CENTRE DE RESSOURCES CYBERSÉCURITÉ

LES FAUX ORDRES DE VIREMENT (FOVI)

Dordogne Périgord Le Département dordogne.fr

atd 24 Agence Technique Départementale

CCI Dordogne

SOMMAIRE

CRC 24
CENTRE DE RESSOURCES CYBERSÉCURITÉ

LE CENTRE DE RESSOURCES EN CYBERSECURITE

OBJECTIFS DU CRC24

- assurer une **résilience territoriale**
- renforcer la **confiance numérique**

4 AXES D'INTERVENTION POUR LE CRC24

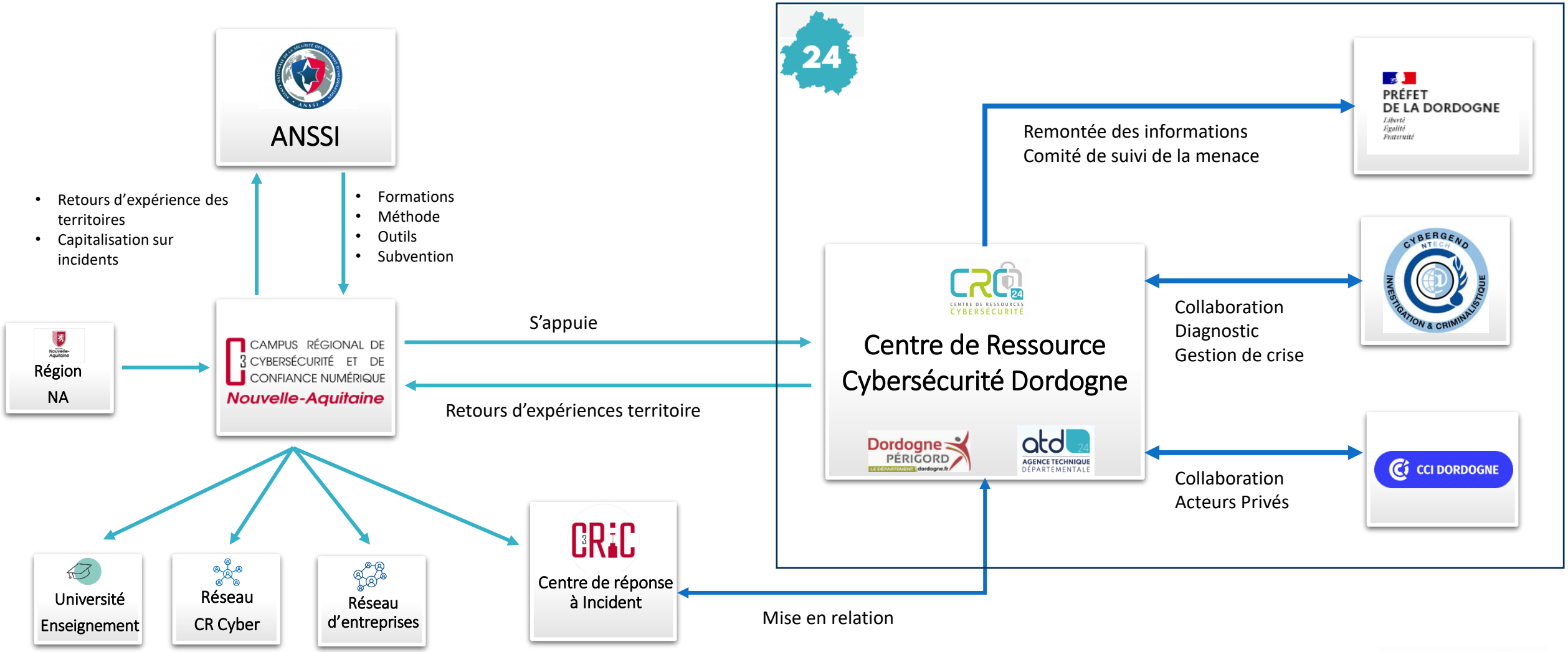
- Les **opérations**
- La **sensibilisation**
- La **formation**
- **L'accompagnement en cas de crise**

