

Panorama de la menace CYBER

29 Septembre 2026



```
bash - antoine@csirt-ucrs:~
```

```
antoine@csirt-ucrs:~$ whoami
```

```
Antoine Parmentier
```

```
antoine@csirt-ucrs:~$ ./get_profile.sh --verbose
```

```
[+] Initializing secure decryption routine... Done.
```

```
[+] Loading CSIRT Operator profile...
```

```
[Identité] : Antoine PARMENTIER
```

```
[Rôle] : Responsable CSIRT (CSIRT - Incident Response)
```

```
[Structure] : Urgence Cyber région Sud (UCRS) - PACA
```

```
[Parcours] : Ancien militaire Marine Nationale
```

```
[Centres d'intérêt] :
```

```
Sport
```

```
Trail
```

```
Randonnée
```

```
antoine@csirt-ucrs:~$ █
```

Le CSIRT Urgence Cyber région sud



Réponse à incident
de 1^{er} niveau

Prévention,
sensibilisation et
montée en maturité

Veille et alerte

- Association de loi 1901
- Etroite collaboration avec l'ANSSI
- Membre de l'InterCERT France depuis Mars 2025



Les chiffres clés



2025

49 incidents

27 signalements

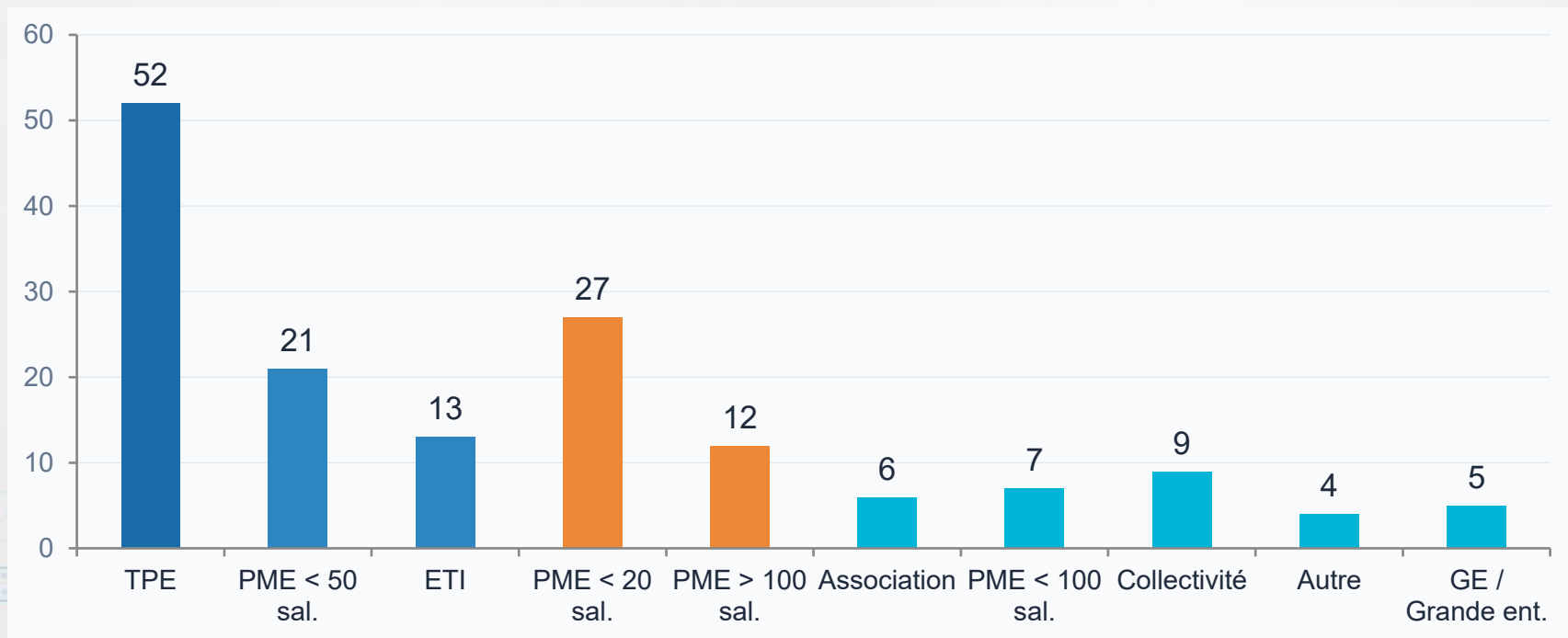
2026 (Au 19/09)

