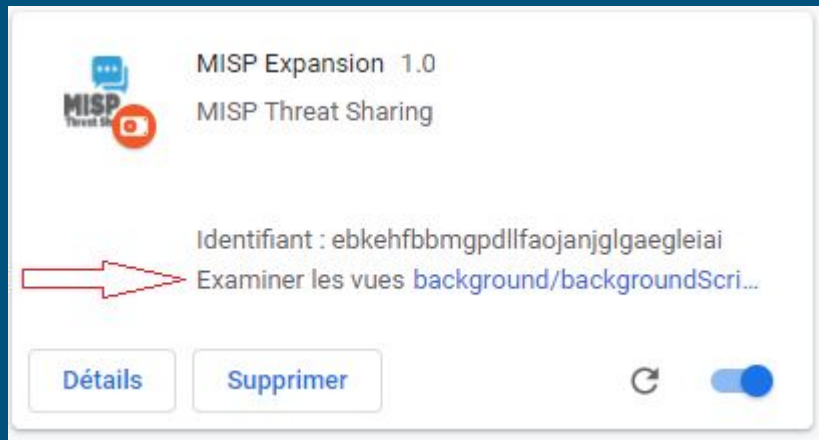
## Le manifeste

- Lie les différents éléments de l'extension
- Est obligatoire

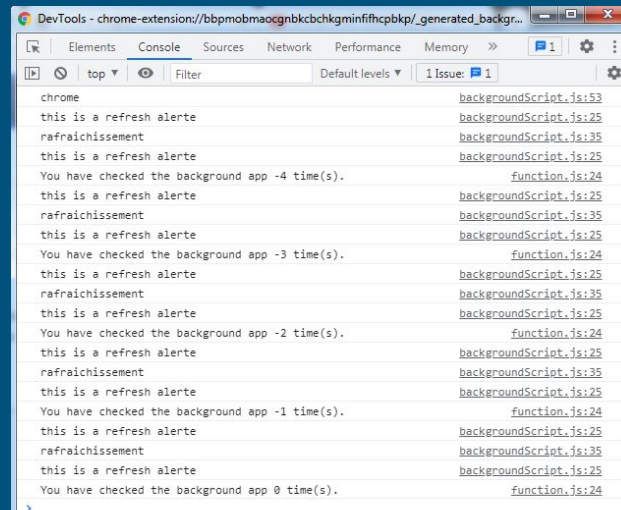
```
{
  "name": "__MSG_extensionName__",
  "version": "1.0",
  "description": "__MSG_extensionDescription__",
  "manifest_version": 2,
  "options_ui": {
    "page": "./option/option.html",
    "browser_style": true,
    "chrome_style": true,
    "open_in_tab": true
  },
  "icons": {
    "16": "resources/icon16.png",
    "48": "resources/icon48.png",
    "128": "resources/icon128.png"
  },
  "browser_action": {
    "default_icon": "resources/icon16.png",
    "default_title": "__MSG_extensionTitle__"
  },
  "permissions": [
    "contextMenus",
    "storage",
    "notifications",
    "<all_urls>",
    "tabs"
  ],
  "background": {
    "page": "./background/backgroundScript.html",
    "persistent": true
  },
  "browser_specific_settings": {
    "gecko": {
      "id": "{16cb6b0a-d815-11eb-b8bc-0242ac130003}"
    }
  },
  "default_locale": "en"
}
```

# Les extensions

## Le script d'arrière plan



Exécuté tant que le navigateur  
est ouvert



### Use of Alarm API.

cpt defined to -5 on extension install.

Each 1 minutes there is a refresh alarm saying the next minutes there is an other alarm, set an other refresh alarm and also a refreshment alarm if not already created at 2 minutes.



So in each row (2 minutes) the refresh alarm (one per minute) and refreshment alarm (one per 2 minutes) are triggered. (1 time refreshment alert and 2 times refresh alert).