UN ACCOMPAGNEMENT COMPLET

- **Se protéger/Prévenir**
- **Gérer un incident**
- **Revenir à la normale**

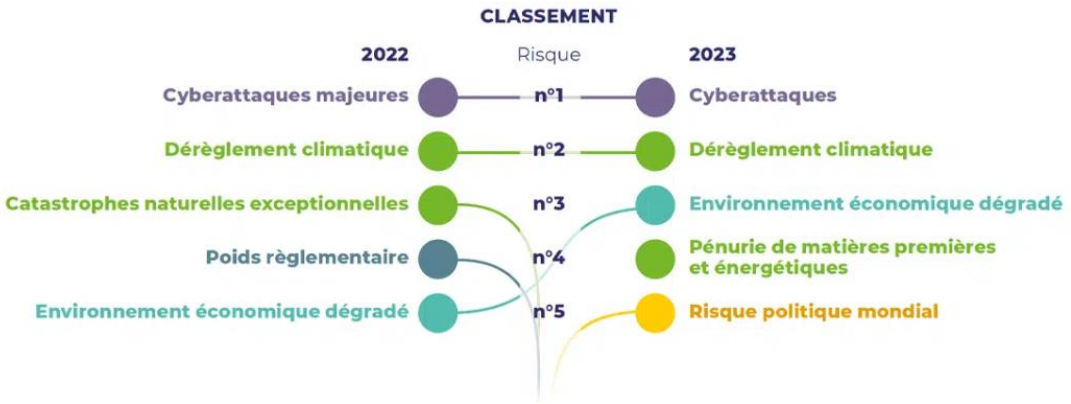
CRC 24
CENTRE DE RESSOURCES CYBERSÉCURITÉ

LE CENTRE DE RESSOURCES EN CYBERSECURITE

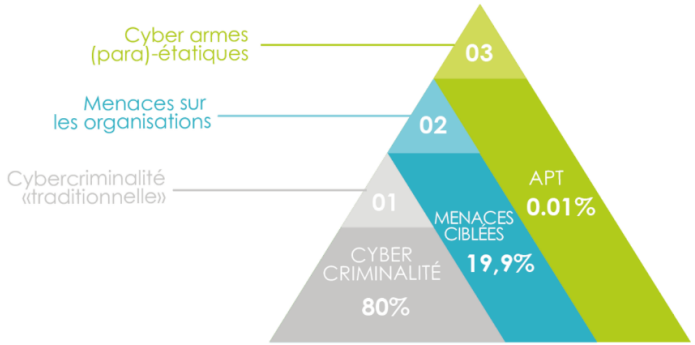


01 | LE CONTEXTE CYBERSECURITE ACTUEL

Principaux risques en France



UNE MENACE PROTÉIFORME



QUELQUES CHIFFRES

- 450 millions d'attaques pour les JO de Tokyo, on s'attend à 8 à 10 fois plus pour les JO de PARIS ;
- **Panorama de la menace 2023 – ANSSI** :
  Top 5 des victimes par rançongiciel (pris en otage du système contre une rançon) :
  1 : TPE/PME/ETI : 34% ↓
  2 : Collectivités territoriales : 24% ↑
  3 – 4 : Entreprises Stratégiques – Etablissement de Santé : 10% ↑
  5 : Association : 9% ↑
- En 2023, c'est plus de 53 cyberattaques recensées dont 33 communes, 9 EPCI/Syndicats/Régies, 5 Départements/Régions et 6 Hôpitaux/SDIS.
- En Nouvelle-Aquitaine c'est 150 incidents traités en avril et octobre 2023 par le Campus Cyber NA

CRC 24
CENTRE DE RESSOURCES CYBERSÉCURITÉ

02 | LES MOTIVATIONS DES PIRATES

ATTAQUE A BUT LUCRATIF

Principales menaces, elles prennent diverses formes : attaques par rançongiciels, attaque point d'eau, compromission de messageries professionnelles…

ATTAQUE A BUT DE DESTABILISATION

Elles consistent en une défiguration des sites internet à des fins politiques ou idéologique ("hacktivisme") et par des attaques à but de sabotage.

ATTAQUE A BUT D'ESPIONNAGE

Visant à compromettre les équipements informatiques afin d'espionner les cibles visées. Ces attaques sont réalisées majoritairement par des groupes opérant pour le compte d'États.

CRC 24
CENTRE DE RESSOURCES CYBERSÉCURITÉ

03 | C'EST QUOI L'ARNAQUE AUX FOVI

- **C'est une escroquerie pouvant provenir d'une tentative de persuasion, de menaces ou de pressions diverses**
- Le but est d'inciter une personne à effectuer un virement planifié ou non sur le compte de cybercriminels en usurpant l'identité d'un dirigeant, d'un fournisseur ou d'un employé.
- L'usurpation provient la plupart du temps d'une personne de confiance ou d'un cadre avec un caractère **« urgent et confidentiel »** ; la technique la plus connue est l'ARNAQUE AU PRESIDENT.
- On peut retrouver plusieurs variantes de FOVI :
  - Usurpation de l'identité d'un fournisseur pour communiquer de nouvelles coordonnées bancaires ;
  - Usurpation de l'identité d'un agent pour changement de coordonnées bancaires
  - Usurpation de l'identité d'un technicien informatique pour récupérer les codes bancaires
- Les escrocs utilisent souvent les mails, le téléphone (appels ou messages) ou même les 2 combinés
- Information importante : les comptes bancaires des escrocs sont souvent à l'étranger ! 
- Cette fraude fait souvent suite au piratage et à l'utilisation de la messagerie de la personne ou de l'entité usurpée 

04 | COMMENT SE PROTEGER ?

Sensibiliser et informer toutes **les personnes pouvant interagir avec les mandatements**, les demandes de virement, **la gestion des RIB**…

Attention à la réception de messages frauduleux d'hameçonnage avec des demandes d'information précises (mots de passe en particulier)

Limiter les publications d'informations permettant d'identifier et de contacter les **agents habilités à effectuer des opérations financières** (demande de virement, modification coordonnées bancaires…)

Utiliser des mots de passe solides pour l'ensemble de vos accès et activer la double authentification dès que c'est possible pour limiter les risques.