98 incidents

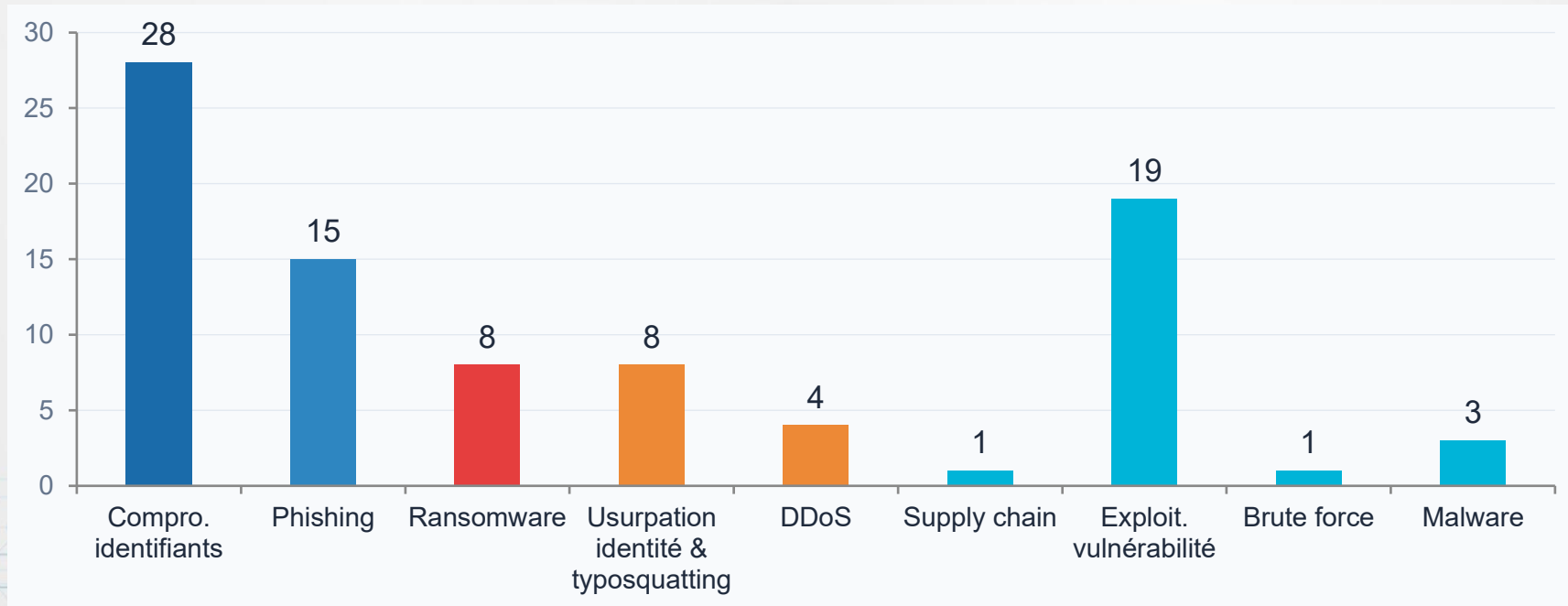
63 signalements

+184% sur le 1er semestre

Structures impactées en 2026



Répartition par catégories des incidents de 2026



Méthodologie – Compromission identifiants



1

Récupération des identifiants

Par phishing, infostealer, password spraying ou achat sur le darknet

2

Accès “discret” à la boîte mail

L'attaquant observe, collecte des informations, identifie les relations

3

Exploitation

Virement frauduleux , campagne de phishing depuis l'adresse légitime, usurpation auprès de partenaires

