



# Une décennie d'outils dans la sécurité de l'information

23 novembre 2019

**Thomas DEBIZE**

UNLOCK  
YOUR BRAIN  
22>23 NOV.



HARDEN  
YOUR SYSTEM  
2019 BREST

\$ whoami



**Thomas DEBIZE**

> <https://github.com/maaaaz>

**01**

Un peu de contexte

**02**

Les outils durant cette décennie

**03**

Des règles d'or pour un outil en or

**04**

En bref

**01**

Un peu de contexte

**02**

Les outils durant cette décennie

**03**

Des règles d'or pour un outil en or

**04**

En bref

# Un peu de contexte

Le domaine de la sécurité de l'information a énormément évolué durant cette **décennie**, notamment en matière **d'outillage**

De **vieux et doux rêves** devenus réalité

- Scanner **l'intégralité de l'espace IPv4** en quelques minutes/heures/jours
- Requêter facilement **diverses** sources d'information **OSINT**
- Compromettre facilement **de vastes infrastructures Windows** en entreprise
- **Fuzzer** tout et n'importe quoi
- **Stocker et casser** d'énormes bases de hash
- ...

Le **développement informatique** devenu quelque chose de **social**

- La communauté infosec **améliorant** ses **capacités** en développement
- Un **soin** et une volonté d'écrire des **outils ergonomiques**
- Des **événements dédiés** à l'outillage (Black Hat Arsenal)
- ➔ De **plus en plus** de passionnés produisant de plus en plus **d'outils de bonne qualité**

De plus en plus d'outils facilitant **l'attaque et la défense**

- De plus en plus de **reconnaissance** pour la Blue team
- Un passage de l'ère du **cassage**, vers celle de **la construction sécurisée**
- Une mise à profit de la **visualisation de données** à travers la **théorie des graphes**

# Un peu de contexte

Mais dans le même temps, nous continuons à utiliser massivement des outils *old school*

Author : Fyodor

---[ Phrack Magazine Volume 7, Issue 51 September 01, 1997, article 11 of 17

-----[ The Art of Port Scanning

-----[ Fyodor <fyodor@dhp.com>


[ Abstract ]

This paper details many of the techniques used to determine what ports (or similar protocol abstraction) of a host are listening for connections. These ports represent potential communication channels. Mapping their existence facilitates the exchange of information with the host, and thus it is quite useful for anyone wishing to explore their networked environment, including hackers. Despite what you have heard from the media, the Internet is NOT all about TCP port 80. Anyone who relies exclusively on the WWW for information gathering is likely to gain the same level of proficiency as your average AOLer, who does the same. This paper is also meant to serve as an introduction to and ancillary documentation for a coding project I have been working on. It is a full featured, robust port scanner which (I hope) solves some of the problems I have encountered when dealing with other scanners and when working to scan massive networks. The tool, nmap, supports the following:

- vanilla TCP connect() scanning,
- TCP SYN (half open) scanning,
- TCP FIN (stealth) scanning,
- TCP ftp proxy (bounce attack) scanning
- SYN/FIN scanning using IP fragments (bypasses packet filters),
- UDP recvfrom() scanning,
- UDP raw ICMP port unreachable scanning,
- ICMP scanning (ping-sweep), and
- reverse-ident scanning.

The freely distributable source code is appended to this paper.

# Un peu de contexte



## the hacker's choice

THC - Aus Erfahrung gut

[news](#) | [releases](#) | [papers](#) | [members](#) | [forums](#) | [links](#) | [contact](#) | [quiz](#) | [phun](#) | [misc](#) | [home](#)

### THE HACKER'S CHOICE

news  
releases  
papers  
members

Welcome to the official THC website. THC is a short form for "The Hacker's Choice". THC was founded in 1995 in Germany by a group of people involved in hacking, phreaking and anarchy. Through the years THC was joined by other experts and grew to probably Germany's best hacking group.



## THC Releases

Welcome to the THC release section. Below you will find the collection of THC software applications. It includes sophisticated network analysis and penetration test tools, cryptographic utilities that mimic fingerprint collisions or extrapolate credit card numbers and a lot of other interesting stuff for the security expert's pleasure.

### 🔗 THC-Hydra

Version: 4.1

Date: 2004-05-22

OS: Unix

Size: 168kb

🔗 Project website: [/thc-hydra](#)

THC-Hydra - the best parallized login hacker is available: for Samba, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more. Includes SSL support and is part of Nessus. VISIT THE PROJECT WEB SITE TO DOWNLOAD WIN32, PALM and ARM BINARIES! Changes: A very nice GTK2 GUI was added (thanks to snakebyte) and a few bugfixes.

## Un peu de contexte

### 2003 Top 75 Tools Results

*From:* Fyodor <fyodor () insecure org>

*Date:* Sun, 4 May 2003 00:33:30 -0700

Hello everyone,

Thanks for the fantastic response to the Nmap user survey! It is now closed, but recorded 1854 responses -- that blew away our goal of 1500 and is over 50% greater than the 2000 survey! I haven't analyzed all the questions/comments yet, but I did go through your recommended tools and create a most-loved list as I did in 2000. Thanks to the increased responses, I was able to expand the list from "Top 50" to

It is worth noting that almost half of the 2003 top 50 are new to the list. Congratulations to these rising stars:

GFI LANguard: A commercial network security scanner for Windows  
Ettercap: In case you still thought switched LANs provide much extra security  
Nikto: A more comprehensive web scanner  
Kismet: A powerful wireless sniffer  
SuperScan: Foundstone's Windows TCP port scanner  
Fport: Foundstone's enhanced netstat  
Network Stumbler: Free Windows 802.11 Sniffer  
N-Stealth: Web server scanner  
AirSnort: 802.11 WEP Encryption Cracking Tool  
NBTScan: Gathers NetBIOS info from Windows networks  
Cain & Abel: The poor man's L0phtcrack  
XProbe2: Active OS fingerprinting tool  
SolarWinds Toolsets: A plethora of network discovery/monitoring/attack tools  
THC-Amap: An application fingerprinting scanner  
OpenSSL: The premier SSL/TLS encryption library  
Honeyd: Your own personal honeynet  
Achilles: A Windows web attack proxy  
Brutus: A network brute-force authentication cracker  
Stunnel: A general-purpose SSL cryptographic wrapper  
Paketto Keiretsu: Extreme TCP/IP  
SPIKE Proxy: HTTP Hacking  
THC-Hydra: Parallized network authentication cracker



# Les questions qui ont donné naissance à cette étude

Dans la **myriade** d'outils créés durant cette décennie

- › Comment sont-ils **construits** ?
- › Où sont-ils **hébergés** ?
- › **Durant combien de temps** sont-ils maintenus ?
- › Sont-ils **vraiment de meilleure qualité** que les précédents ?

En bref, comment tout cela à **évolué** ?

**01**

Un peu de contexte

**02**

Les outils durant cette décennie

**03**

Des règles d'or pour un outil en or

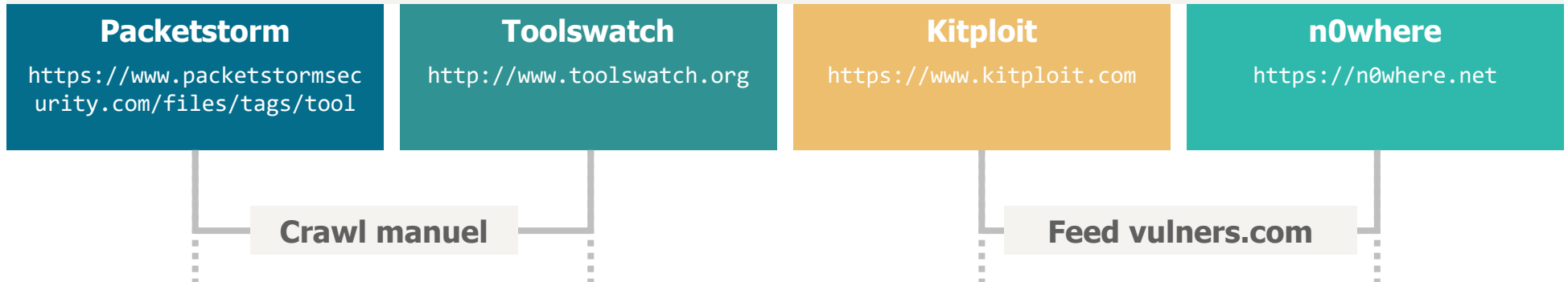
**04**

En bref

# Périmètre et limitations de l'étude

## Qu'ai-je fait ?

- Analyser les métadonnées de **4 sources majeures de publications d'outils**



## Comment ?

- Avec **Dataiku Data Science Studio free edition**. Un Microsoft Excel dopé aux technologies modernes
- Pour vous faire une idée : <https://www.dataiku.com/learn/portals/tutorials.html>

## Combien d'entrées ont été collectées ? Sur quelle période ?

Source	Nombre d'entrées	Période
Packetstorm	6872 entrées	janvier 1994 - octobre 2019
Toolswatch	1642 entrées	décembre 2010 - juin 2019
Kitploit	3331 entrées	décembre 2010 - octobre 2019
n0where	1052 entrées	juin 2010 - octobre 2019

# Merci **vulners.com**

**vulners.com** indexe de nombreuses sources d'informations de **l'écosystème infosec** et les expose comme **données structurées** via une **API gratuite**

- Blogs
- Flux de vulnérabilités, IOC, exploits
- Produits et vendeurs
- News
- ...

