

# DocteurPC

Informatique aux Professionnels et Particuliers



## TRIBUNE LIBRE

JEUDI 21 MAI 2026



- 1. QUI SOMMES NOUS ?**
- 2. QUELQUES CHIFFRES CLÉS CYBER**
- 3. LES TYPES D'ATTAQUE ET TYPE D'HACKER**
- 4. L'IA ET SOLUTION DE PROTECTION**

# 1. QUI SOMMES-NOUS ?

# NOUS SOMMES

- Spécialiste de l'informatique et Cybersécurité aux TPE/PME, collectivités et les particuliers
  - Créée en Février 2018 - Plus de 2300 Clients de toutes secteurs d'activité
  - Rayon d'action de 60Km autour de Dinan
  - 5 Collaborateurs dans la société ( 2 Co-Gérants et 3 Salariés dont 1 Alternant)
- 
- Vente et Réparation
  - Mise en service, Installation et Maintenance
  - Contrats de Maintenance
  - Conseils et Audit en Informatique et Cybersécurité

**RÉFÉRENCÉ SUR  
LA PLATEFORME  
CYBERMALVEILLANCE.GOUV.FR**



**RÉPUBLIQUE  
FRANÇAISE**

*Liberté  
Égalité  
Fraternité*



Assistance et prévention  
en sécurité numérique

## 2. QUELQUES CHIFFRES CLÉ

Chiffres clé sur la cybersécurité en 2026

## QUELQUES CHIFFRES

Plus de

# 65%

des TPE/PME en France  
ont subi un  
cyberattaque en 2025

C'est

# 3%

de plus qu'en 2024

Coût moyen TPE/PME

# 32 890 €

pour la résolution d'une  
cyberattaque.  
Sans compter la perte  
d'exploitation

Cependant

# 1 TPE/PME sur 8 + de 230 000 €

pour la résolution d'une  
cyberattaque.  
Sans compter la perte  
d'exploitation

Estimation de

# 10%

d'augmentation des  
cyberattaques en 2026

Plus de

# 60%

des TPE/PME ne sont  
toujours pas protégés  
correctement

Soucre : [www.data.gouv.fr](http://www.data.gouv.fr)  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

**“LES CYBERCRIMINELS CIBLENT SOUVENT LES ENTREPRISES AFFICHANT DES LACUNES SPÉCIFIQUES EN MATIÈRE DE SÉCURITÉ, LES TPE ET PME SONT PARTICULIÈREMENT VULNÉRABLES, SOUVENT EN RAISON DE RESSOURCES LIMITÉES CONSACRÉES À LA CYBERSÉCURITÉ.”**

Source : Anssi - [cyber.gouv.fr](https://cyber.gouv.fr)

# 3. LES DIFFERENTS TYPE D'ATTAQUE ET TYPE DE CYBERCRIMINEL

# LES ATTAQUES LES PLUS REGULIERS

	<b>Phishing (Hameçonnage)</b>	<b>Ransomware (Rançongiciel)</b>	<b>DDOS (Déni de service)</b>
<b>Méthode (Les plus reguliers)</b>	Mail, SMS, Téléphone	Attaque Direct, Logiciel téléchargé, Mail	Ordinateurs Zombie en ciblage direct
<b>But</b>	Voler des informations (Bancaire, Clients, Confidentiels)	Réclamer de l'argent du rançon qui chiffre vos données	Ralentir/couper l'accès aux services réseau
<b>Solutions</b>	Parefeu Sylink / MailinBlack	Parefeu Sylink / MailinBlack	Parefeu Sylink

# LES TYPES DE CYBERCRIMINEL

## WHITE HAT



### HACKERS ÉTHIQUES

Se sont des pirates qui s'introduit sur des systèmes avec l'autorisation du propriétaire, afin de trouver les failles et les faiblesses des systèmes en place

## BLACK HAT



### HACKERS MALVEILLANTS

Cybercriminels professionnels, Ils piratent illégalement des systèmes avec des intentions malveillantes.  
Ils sont a l'origine des Ransomwares et ils exploite les failles des entreprises