4

Persistance

Règle de transfert, accès maintenu pendant des semaines ou des mois

1er type d'incident traité par notre centre

15

incidents phishing
jan-sept 2026

30%

des incidents UCRS
ont un vecteur phishing

Kali365

kit PhaaS M365
alerte FBI mai 2026

Kali365 - Phishing-as-a-Service sans vol de mot de passe (mai 2026)

Plateforme distribuée via Telegram, repérée en avril 2026, alerte FBI le 21 mai 2026. Cible les comptes Microsoft 365 en détournant le flux OAuth 2.0 device code flow. La victime saisit elle-même un code appareil sur la vraie page Microsoft, autorisant l'appareil de l'attaquant. Résultat : accès direct à Outlook, Teams, OneDrive, sans mot de passe et sans être bloqué par le MFA.

Phishing

De : Noah Torvic <safran.dpo@safrangroup.com>

Envoyé : jeudi 30 juillet 2026 09:19

À : [REDACTED]

Objet : Depot de reclamation

***[EMETTEUR EXTERNE] : Ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe à moins qu'ils ne proviennent d'un expéditeur fiable, ou que vous ayez l'assurance que le contenu est sûr.

Bonjour,

Veuillez trouver ci dessous le document PDF exposant les éléments de ma réclamation.

[Document a télécharger](#)

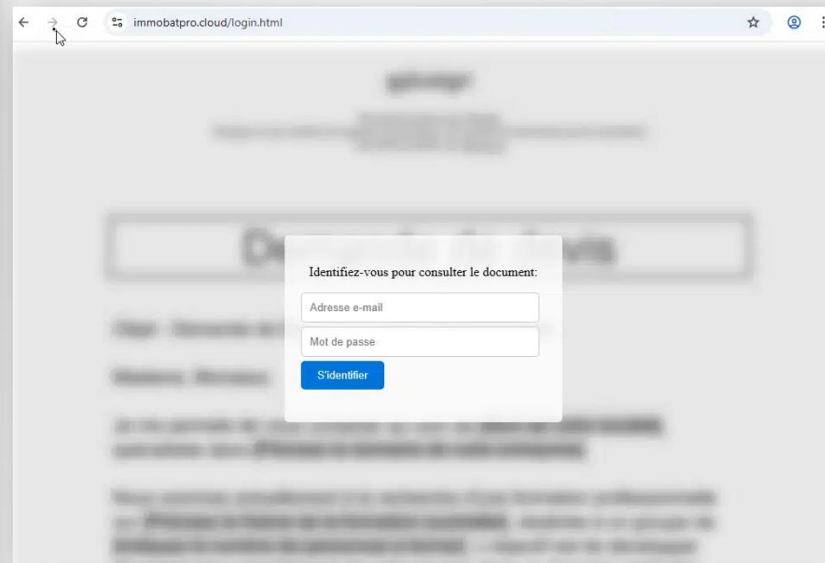
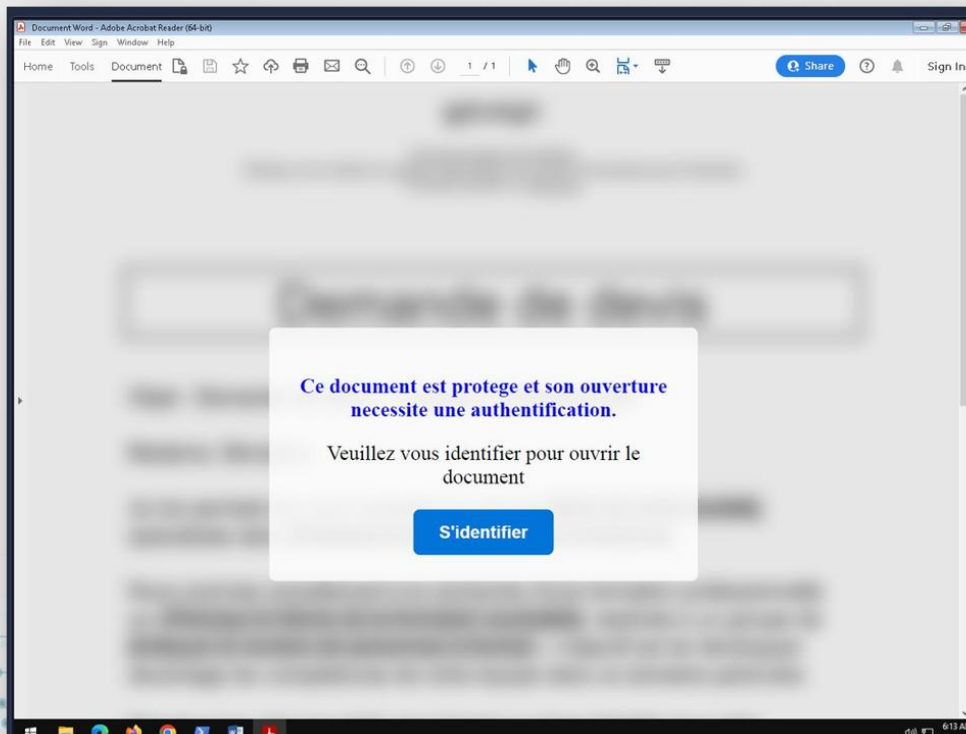
Je vous remercie de bien vouloir en prendre connaissance et de me faire part des suites qui seront données à ma demande dans les meilleurs délais.