**Merci à eux !**



Archive	
GET	/archive/collection/ Get entire collection of bulletins in ZIP
GET	/archive/getsploit/ Get whole exploit database in ZIP
GET	/archive/distributive/ Get affected packages for specified OS in ZIP
GET	/archive/nasl/ Get NASL scripts in ZIP

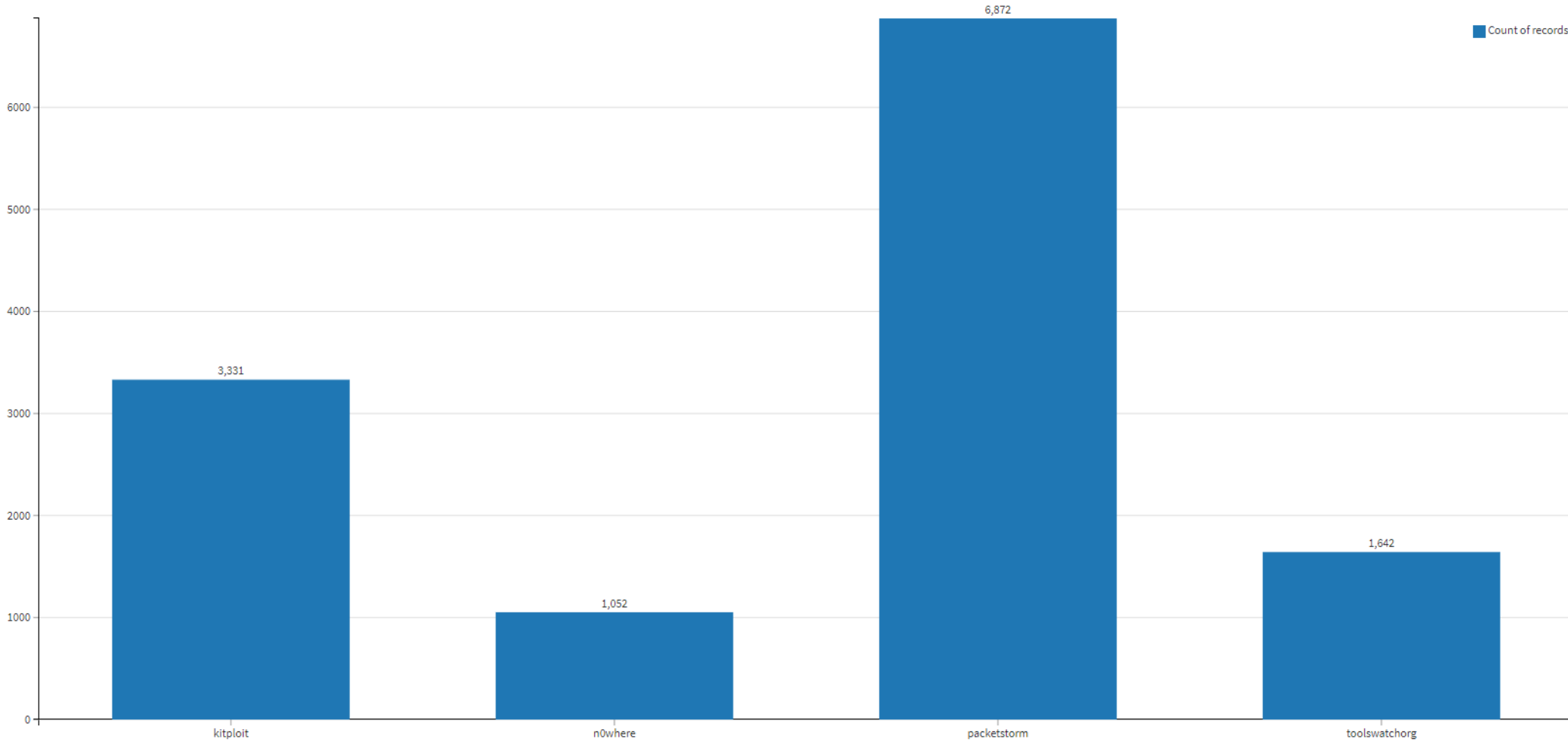
Tout d'abord, le jeu de données (*dataset*) source,  
alias "la cause de tous les biais de l'étude"

# Distribution des entrées par source depuis 1994

Run: In DSS

Count of records per source since 1994 until 2019 

12897 records  





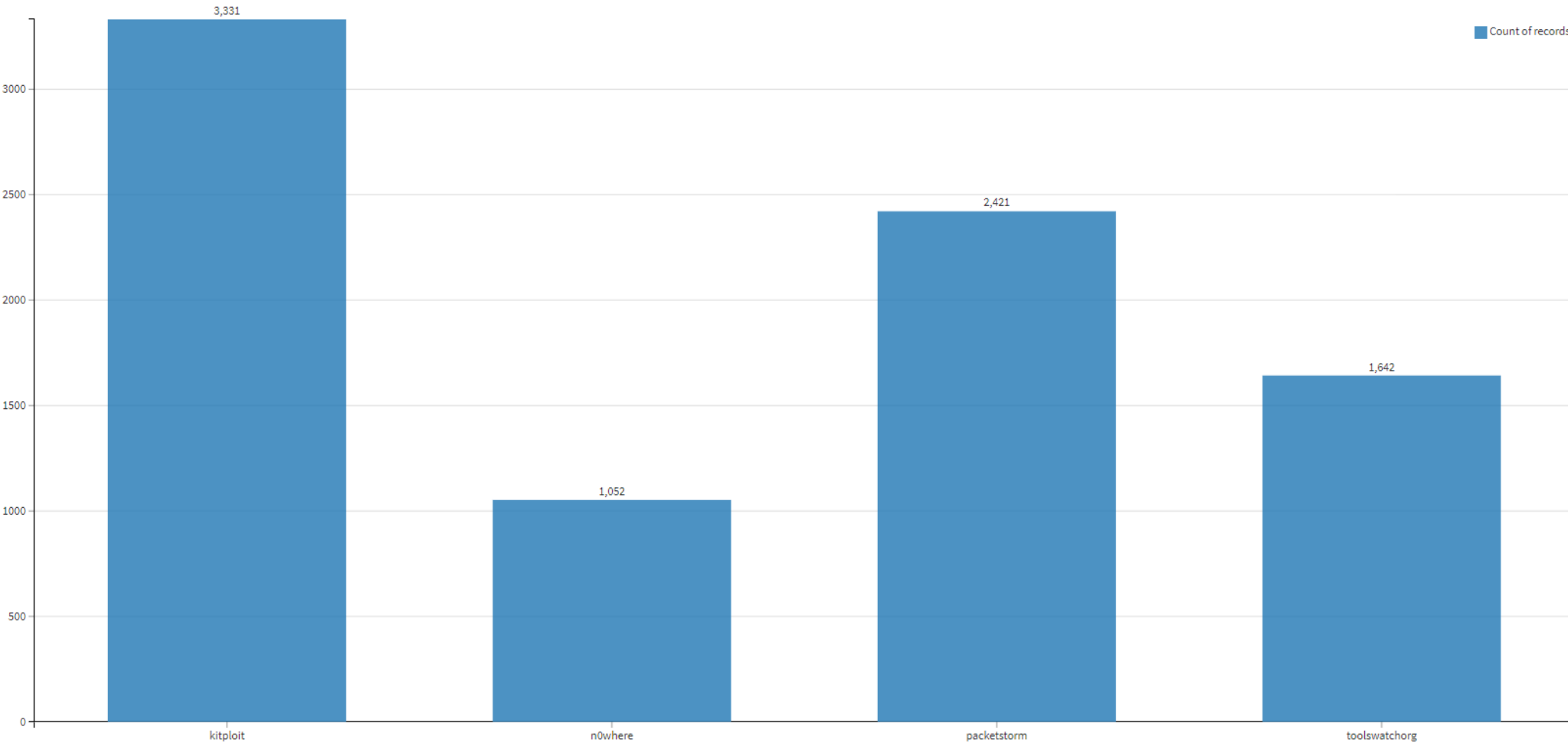
**Non pertinent** car seul **Packetstorm** existait avant 2010 😊