When refreshment alert is triggered,  $cpt = cpt + 1$ .

if  $cpt = 5$  then  $cpt = -1$

# Les extensions

## Les options

Description	MISP Threat Sharing
Version	1.0
Taille	< 1 Mo
Identifiant	ebkehfbmgpdlfaojanjlgaeleial
Examiner les vues	<ul style="list-style-type: none"><li><a href="#">background/backgroundScript.html</a></li></ul>
Autorisations	<ul style="list-style-type: none"><li>Consulter votre historique de navigation</li><li>Afficher les notifications</li></ul>
Accès au site	Autorisez cette extension à lire et à modifier toutes vos données sur les sites Web que vous consultez : ?
	<p><input type="radio"/> En cas de clic</p> <p><input type="radio"/> Sur des sites spécifiques</p> <p><input checked="" type="radio"/> Sur tous les sites</p>
Autoriser en navigation privée	Avertissement : Google Chrome ne peut pas empêcher les extensions d'enregistrer l'historique de votre navigation. Pour désactiver cette extension en mode navigation privée, désélectionnez cette option. <input type="checkbox"/>
Autoriser l'accès aux URL de fichier	<input checked="" type="checkbox"/>
Recueillir les erreurs	<input checked="" type="checkbox"/>
Options d'extension	 

# Les extensions

## Le script de contenu

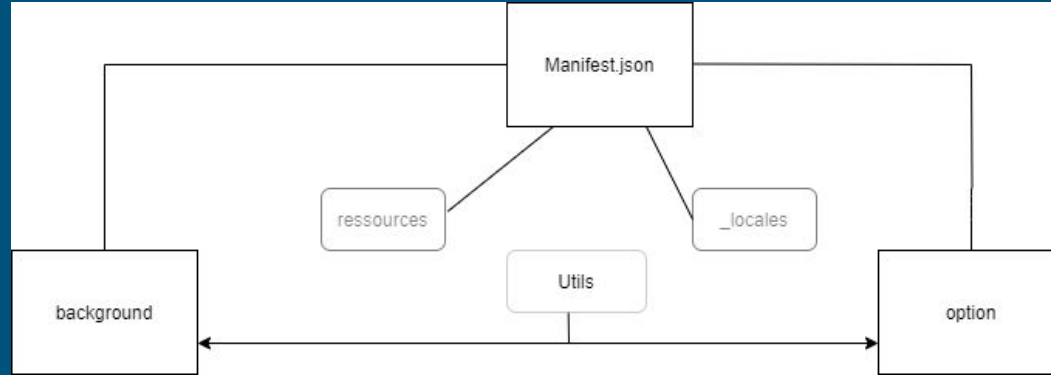
- S'exécute uniquement sur une ou un ensemble de pages
- Doit être indiqué ainsi que son url d'utilisation dans le manifest.json
- APIs utilisables limitées pour des raisons de sécurité :
  - Accès au storage
  - Accès à l'envoi de messages
  - Accès aux fonctions de Runtime (effet sandbox) -> sandbox avec Manifest V3
- Toutes les API sont utilisables dans une fonction Runtime

# Les extensions

## La fenêtre popup

- S'exécute uniquement lors du click sur le browser action du navigateur et est existant tant que la popup est ouverte
- Défini dans le manifest.json via browser ou page action (si fonctionnelle par page ou n'importe quand)
- Même contraintes que les scripts de contenu

# MISP Expansion



## Background



## Options

- Gère la sélection de l'utilisateur en continu
- Appel la fonction de fetch à MISP et génère l'affichage de la réponse
- Gère l'initialisation de l'extension

- Gère les options des requêtes fetch
- Gère les credentials de l'utilisateur
- Permet à l'utilisateur de définir les précédents points

Chaque partie est gérée par une page HTML, permettant d'utiliser plusieurs fichiers javascript ainsi que d'ajouter une règle CSP pour chaque parties

# MISP Expansion

Retour	Alt+Gauche
Avancer	Alt+Droite
Actualiser	Ctrl+R
Enregistrer sous...	Ctrl+S
Imprimer...	Ctrl+P
Caster...	
 Créer un code QR pour cette page	
Traduire en English	
 Rechercher l'url de la Page	
Afficher le code source de la page	Ctrl+U
Inspecter	

MISP Expansion Advanced Response

**<https://www.facebook.com/>**

**<https://misppriv.circl.lu>**

Nombre d'événements dans la requête: 23

Nombre d'événements maximum affichés: 100

**Evenement : 1**

Nombre d'attributs dans l'événement: 18

Nombre d'objets dans l'attribut Event: 6

<https://misppriv.circl.lu/events/view/57dfeabb-fb00-4314-a487-4c6b950d210f>

event\_info: hacked sites - 2016-09-19 - origin: pastebin.com/fbNHdaHF

UUID: 57dfeabb-fb00-4314-a487-4c6b950d210f

id548742

event\_id: 4940

**Evenement : 2**

Nombre d'attributs dans l'événement: 19

Nombre d'objets dans l'attribut Event: 6

<https://misppriv.circl.lu/events/view/57dfeabb-fb00-4314-a487-4c6b950d210f57dfeabb-fb00-4314-a487-4c6b950d210f>