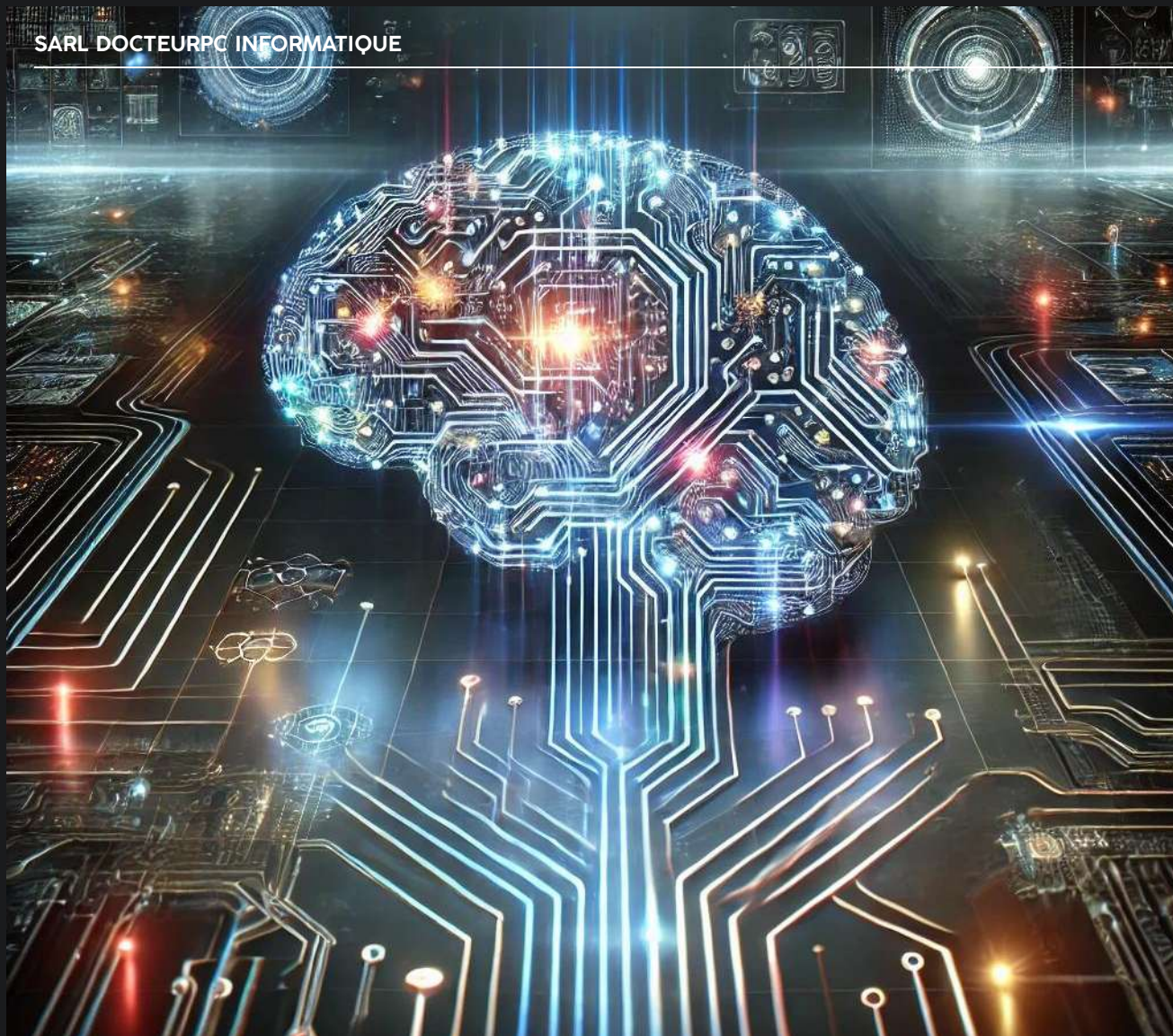
## GRAY HAT



### HACKERS DOUBLE FACE

Se sont des pirates qui travaille dans l'illégalité, car ils attaque des systèmes sans le consentement des propriétaires du système, mais ils alerte le propriétaire sans exploiter la faille trouver

# 4. L'IA ET SOLUTION DE PROTECTION



**L'IA EST DE PLUS  
EN PLUS PRESENT  
DANS NOTRE  
QUOTIDIEN**



OpenAI  
ChatGPT **4.0**



Copilot

Gemini

# PAREFEU SYLINK BOX SOLUTION 100% FRANÇAISE

## SYLink BOX Firewall

- IDS (Intrusion detection system)
- IPS (Intrusion protection system)
- EDR (Endpoint detection and Response)
- VPN (Virtual Private Network)
- **L'IA** embarquée est basée sur un algorithme complexe d'apprentissage intelligent.

**SYLink**  
TECHNOLOGIE



# MAILINBLACK

## SOLUTION 100% FRANÇAISE

- Protection des emails (Protect) : Filtre pour bloquer les mails spams, mais avec les virus et les tentatives de phishing (hameçonnage) avant qu'ils n'atteignent la boîte de réception.
- Système d'authentification unique : Lorsqu'un expéditeur inconnu vous écrit pour la première fois, il reçoit une demande automatique pour prouver qu'il est humain (souvent via un petit test ou un captcha) afin de valider l'envoi.

En bref, c'est une solution tout-en-un pour sécuriser les communications par email des entreprises et réduire le risque d'erreur humaine face aux cyberattaques.



# CONCLUSION

- Les TPE/PME sont d'avantage cible vu la manque de protection et moyens mises en place par les entreprises
- Protéger les systemes de mails pro avec MailinBlack
- Il est primordiale de se protéger avec un système de Parfeu performant avec IDS, IPS et EDR

# MERCI !

Pour plus d'informations :

**James LLOYD**

02.57.69.00.76

[contact@docteurpcinfo.fr](mailto:contact@docteurpcinfo.fr)

**DocteurPC**  
Informatique aux Professionnels et Particuliers