# Distribution des entrées par source depuis 2010

Run: In DSS

Count of records per source since 2010 until 2019 

8446 records  

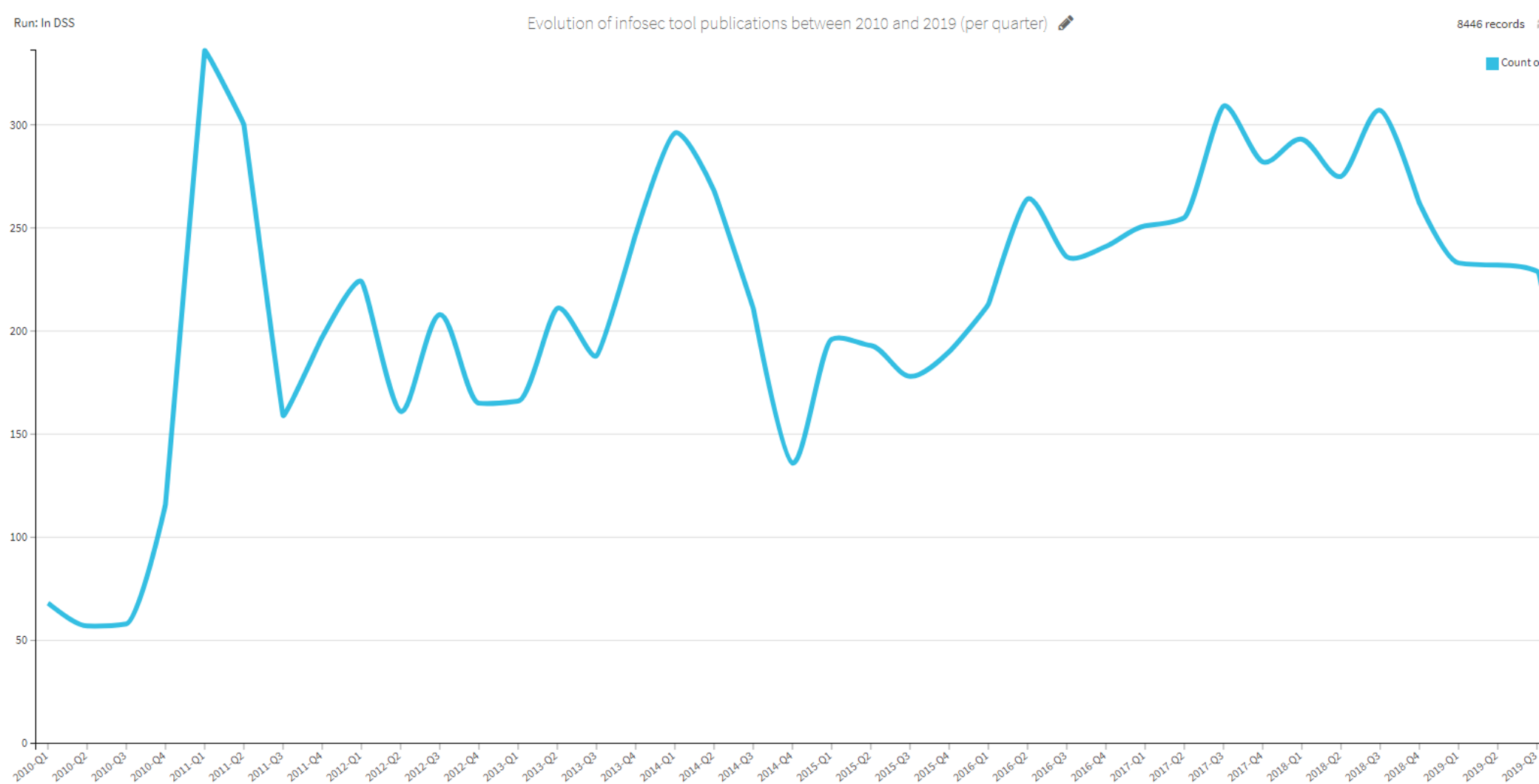


**Pertinent** car les sources ont **le même ordre de grandeur** pour le nombre de publications depuis 2010

Puis, l'évolution

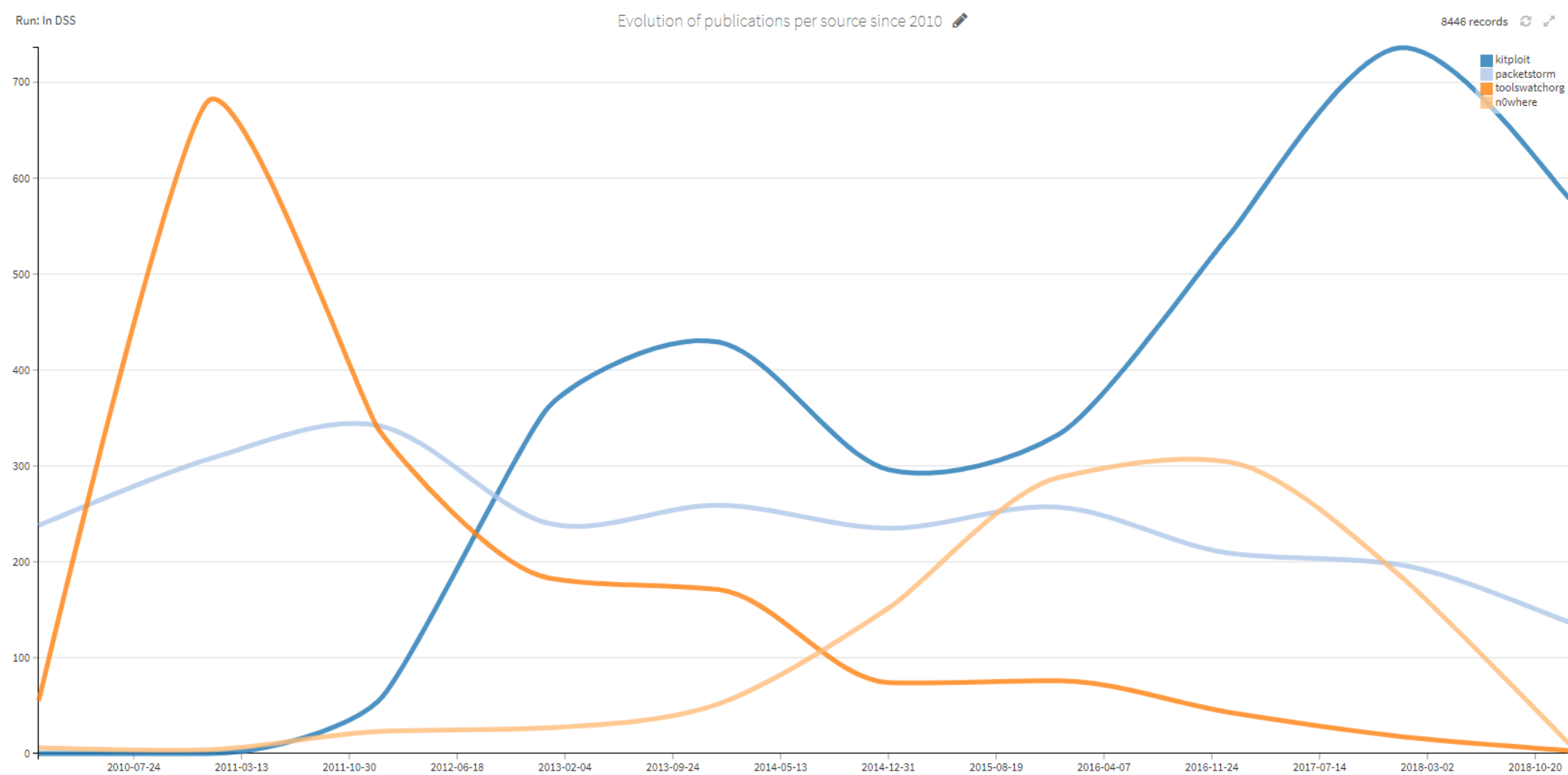


# Evolution du **nombre de publications** (par trimestre) depuis 2010



- **De plus en plus** de publications

# Evolution du **nombre de publications** par source depuis 2010

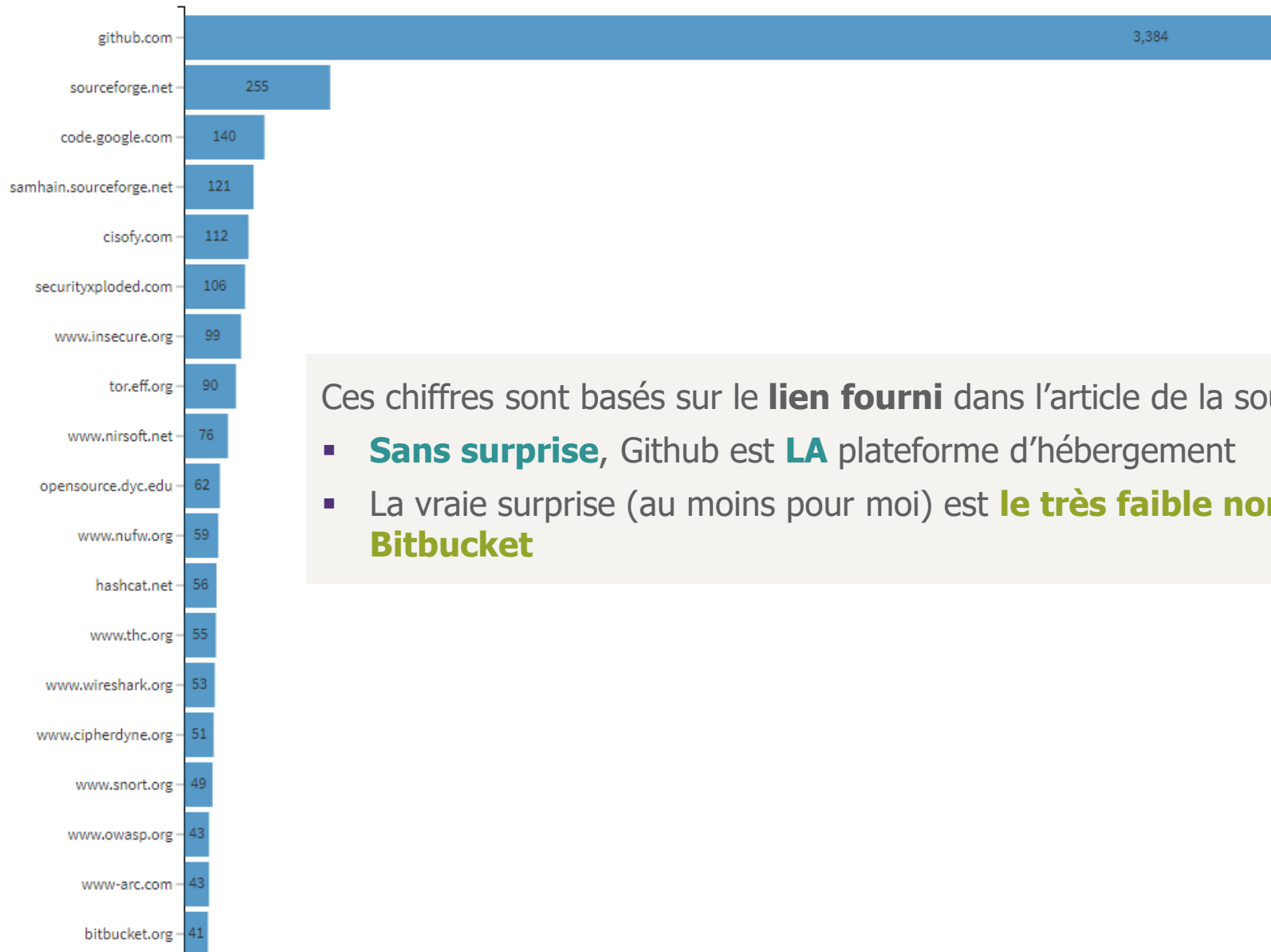


- **De moins en moins de** publications par **toolswatch**
- **Packetstorm**, la référence *old school*, **maintenait** son rythme de publications, mais tend désormais à **diminuer**, tandis que **Kitloit** tend à devenir la **nouvelle source de référence**