Je reste à votre disposition pour tout complément d'information.

Cordialement.

Noah Torvic

Phishing



Rançongiciel - fonctionnement et tendances



128

rançongiciels
ANSSI 2025

Qilin

souche n°1
21% des cas
700+ victimes mondiales

8

incidents ransomware
UCRS jan-sept 2026

Double / triple extorsion : le modèle standard en 2026

■ Chiffrement des données + demande de rançon (extorsion 1)

■ Menace de publication des données exfiltrées (extorsion 2)

■ DDoS affectant la disponibilité des services de l'entreprise (extorsion 3)



ATTENTION :
VOS FICHIERS ONT ÉTÉ VERROUILLÉS ET CHIFFRÉS



Tous les documents, photos, vidéos et sauvegardes sur cet appareil sont verrouillés. Nous seuls détenons la clé. Les méthodes de récupération conventionnelles échoueront.

POUR RÉCUPÉRER VOS FICHIERS

Payez la rançon en Bitcoin. Un compte à rebours est affiché à droite. Vous avez 14 jours. Après 14 jours, votre clé de déchiffrement est supprimée définitivement. Vos fichiers seront irrécupérables — perdus à jamais. Vous pouvez envoyer des paiements progressivement jusqu'à atteindre le montant total.

APPAREIL EN LIGNE VS HORS LIGNE

Si vous gardez votre appareil en ligne : le déchiffrement se déclenche automatiquement lorsque le paiement complet est confirmé.

Si vous déconnectez votre appareil d'Internet : [cliquez ici](#) pour les instructions de déverrouillage manuel.

PREUVE QUE NOUS POUVONS DÉCHIFFRER

Plusieurs fichiers ont été déverrouillés. Cliquez sur « Afficher la preuve du fichier » à gauche. Le reste sera décrypté après paiement.

PAIEMENT

Envoyez le montant exact en BTC indiqué ci-dessous. Couvrez les frais du réseau. Sous-paiement = pas de déchiffrement.

Si vous ne pouvez pas tout payer en même temps, vous pouvez envoyer plusieurs paiements jusqu'à ce que le montant total soit payé avant la fin du compte à rebours.

Garde ça privé. L'implication de tiers — y compris les forces de l'ordre ou l'utilisation d'outils de déchiffrement — sera automatiquement détectée et vos fichiers ne seront pas récupérables. Tes dossiers, ton choix.