event\_info: hacked sites - 2016-09-19 - origin: pastebin.com/fbNHdaHF

UUID: 57dfeabb-fb00-4314-a487-4c6b950d210f

id548742

event\_id: 4940

# Sécurité

---

- Guide des Bonnes Pratiques
- Content Security Policy personnalisées



# Content Security Policy

---

- Permet de définir les niveaux d'autorisations des éléments du web (Pages HTML, serveur, ...) via des règles
- Default-src permet de définir tous les éléments en une fois
- Les règles sont définies avec 'none' 'self' '\*' ou une liste d'urls
- D'autres règles telles que inline-safe pour les scripts ou les styles HTML
- CSP active par défaut dans une extension avec \*
- Règles inline-script & unsafe-eval appliquées automatiquement
- Ressources si indiquées dans le manifest

# Content Security Policy

---

- Prévenir les menaces : default-src 'none' puis ajuster au cas par cas
- script-src 'self' pour que l'extension fonctionne

Autorisations entre les parties de notre extension pas uniformes  
-> Impossible de définir une règle par défaut dans le manifeste  
CSP manifest > CSP des pages

# Content Security Policy

---

Réponse html

```
<meta http-equiv="Content-Security-Policy" content="default-src 'none'">
```

Script d'arrière plan html & Visualisation d'instances html

```
<meta http-equiv="Content-Security-Policy" content="default-src 'none'; connect-src *; script-src 'self'">
```

Autre pages html

```
<meta http-equiv="Content-Security-Policy" content="default-src 'none'; script-src 'self'">
```

# Guide PS

- Inline script & unsafe eval ✗
- innerHTML ✗
- home made gui ✗
- Storage : stockées en clair

DOM functions ✓

API ✓

# Guide PS

## APIs



- Communes aux différents navigateurs
- Gérées par des groupes qualifiés et fiables (sécurité)
- Sécurisées

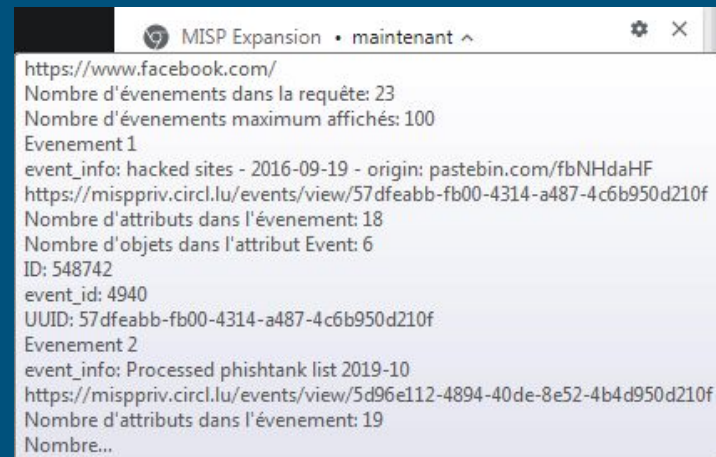
Ne pas faire n'importe quoi !

# Guide PS

## APIs



Retour	Alt+Gauche
Avancer	Alt+Droite
Actualiser	Ctrl+R
Enregistrer sous...	Ctrl+S
Imprimer...	Ctrl+P
Caster...	
 Créer un code QR pour cette page	
Traduire en English	
 Rechercher l'url de la Page	
Afficher le code source de la page	Ctrl+U
Inspecter	



# Guide PS

innerHTML / DOM functions

innerHTML n'échappe pas les caractères

```
htmlElement.innerHTML = '<td id="'+INSTANCE+j+'"> value</td>'
```



```
value = "</td><script type='module' src='./somewhere/the_malicious_content.js'></script>";
```

```
htmlElement.innerHTML = '<td id="'+INSTANCE+j+'"></td>';  
document.getElementById(TABLE).appendChild(htmlElement);  
document.getElementById(INSTANCE+j).textContent = value;
```

```
htmlElement = document.createElement("td");  
htmlElement.setAttribute("id", INSTANCE+j);  
document.getElementById(TABLE).appendChild(htmlElement);  
document.getElementById(INSTANCE+j).textContent = value;
```



# Guide PS

Storage en clair  
Données sensibles ✖

Fonction de crypto : XOR avec un salt (42 chars) sur la clé et l'url





# Conclusion