# Distribution des plateformes d'hébergement des outils (à date)

Run: In DSS

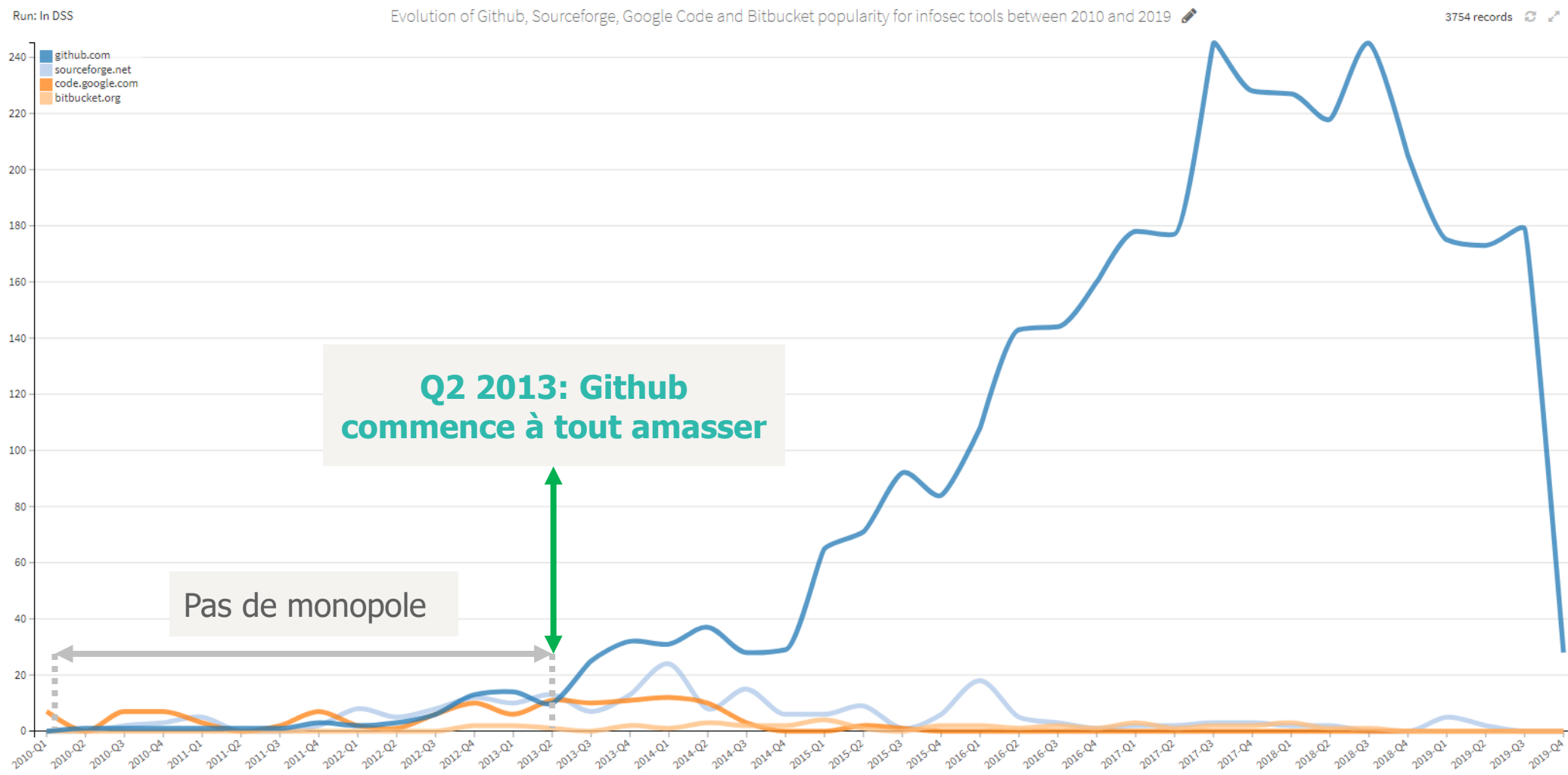
Current top 20 of tool hosting platforms 🖊



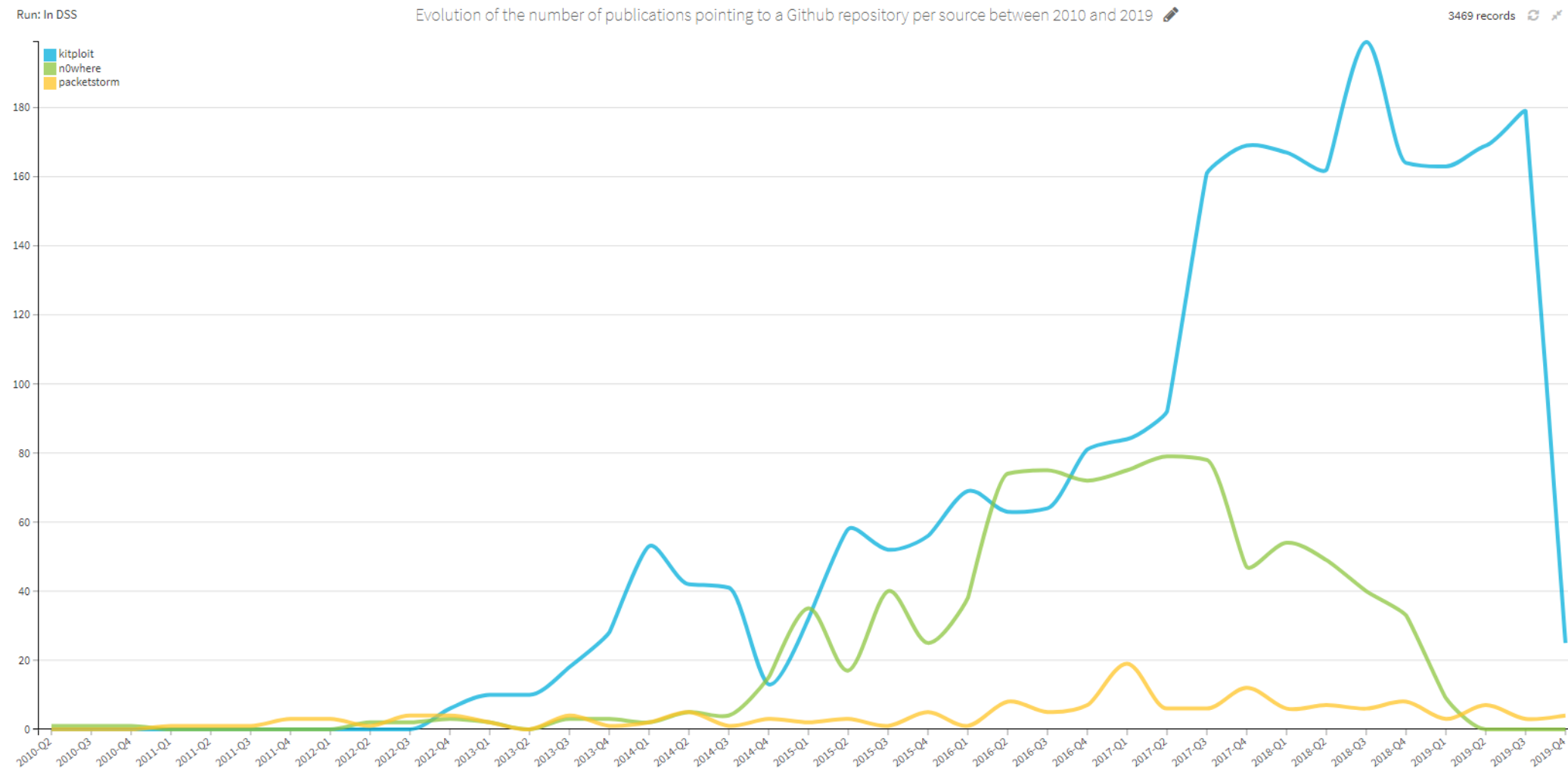
Ces chiffres sont basés sur le **lien fourni** dans l'article de la source de publication

- **Sans surprise**, Github est **LA** plateforme d'hébergement
- La vraie surprise (au moins pour moi) est **le très faible nombre pour Bitbucket**

# Evolution de la popularité de **Github**, **Sourceforge**, **Google Code** et **Bitbucket** pour les outils infosec entre 2010 et 2019



# Evolution du **nombre de publications pointant vers un dépôt Github** par source entre 2010 et 2019



- **Packetstorm** ne suit pas la mouvance, et continue ainsi à apporter de la diversité

Ok, bon si tout est hébergé sur Github,  
faisons un focus sur Github !

# Quelques statistiques pour les **2300+ Github** dépôts analysés

## Stars

**Moyenne:** 1053

**Médiane:** 292

**Ecart-type:** 2968

## Forks

**Moyenne:** 188

**Médiane:** 70

**Ecart-type:** 451

## Watchers

**Moyenne:** 1053

**Médiane:** 292

**Ecart-type:** 2968

(1 étoile induit 1 watch)