Prendre le temps de **vérifier les différents éléments** surtout si l'opération est inhabituelle ; les escrocs peuvent se montrer très insistant en émettant un caractère d'urgence.

Si un collaborateur est contacté avec insistance par une personne qui le presse d'effectuer un virement: il doit en référer immédiatement à sa hiérarchie, et au moindre doute, il est conseillé de contacté l'interlocuteur habituel pour vérifier que **l'ordre émane bien de lui**.

04 | LES PRINCIPAUX SIGNAUX QUI PEUVENT ALERTER

- Transmission de factures par messagerie électronique ou par courrier (portail chorus pro)
- Demandes de changement de coordonnées bancaires ou d’affacturage
- Courriels d'interlocuteurs utilisant des adresses électroniques suspectes : bien regarder ce qu’il y a après le @
- Demande de confirmation d'un virement ou d'une date de paiement (portail chorus pro)
- Des fautes d'orthographe, logo ou adresse de messagerie légèrement modifiés, un préfixe téléphonique inhabituel…

CRC 24
CENTRE DE RESSOURCES CYBERSÉCURITÉ

05 | QUE FAIRE SI ON EST VICTIME D'UN FOVI

Identifier le ou les virement(s) frauduleux en instance ou à venir à destination des coordonnées bancaires frauduleuses.

Informer la hiérarchie, le service « finance » et demander le blocage des coordonnées bancaires frauduleuses.

Alerter immédiatement l'établissement bancaire, demander la suspension du virement et/ou le retour des fonds.

Conserver toutes les preuves possibles : numéro de téléphone, messages ou mails reçus, les ordres de virements, les demandes de modification de RIB…..

Si l'origine de la fraude est liée à un compte de messagerie, il faut modifier le mot de passe rapidement et activer la double authentification si c'est possible.

Déposer plainte : cette action doit se faire en parallèle de tous les points précédents. L'établissement bancaire aura besoin du PV de plaine pour appuyer les démarches et la récupération des fonds.

Le temps de réaction est primordial dans ce type d'attaque

06 | EXEMPLES D'ARNAQUE AU FOVI

38 millions d'euros envolés

L'affaire démarre en décembre 2021, quand le comptable du promoteur immobilier francilien Sefri-Cime reçoit un appel. Au bout du fil, un homme qui se fait passer pour l'avocat d'un grand cabinet. L'escroc prétexte «une opération confidentielle de rachat de sociétés», le tout avec l'accord du président de l'entreprise.
Pour crédibiliser davantage le scénario, le comptable reçoit dans la foulée un courriel usurpant l'identité du PDG qui lui confirme que l'opération est réalisée à sa demande.
40 virements vont être effectués en quelques semaines pour un montant total de 38 millions d'euros
L'escroc avait insisté auprès du comptable pour qu'il n'en parle à personne et ainsi l'isoler.

Saône-et-Loire : le conseil départemental victime d'une arnaque "au faux président" à hauteur de 350 000 euros

Croyant verser une subvention au profit du Sdis de Saône-et-Loire, le conseil départemental a en fait effectué un virement bancaire sur autre compte et l'argent s'est envolé. Le versement a été effectué après la production d'un faux RIB, le piratage de la boîte mail du Sdis 71 et l'usurpation de la signature du président du conseil départemental.
Des voleurs qui ont copié le formulaire utilisé par le service habilité à demander les virements de la part de cette collectivité. Voyant la signature apposée sur le document, le service comptable du conseil départemental s'est ainsi fait prendre.
Les services de la DGFiP sont intervenus rapidement en lien avec la Banque de France pour bloquer le virement frauduleux.

06 | EXEMPLES D'ARNAQUE AU FOVI

Association de gestion et de comptabilité CDER dans la Marne

1 : Piratage Boite mail et ligne téléphonique du Président
2 : Familiariser avec son style, ses expressions..
3 : Identification personne en charge des affaires comptables

Contact par WhatsApp et par Mail en se faisant passer pour le Président pour une demande de virement à l'étranger.

Soyez discrète : rachat d'entreprise et opération boursière !

Opération réalisée une dizaine de fois pour plusieurs millions d'euros détournés !

Le « vrai » président n'a jamais été en contact avec qui que ce soit.

Appels d'un avocat factice d'un cabinet réputé pour rendre les opérations de virements crédibles

07 | GESTION DE CRISE

Je fais face à un incident,
JE CONTACTE :

et/ou

CRIC

www.campuscyber-na.fr/signaler-incident

0805.2929.40 (appel gratuit)

Vous apporte une **réponse technique**

Ouvre un incident au CRIC

CRC24 CENTRE DE RESSOURCES CYBERSÉCURITÉ

contact@crc.dordogne.fr
05.53.06.65.65

Vous indiquent les **1ers réflexes à adopter**

Parallèlement le CRC24 vous accompagne pour

- Contacter la Gendarmerie/Police
- Déposer une pré-Plainte en ligne
- Contacter le DPD (Délégué à la Protection des Données)


CRC 24
CENTRE DE RESSOURCES
CYBERSÉCURITÉ