[Après récupération : transférez les fichiers vers un appareil sécurisé. Ce système reste vulnérable.](#)

▲ VOUS DEVEZ PRYER : ▲

0.0034

À cette adresse Bitcoin :
[BC1Q9qr4FRSK9vu6P42kng39npg4H53U4WecvF03](https://blockchain.info/address/BC1Q9qr4FRSK9vu6P42kng39npg4H53U4WecvF03)

**BITCOIN**
Scannez le QR ou copiez l'adresse pour payer

SCANNER LE
CODE QR



COPIEZ L'ADRESSE CI-DESSOUS

BC1Q9qr4FRSK9vu6P42kng39npg4H53U4WecvF03

▶ Cliquez sur l'adresse pour copier - ou clic droit

0.0034

COMPTÉ À
REBOURS

10

JOURS

04 43 12

HRS MIN SEC

Nouveau dans le monde des cryptomonnaies ? Cliquez ici pour un guide supplémentaire sur la façon de payer



30/09/2026

urgencecyber-regionsud.fr 4

Télécharger l'échantillon de données

COMMUNIQUÉ – INCIDENT DE SÉCURITÉ

Intrusion dans le système d'information de

Après la DGFiP, et bien d'autres entreprises, c'est désormais au tour de de faire face à une intrusion dans son système d'information, révélant une nouvelle fois les lacunes de certaines organisations dans la protection des données personnelles.

Une **intrusion** dans le système d'information de est survenue **entre le 10 et le 14 août 2026**. Des données personnelles de clients et d'intervenants ont potentiellement été consultées et exfiltrées. À ce jour, **l'entreprise n'a pas notifié cette violation à la CNIL**, alors que le RGPD lui impose de le faire dans un délai de 72 heures, et n'a informé aucune des personnes concernées.

PÉRIODE DE L'INTRUSION
10 → 14 août 2026

DÉTECTION INTERNE
15 août 2026

DÉLAI LÉGAL CNIL (72 h)
Expiré le 18 août

NOTIFICATION CNIL
X Non effectuée

Chronologie des faits

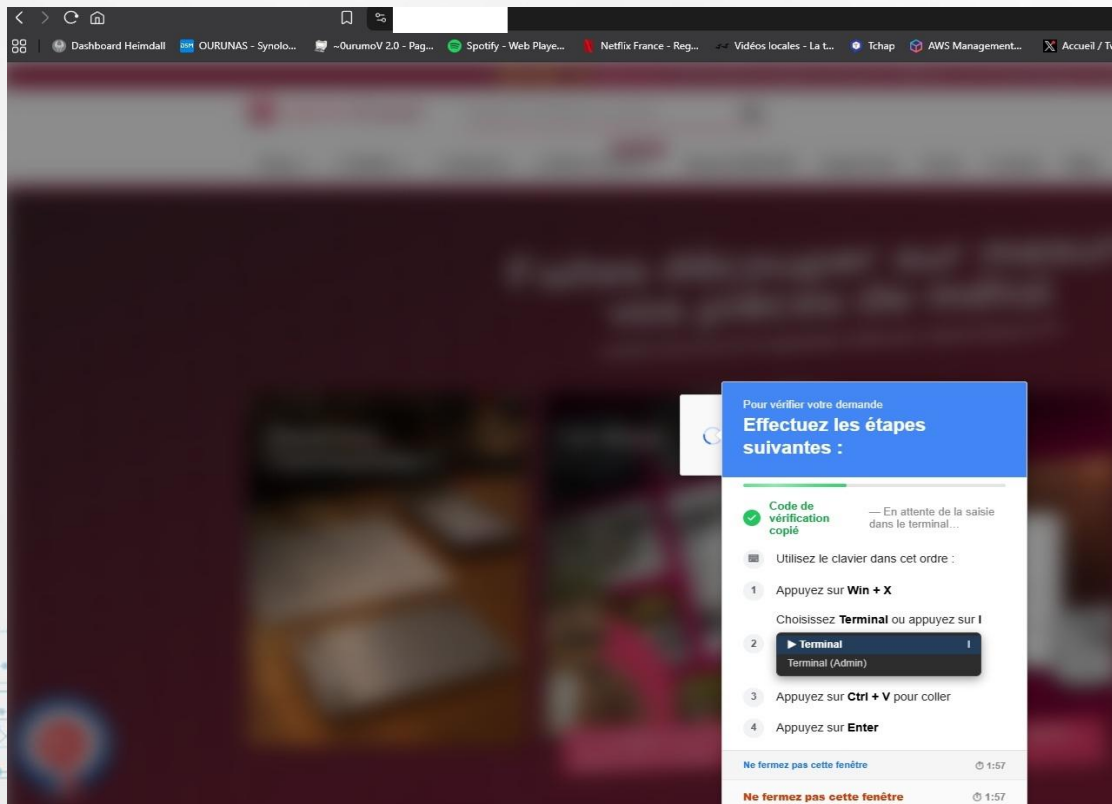
- 10 août 2026
Compromission d'identifiants d'un compte administrateur via une campagne d'hameçonnage. Début de l'intrusion.
- 10 → 14 août 2026
L'attaquant accède à la base clients : noms, prénoms, adresses postales, e-mails, numéros de téléphone et historiques de prestations d'environ **12 400 clients** et **850 intervenants**.
- 14 août 2026

