


# Faux positifs dans la cybersécurité



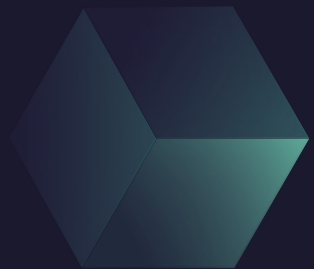


Qu'est-ce qu'un faux positif ?

Quels sont les types de faux positifs ?

Quels sont les impacts ?





Qu'est-ce  
qu'un faux  
positif ?



Sécurité Windows



## Protection contre les virus et menaces

### Menaces détectées

L'antivirus Microsoft Defender a détecté des menaces. Obtenir des détails.



### Menace bloquée

04-09-22 11:31

Grave



Détecté : Behavior:Win32/Hive.ZY

État : Supprimé

Une menace ou une application a été supprimée de cet appareil.

Date : 04-09-22 11:31

Détails : Ce programme est dangereux et il exécute des commandes émanant d'une personne malveillante.

### Éléments affectés :

behavior: pid:11404:74439979291537

[En savoir plus](#)

Actions



## Les Antivirus

- McAfee Faux Positif svchost.exe (W32/Wecorl.a)
- AVG qui a détecté C:\Windows\system32\user32.dll en Trojan Horse PSW.Banker4.APSA et AVG
- Trend-Micro qui a détecté le fichier C:\Windows\system32\svchost.exe
- Avast! qui a détecté C:\Windows\system32\kernel32.dll
- Windows defender Behavior:Win32/Hive.ZY
- Etc...



[Home](#) [How It Works](#)



**leblogduhacker.fr**

Caution. We tested this link and found it might send your personal information to people online who can use it to access your financial information, or steal your identity.

Website Category:  
Phishing, Blogs/Wiki

Want us to take another look at the rating for this link?

[Request a Review](#)

Site Safety Information for leblogduhacker.fr

# Les URLs

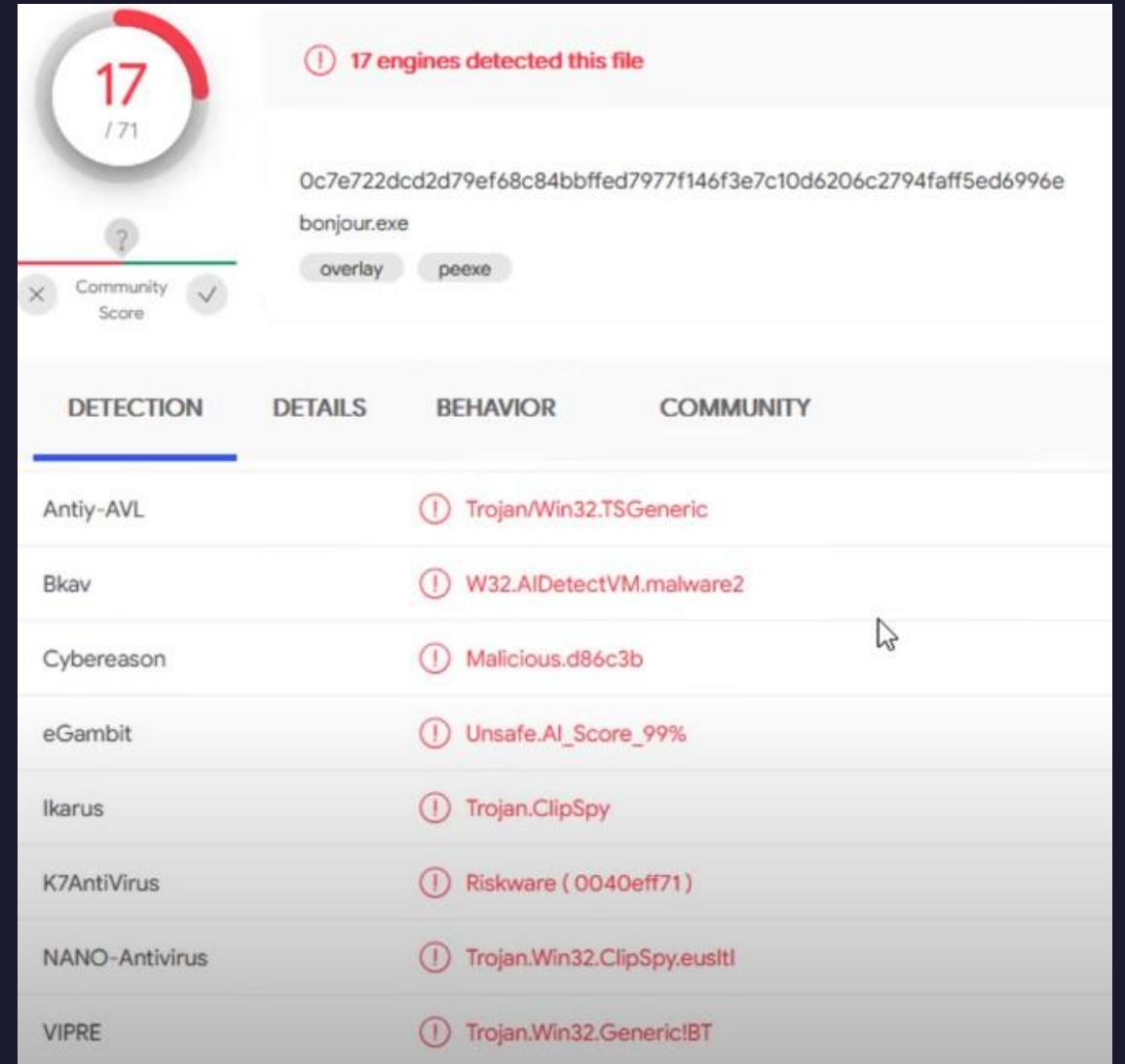
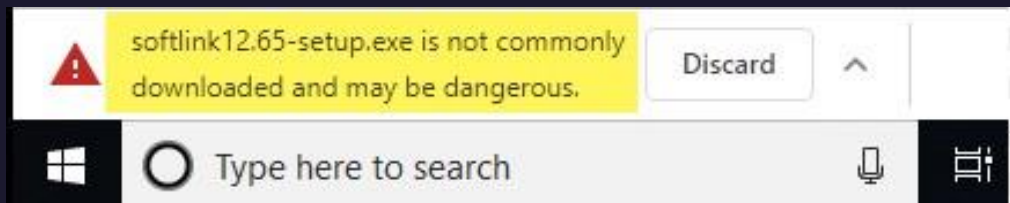
- Phishing
- Base de données jQuery instable
- Liste noire
- Site détecté malveillant
- Etc...