## Releases

**Moyenne:** 5

**Médiane:** 0

**Ecart-type:** 18

## Size

**Moyenne:** 15 MB

**Médiane:** 993 KB

**Ecart-type:** 61 MB

## Commits

**Moyenne:** 522

**Médiane:** 71

**Ecart-type:** 1941

## Durée de maintenance

**En jours, dernier – premier commit sur master**

**Moyenne:** 910 (2,5 années)

**Médiane:** 626 (1,7 années)

**Ecart-type:** 976 (2,6 années)

## All Issues

**Moyenne:** 224

**Médiane:** 16

**Ecart-type:** 2030

## Open issues

**Moyenne:** 25

**Médiane:** 3

**Ecart-type:** 96

## All Pull Requests

**Moyenne:** 69

**Médiane:** 4

**Ecart-type:** 398

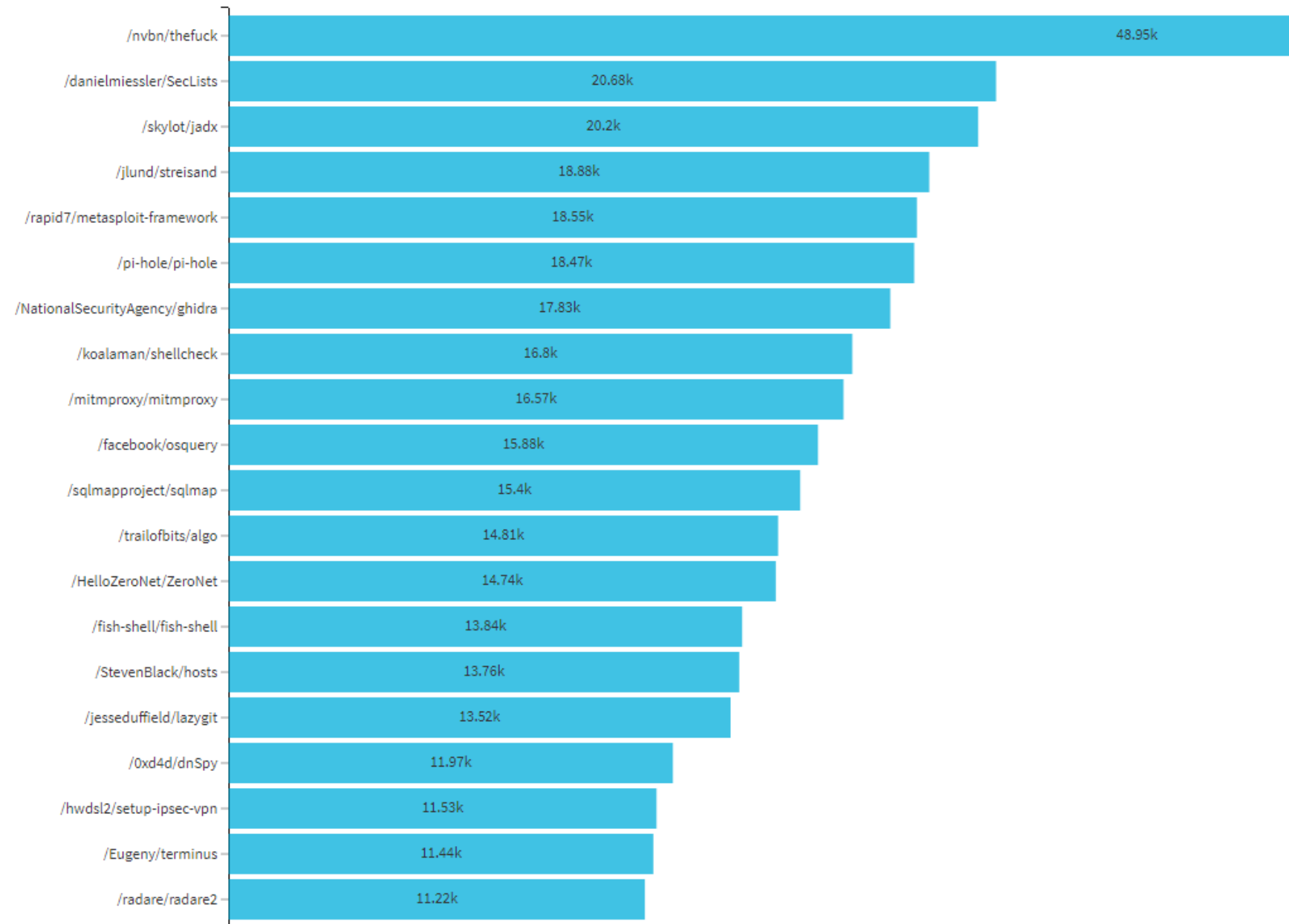