Ce que

aurait dû faire

- X Dissimuler l'incident et le traiter « en interne » pour préserver l'image de marque.
- ✓ Documenter immédiatement la violation dans le registre prévu à l'art. 33 §5 (faits, effets, mesures).
- ✓ Réaliser une analyse de risque pour les droits et libertés des personnes (nature des données, volume, usages malveillants possibles).
- ✓ Notifier la violation à la CNIL via son téléservice dédié, au plus tard le 18 août – une notification pouvant être effectuée par phases si toutes les informations ne sont pas encore disponibles (art. 33 §4).
- ✓ Informer sans délai les 12 400 clients et 850 intervenants (risque élevé : hameçonnage ciblé), avec des recommandations concrètes (vigilance, changement de mots de passe, signalement des messages suspects).
- ✓ Mesures techniques : réinitialisation des identifiants, déploiement de l'authentification multifacteur, investigation forensique, durcissement de la supervision.
- ✓ Se faire accompagner : dépôt de plainte, échanges avec l'ANSSI, et pour une structure de cette taille, la plateforme d'assistance cybermalveillance.gouv.fr.

Faits marquants 2026



Signalement de fuite de données

- FULL DATABASE (FOR SALE)

Start new topic

Below you will find all the tables and their samples, we have over 1 million datas in our possession.

ATTENTION: Serious buyers only.

STARTING PRICE: 10K (negotiable if above 3.5K)

PAYMENT: XMR only or btc, non-negotiable.

CONTACT (SESSION) : 0598f12842457ec9a83f3acbdbb97c9e04e178f58adc8d43bc0381a8cad2c8d5bXXX

Website :

1. COT_REGLEMENT

File: COT_REGLEMENT.csv

Row count: **19,925**

Data type: Premium settlement records, transaction amounts, payer names, bank routing BIC/IBAN, direct debit schedules.

This table contains payment and settlement data.

Columns:

timestamp, COT_CO_BIC, COT_CO_RUM, COT_CO_IBAN, MUT_ID_MREG, IND_SY_INDIVIDU, COT_DT_JOUR_RGLT, COT_SY_REGLEMENT, IND_CO_STRUCTURE, COT_CO_AGENT_RGLT, COT_FL_REMB_TIERS, COT_LB_REMB_TIER

Les développeurs sont-ils une cible privilégiée?