# Les Téléchargements

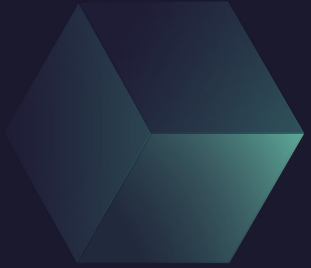
Bonjour en langage C

```
1  #include <stdlib.h>
2  #include <stdio.h>
3
4  int main() {
5
6      printf("Bonjour");
7  }
```



The VirusShare analysis interface for the file "fichier.exe" (MD5: 0c7e722dcd2d79ef68c84bbffed7977f146f3e7c10d6206c2794faff5ed6996e). The interface shows a "17 / 71" engine detection score and a "Community Score" section. The "DETECTION" tab is active, displaying a list of engines and their detection results.

Engine	Detection Result
Antiy-AVL	Trojan.Win32.TSGeneric
Bkav	W32.AIDetectVM.malware2
Cybereason	Malicious.d86c3b
eGambit	Unsafe.AI_Score_99%
Ikarus	Trojan.ClipSpy
K7AntiVirus	Riskware ( 0040eff71 )
NANO-Antivirus	Trojan.Win32.ClipSpy.eusltl
VIPRE	Trojan.Win32.Generic!BT



Quels sont les  
types de faux  
positifs ?







Faux positif par signature

Cette fausse détection peut se produire lorsqu'un outil de cybersécurité détecte, au sein d'un objet non malveillant, une signature identique à celle d'un objet malsain connu.



Faux positif par comportement

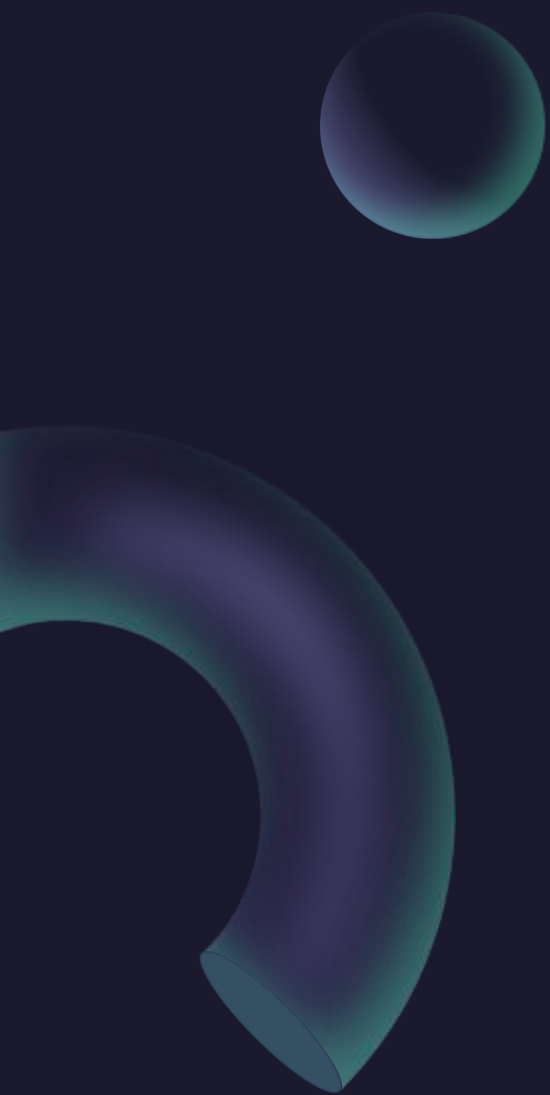
La majorité des solutions de sécurité ont plusieurs niveaux de protection et intègrent plusieurs technologies de détection des parasites.



Faux positif crapuleux



Le faux positif crapuleux est tout simplement le fait de faire croire que la machine a été infectée par des parasites. Des personnes tentent en effet de semer le doute en développant de nombreux sites internet piégés.



Quels sont les  
impacts ?



**« Une attaque notable d'Emotet sur la ville d'Allentown, en Pennsylvanie, nécessita une aide directe de l'équipe de réponse aux incidents de chez Microsoft pour le nettoyage, et elle aurait coûté plus de 1 million de dollars à corriger. »**

- Visibilité
- La réputation
- Crédibilité
- Financier
- Confiance
- Moral des personnes
- Etc...



Merci à tous !  
Des questions ?