## Open Pull Requests

**Moyenne:** 2

**Médiane:** 0

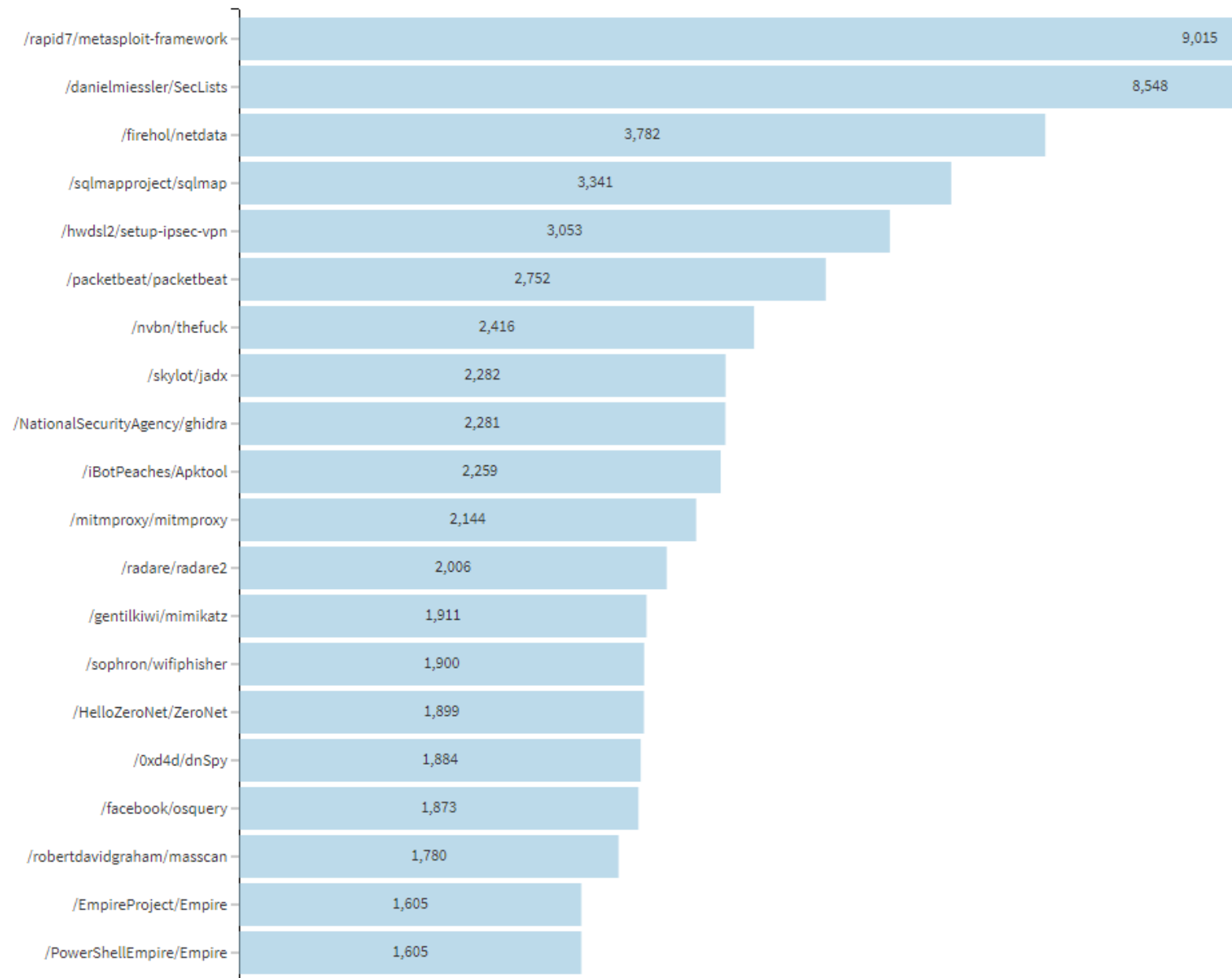
**Ecart-type:** 9

# Top 20 des outils avec le plus grand nombre d'étoiles sur Github

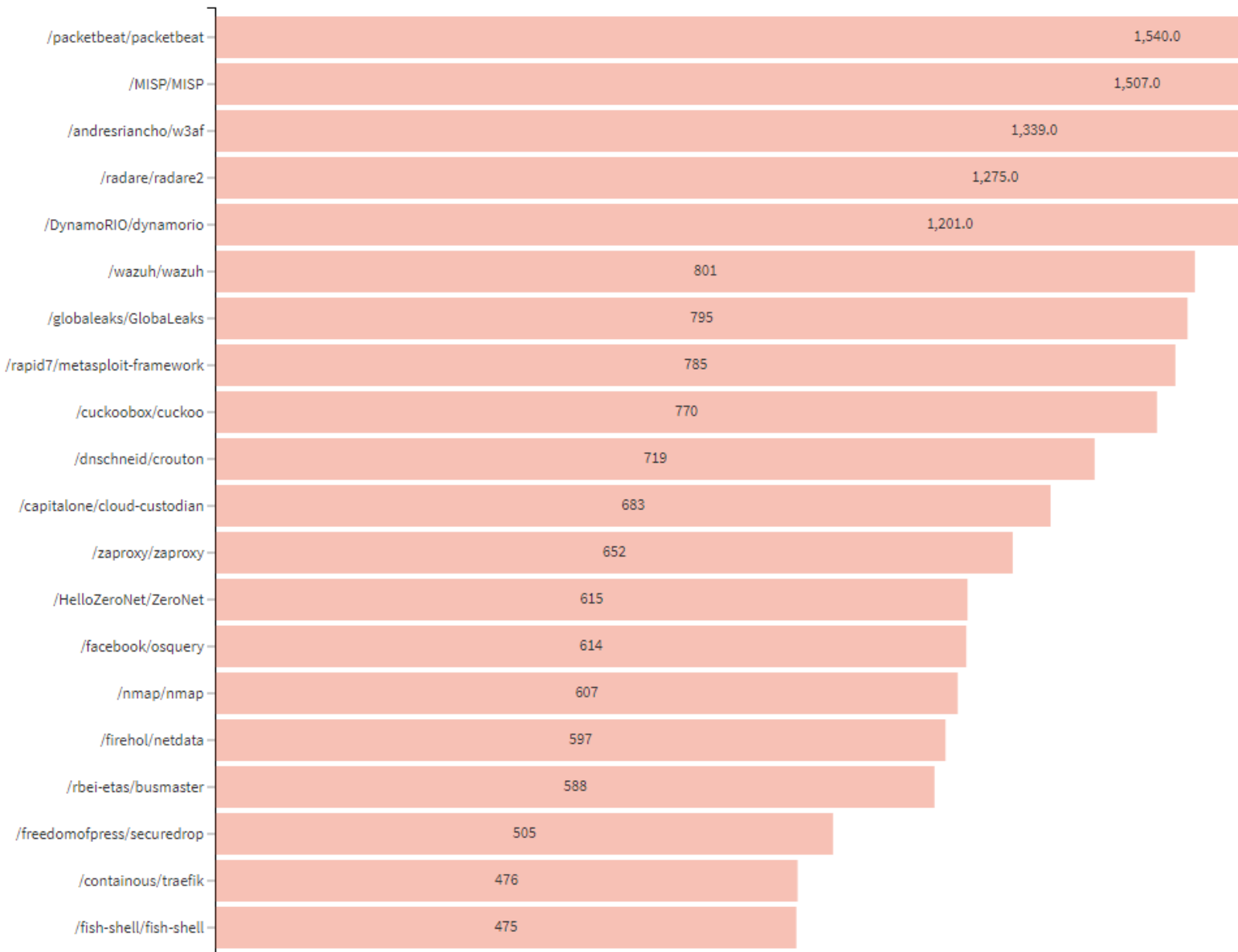




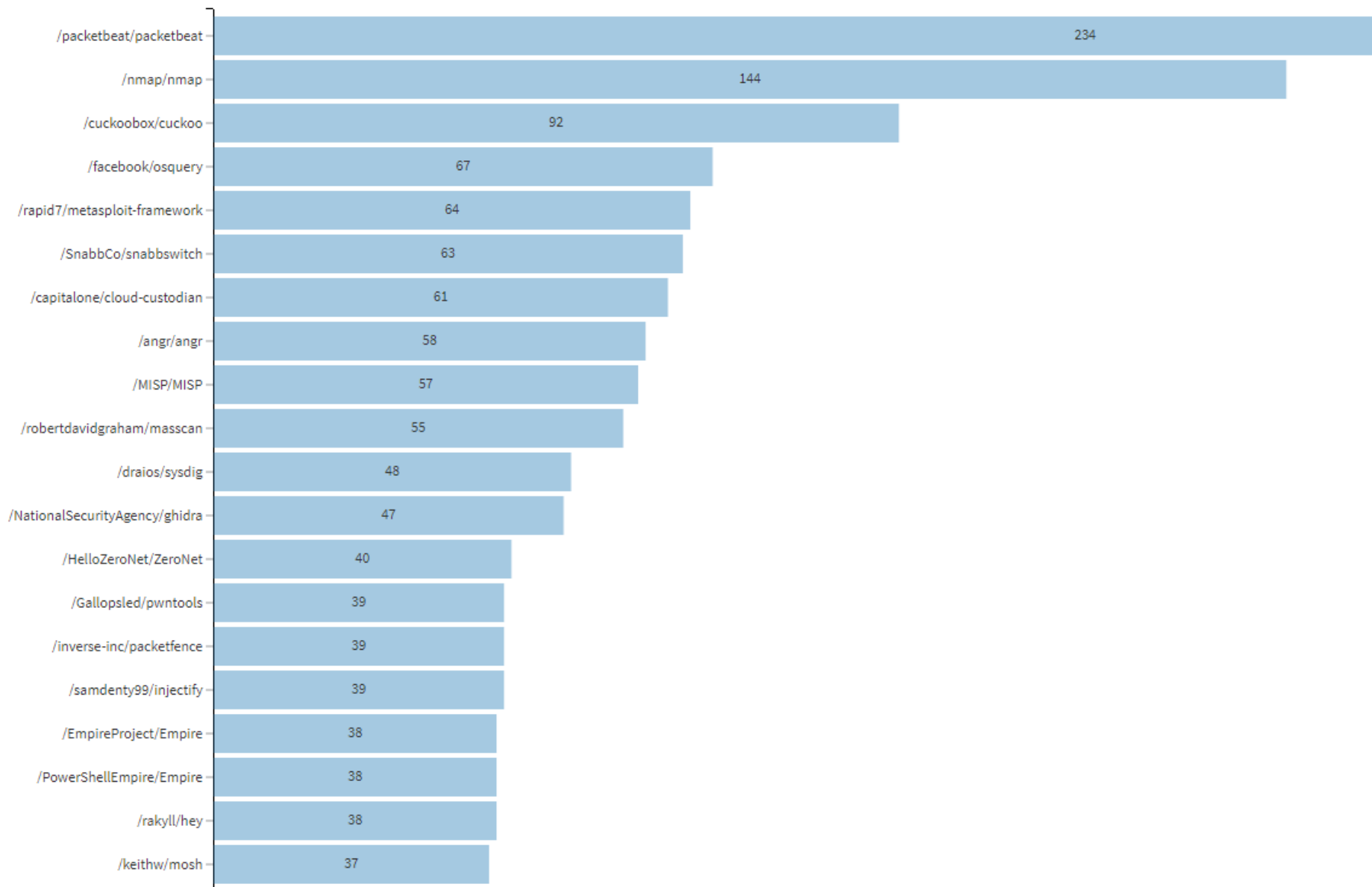
# Top 20 des outils infosec les **plus forkés** sur Github



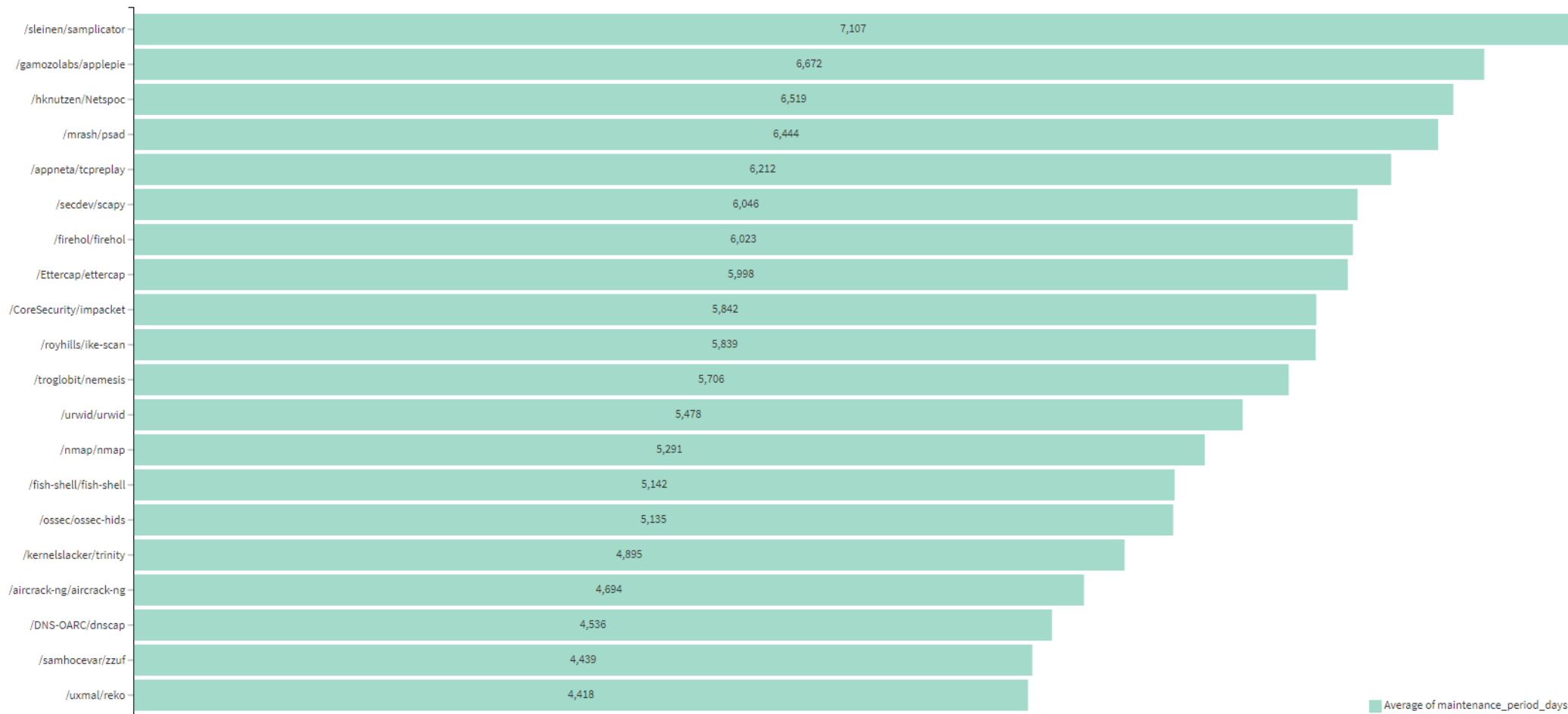
# Top 20 des outils infosec avec le **plus grand nombre d'issues ouvertes** sur Github



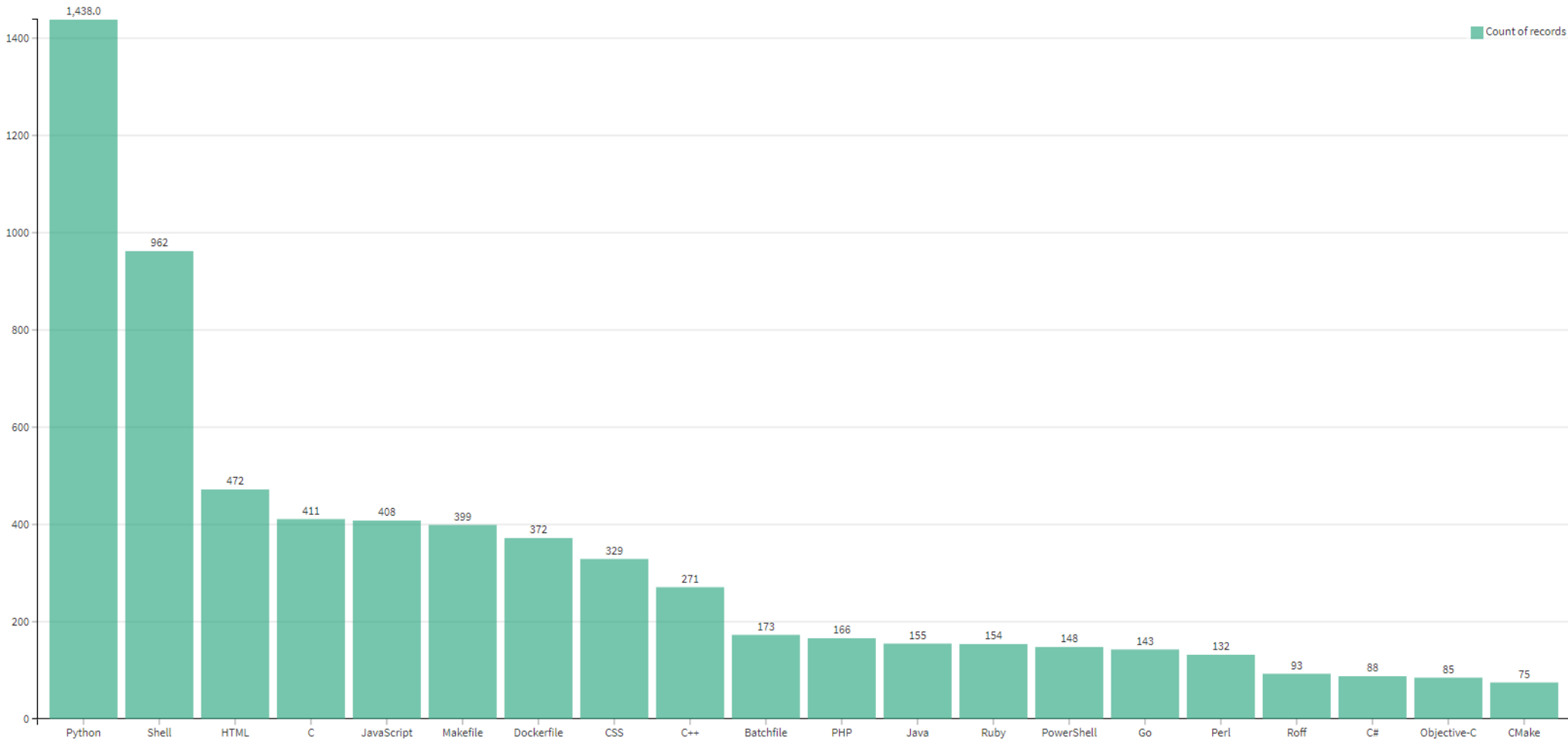
# Top 20 des outils infosec avec le **plus grand nombre de pull requests ouvertes** sur Github