Accès étendus

*Clés API, mot de passe,
tokens...*

Point d'entrée vers la production

*Pipelines CI/CD, travail
collaborative...*

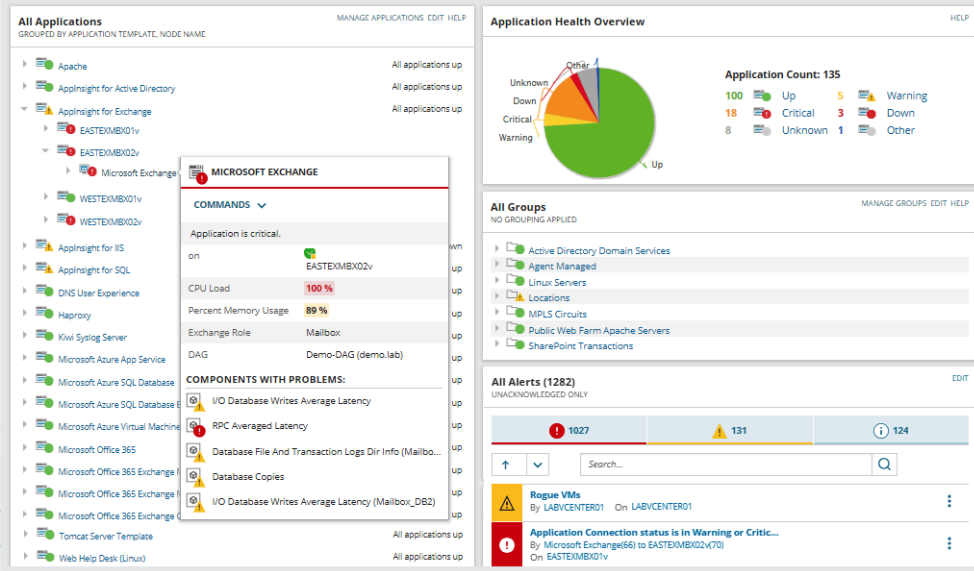
Surface d'attaque élevée

*Plugin, Extensions IDE
malveillantes, GIT piégé*

Attaque par supply chain



Application Summary

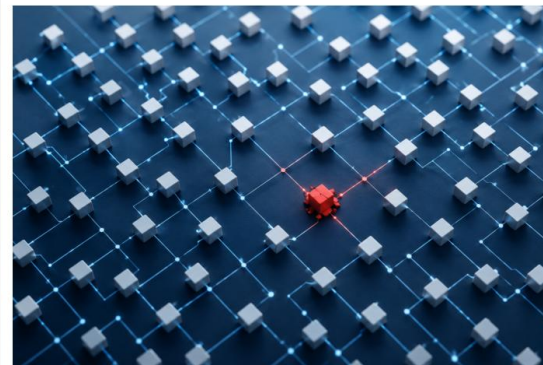


[CYBERATTACHE]