# Top 20 des outils infosec avec la **plus longue durée de maintenance**

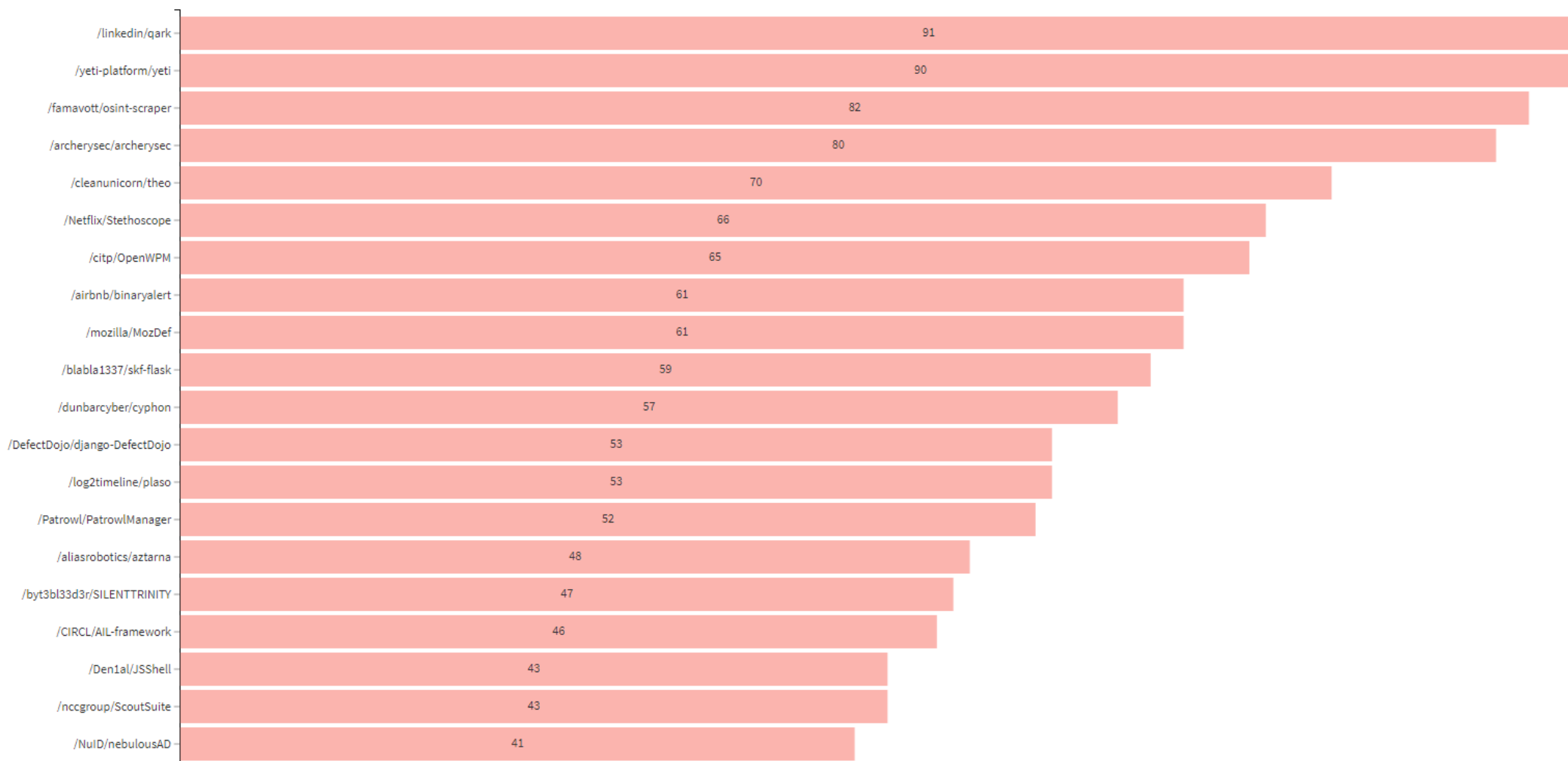


# Top 20 des **langages de programmation les plus fréquemment utilisés** pour les outils infosec sur Github

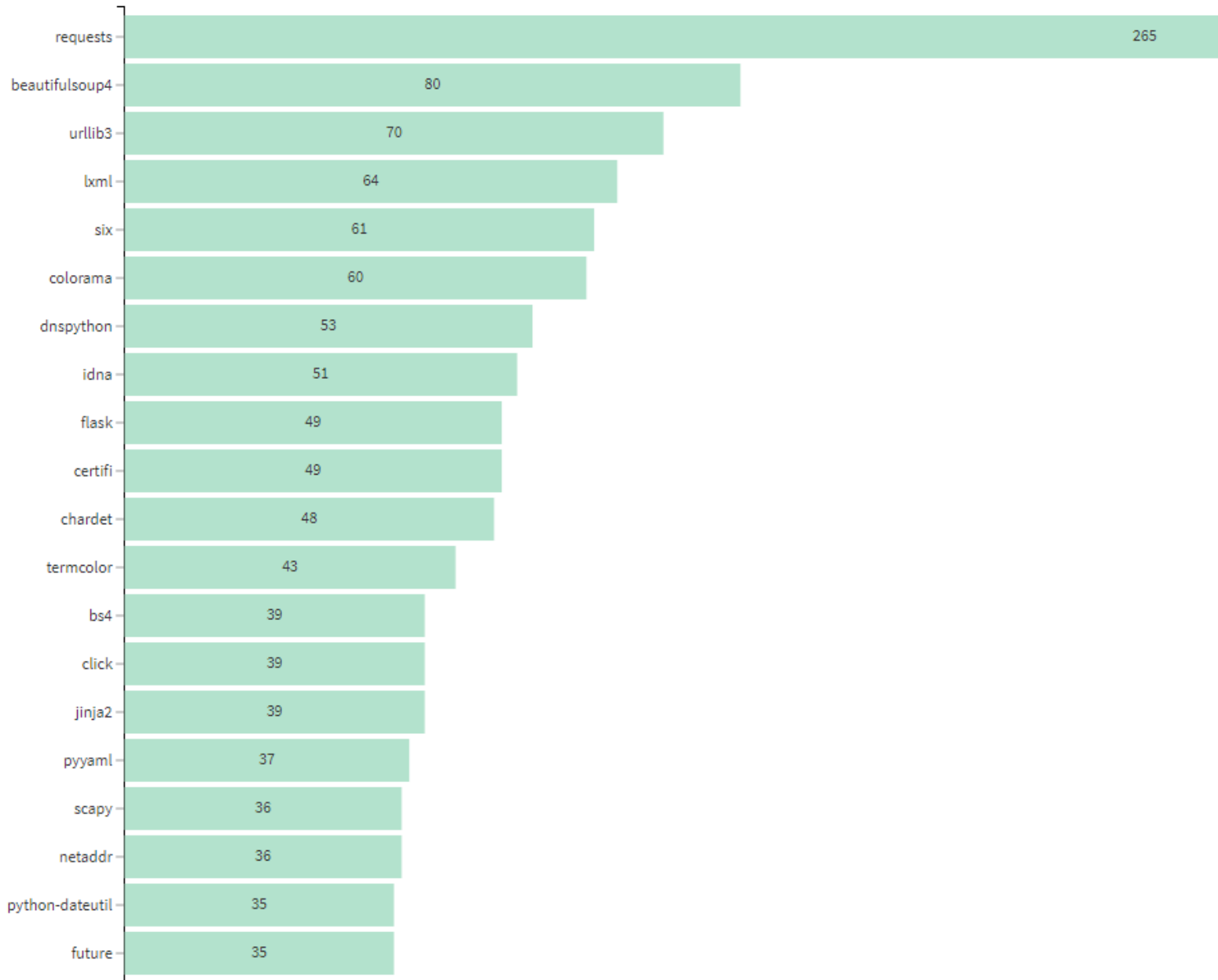


Ok, bon si tout est développé en Python,  
faisons un focus sur Python !

# Top 20 des outils infosec en Python qui ont le **plus grand nombre de dépendances**

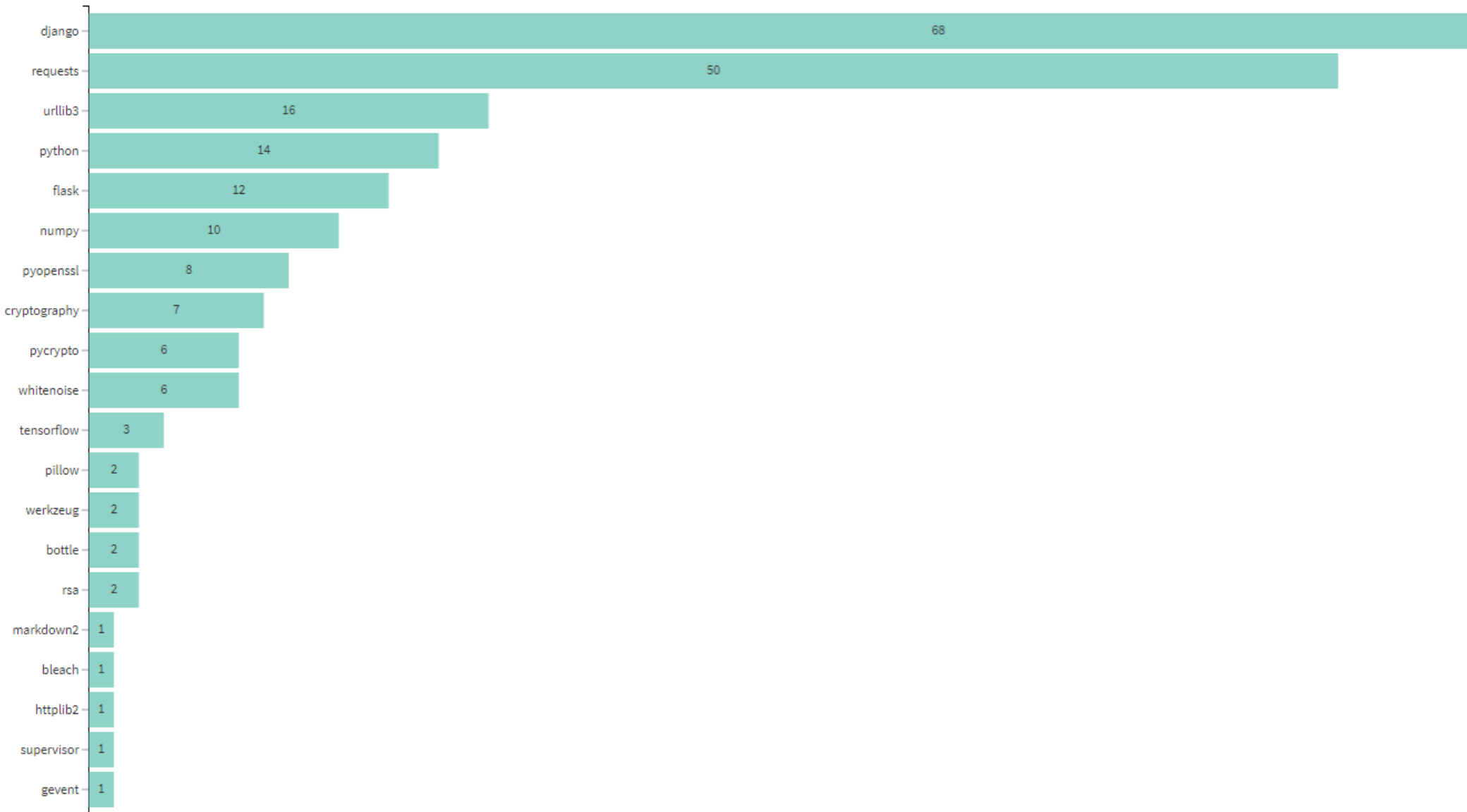


# Top 20 des modules tiers Python les plus utilisés





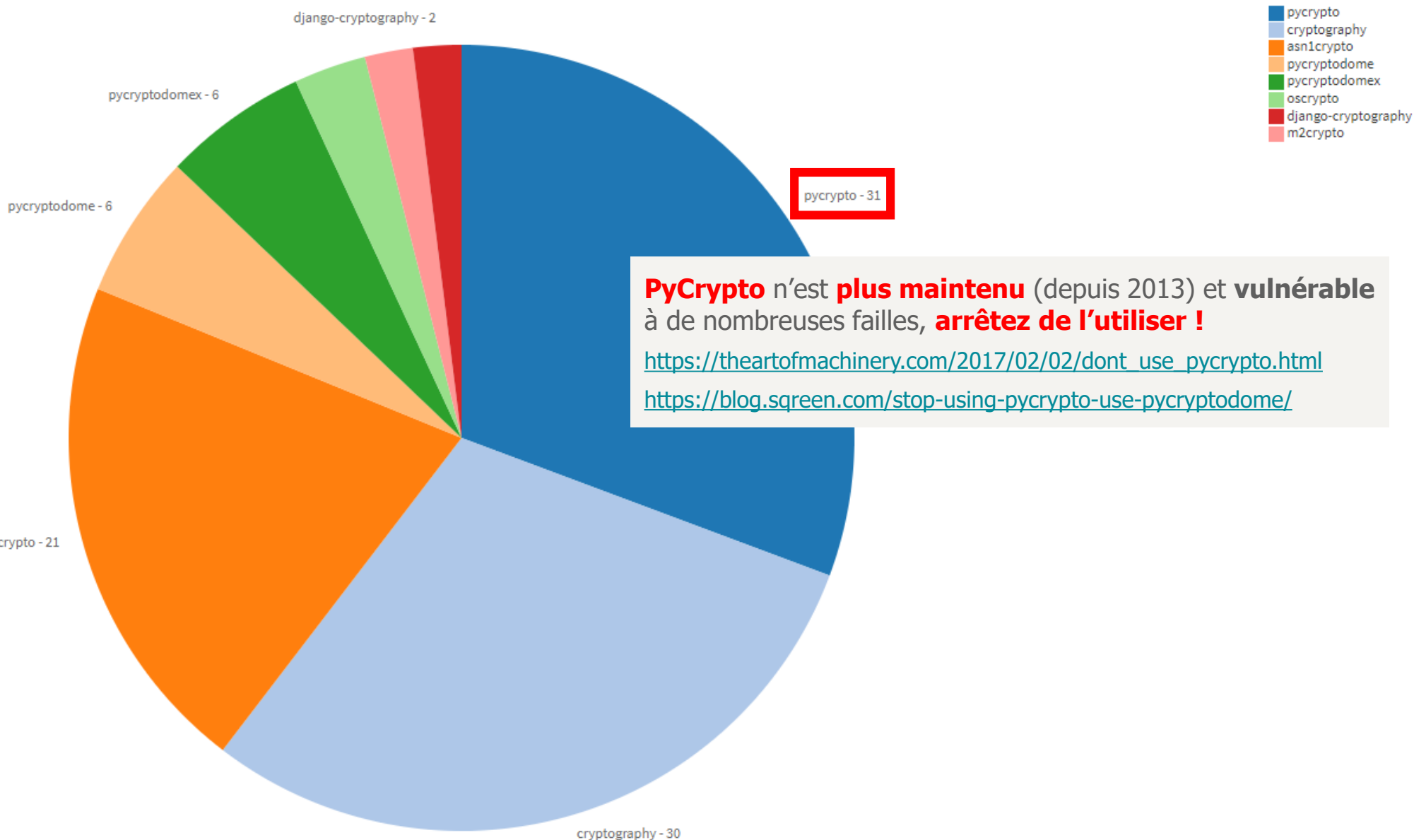
# Top 20 des modules tiers Python les plus fréquemment vulnérables



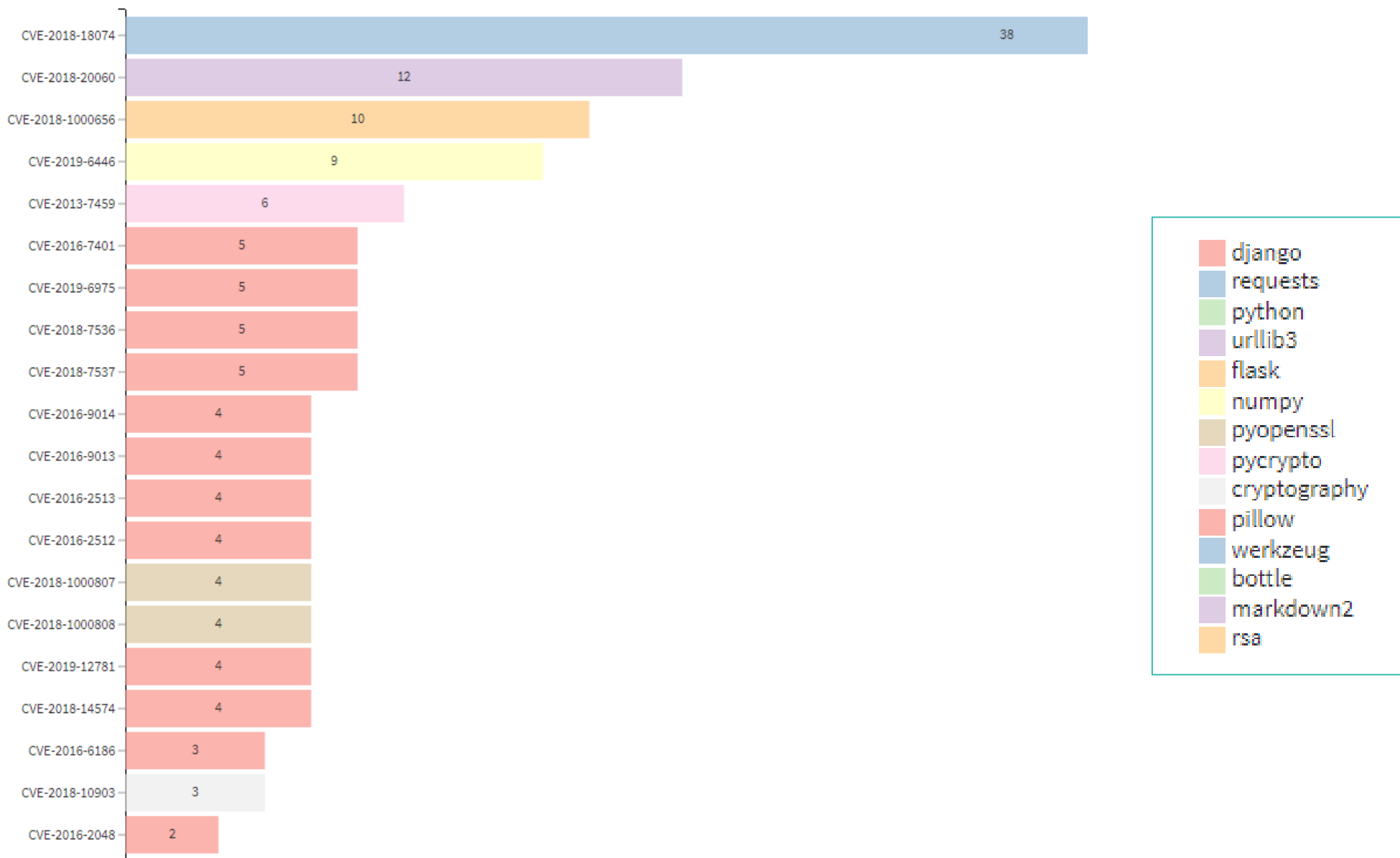
# Distribution des modules crypto Python les plus fréquemment choisis

Distribution of Python crypto module choice for infosec tools

101 records



# Top 20 des **failles les plus rencontrées** pour les modules tiers **Python** utilisés par les outils infosec



Coucou, tu veux voir mon git ?

**Le code et détail de l'étude, ainsi que les datasets enrichis  
sont disponibles sur Github**



<https://github.com/maaaaz/adecadeofinfosectools>

**01**

Un peu de contexte

**02**

Les outils durant cette décennie

**03**

Des règles d'or pour un outil en or

**04**

En bref

# Des règles d'or pour un outil en or (de mon point de vue)

Accepter des options et les parser avec une bibliothèque standard	Le packager et rendre l'installation facile	Supporter l'authentification NTLM
Concevoir avec modularité afin de faciliter les contributions publiques	Fournir des exécutables ou des conteneurs (cela aide les attaquants ET les défenseurs)	Supporter l'authentification Kerberos
Utiliser l'exécution asynchrone (limitation IO → multithreading limitation CPU → multiprocessing)	Chiffrer les flux	Supporter la proxification HTTP
Le rendre utilisable <i>worldwide</i> UTF-8 ! UTF-8 ! UTF-8 !		Supporter la proxification SOCKS
Fournir plusieurs niveaux de verbosité	Fournir une sortie facile à parser en CSV / JSON	Accepter une entrée unitaire ou en masse
		Utiliser des dépendances non vulnérables et évolutives

**01**

Un peu de contexte

**02**

Les outils durant cette décennie

**03**

Des règles d'or pour un outil en or

**04**

En bref

[INSERER UNE CONCLUSION ICI]

Les bons outils **fonctionnent**,  
Les meilleurs **sont scalables**,  
Les illustres **durent.**



# Questions ?

**Thomas DEBIZE**

> [tdebize@mail.com](mailto:tdebize@mail.com)  
> <https://github.com/maaaaz>