Cybersecurite - Logiciel

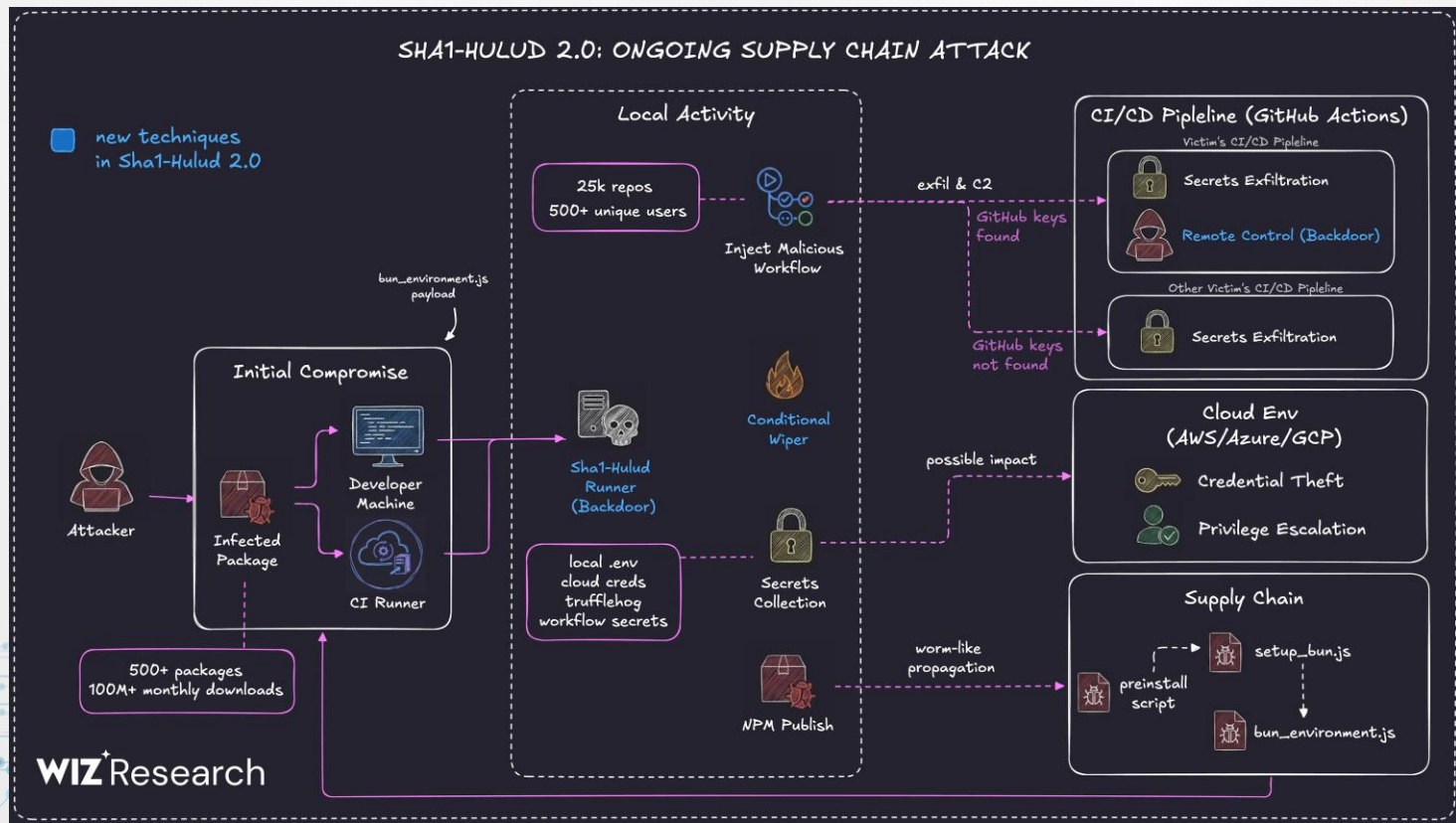
Une attaque supply chain compromet plus de 30 packages npm de Red Hat

3 juin 2026



Une attaque visant des packages officiels publiés sous le compte npm de Red Hat rappelle la fragilité de la chaîne logicielle moderne. Les chercheurs de Microsoft ont identifié plus de trente paquets compromis capables de voler des identifiants et des secrets présents sur les postes de développeurs et dans les environnements CI/CD.

Le ver "Shai-Hulud"



Le splosquatting : L'IA hallucine!

- Nouvelle forme du typosquatting
- Objectif : enregistrer le nom d'un paquet inventé par un outil d'IA et à attendre que quelqu'un l'installe.

38%

Noms inspirés de paquets
existants

13 % : fautes typographiques
51 % : paquets inventés

8,7%

Paquets approuvés sur d'autres
écosystèmes (npm)



[The Rise of Slopsquatting: How AI Hallucinations Are Fueling a New Class of Supply Chain Attacks | Socket](#)

Bonnes pratiques

- 1 Apprendre à séparer ses usages pro-perso
- 2 Adoptez le principe du moindre privilège
- 3 Effectuez régulièrement des tests de sécurité et des audits
- 4 Sécurisez le stockage et la transmission des données



Merci de votre écoute



Urgence Cyber région Sud

CSIRT territorial PACA

 urgencecyber-regionsud.fr

En cas d'incident cyber : contactez-nous immédiatement - accompagnement gratuit et réactif

 **0 805 036 083**