Breizh Cyber

COMMUNIQUÉ DE PRESSE

Le mardi 19 novembre 2024,
à l'European Cyber Week de Rennes

Collectivités, associations et entreprises face aux cyber-attaques

Breizh Cyber, le centre de réponse de la Région, a traité plus de 100 incidents

« *La souveraineté numérique, comme la souveraineté alimentaire ou énergétique, est une garantie de notre indépendance* », martèle le Président Loïg Chesnais-Girard. Voilà pourquoi, il y a un an, la Région Bretagne lançait son « *Samu numérique* », selon l'expression de Jérôme Tré-Hardy, conseiller régional délégué au numérique, à la cybersécurité et aux données. La mission de Breizh Cyber ? Apporter une réponse rapide aux collectivités, associations, PME et ETI (petites et moyennes entreprises, entreprises de taille intermédiaire) victimes de cybermalveillance. Piratage, hameçonnage, rançongiciels : en un an, les experts du centre de réponse régional ont reçu plus de 300 appels et traité 114 incidents. Ils ont aussi mené des actions de prévention et de sensibilisation auprès des publics les plus divers.

Breizh Cyber a reçu **301 appels** sur son numéro vert (0 800 200 008), **traité 114 incidents et réalisé 65 signalements de vulnérabilité** au cours de sa première année d'activité, au profit des entreprises, collectivités locales ou associations du territoire.

Des incidents très variés

Dans le « top 3 » des incidents les plus courants, on trouve : le **piratage de compte**, l'**hameçonnage** (phishing) et le **rançongiciel.**

Le piratage et l'hameçonnage (le plus souvent de messageries) sont, en réalité, le prélude à d'autres attaques, comme le vol d'identifiants de connexion, ou à des tentatives de fraude au changement de RIB, par exemple.

Les rançongiciels représentent les incidents les plus graves pour les victimes : ils entraînent le plus souvent un blocage complet de l'activité.

Des **incidents sur la chaîne d'approvisionnement** logiciel sont également signalés. Octave, un éditeur spécialisé dans le commerce de détail, a été attaqué en août, entraînant dans son sillage des difficultés majeures pour nombre de ses clients, dont au moins 8 en Bretagne. Plusieurs **usurpations d'identité** d'entreprises et de collectivités locales ont également été signalées.

De droite à gauche, Jérôme Tré-Hardy, conseiller régional, Vincent Strubel, DG de l'ANSSI, Guillaume Chéreau, directeur de Breizh Cyber et son équipe

Dans 90% des cas, Breizh Cyber a la capacité d'accompagner directement les victimes dans la réponse à ces incidents. Pour les cas les plus graves et spécifiquement pour les incidents de type rançongiciel, Breizh Cyber oriente les victimes vers des prestataires d'investigation numérique et/ou de récupération de données.

Des coopérations aux niveaux national et local

À l'initiative de Breizh Cyber, les centres de réponse de métropole (CSIRT) et d'outre mer ont mené cette année une **campagne de recherche en vulné-**

SERVICE PRESSE
02 99 27 13 54 | presse@bretagne.bzh
Odile Bruley (06 76 87 49 57) | Sylvain Le Duigou (06 42 32 13 57) | Aymery Bot (07 50 12 41 30) | Sébastien Jédor (06 22 49 94 69)
www.bretagne.bzh/espace-presse @bretagne_presse

rabilité au profit de l'ensemble des **collectivités locales**. Cette initiative, rendue possible grâce à la politique d'ouverture des données de l'État, vise à renforcer la cybersécurité de ces entités publiques. Bilan : 186 d'entre elles présentaient des équipements vulnérables, parmi les 25 000 analysés, soit un taux de 0,73%.

Au niveau national, les CSIRT territoriaux sont désormais **intégrés au dispositif de réponse opérationnelle « CERT-FR » de l'ANSSI** (Agence nationale de sécurité des systèmes d'information). A ce titre, les appels reçus par le CERT-FR qui concernent des entités bretonnes sont remontés vers Breizh Cyber (et réciproquement, selon les horaires).

Au niveau local, avec la signature d'une c**onvention de coopération entre la Région Bretagne et le syndicat mixte Mégalis** pour l'année 2024, Breizh Cyber a réalisé de nombreuses actions autour de la cybersécurité au profit des collectivités locales bretonnes, en partenariat avec cet opérateur.

D'autre part, Breizh Cyber a lancé le **référencement des prestataires de réponse à incidents** qui opèrent sur le territoire breton. Ces référencements se sont matérialisés par la signature d'une **charte** définissant les engagements de chacune des parties. À ce jour, **15 prestataires de confiance** ont été référencés.

Sensibiliser tous les publics

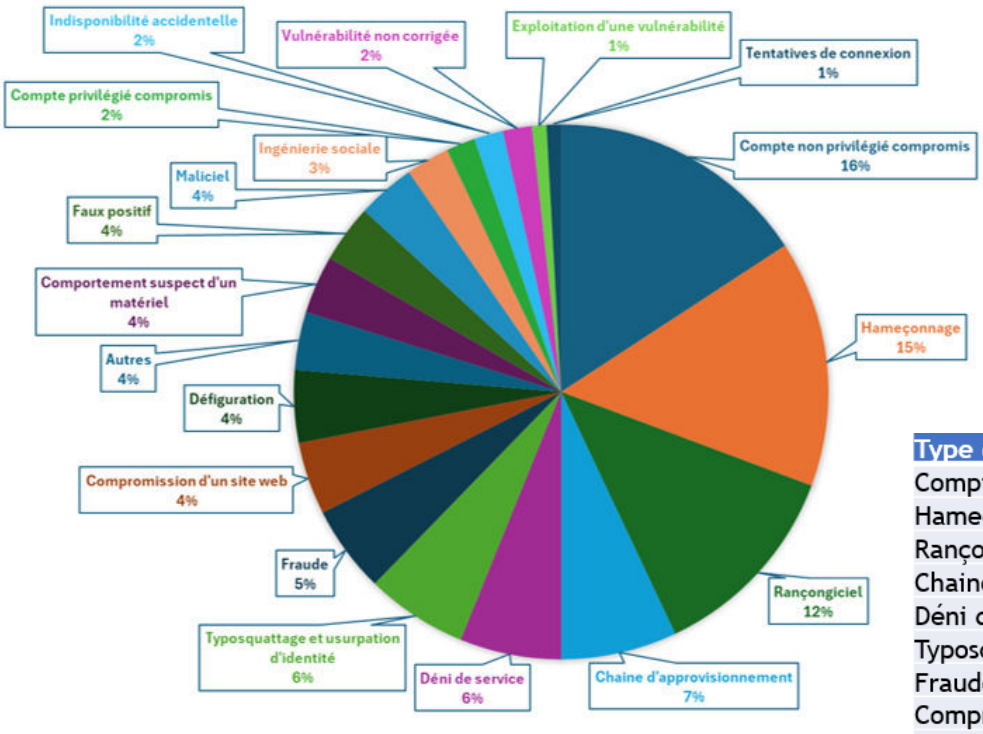
Le centre de réponse de la Région Bretagne intervient aussi auprès du grand public et des professionnels lors d'événements aussi divers que le Cybermoi/s organisé par Cybermalveillance.gouv.fr, le Forum Economique Breton, le West Web Festival, les rencontres des experts comptables de Bretagne...

Des sessions de sensibilisation sont également organisées avec des **syndicats professionnels** comme l'UIMM, le MEDEF, la CPME, le CNAM et les CCI.

Les usagers peuvent aussi s'informer sur le site web et le compte LinkedIn de BreizhCyber.

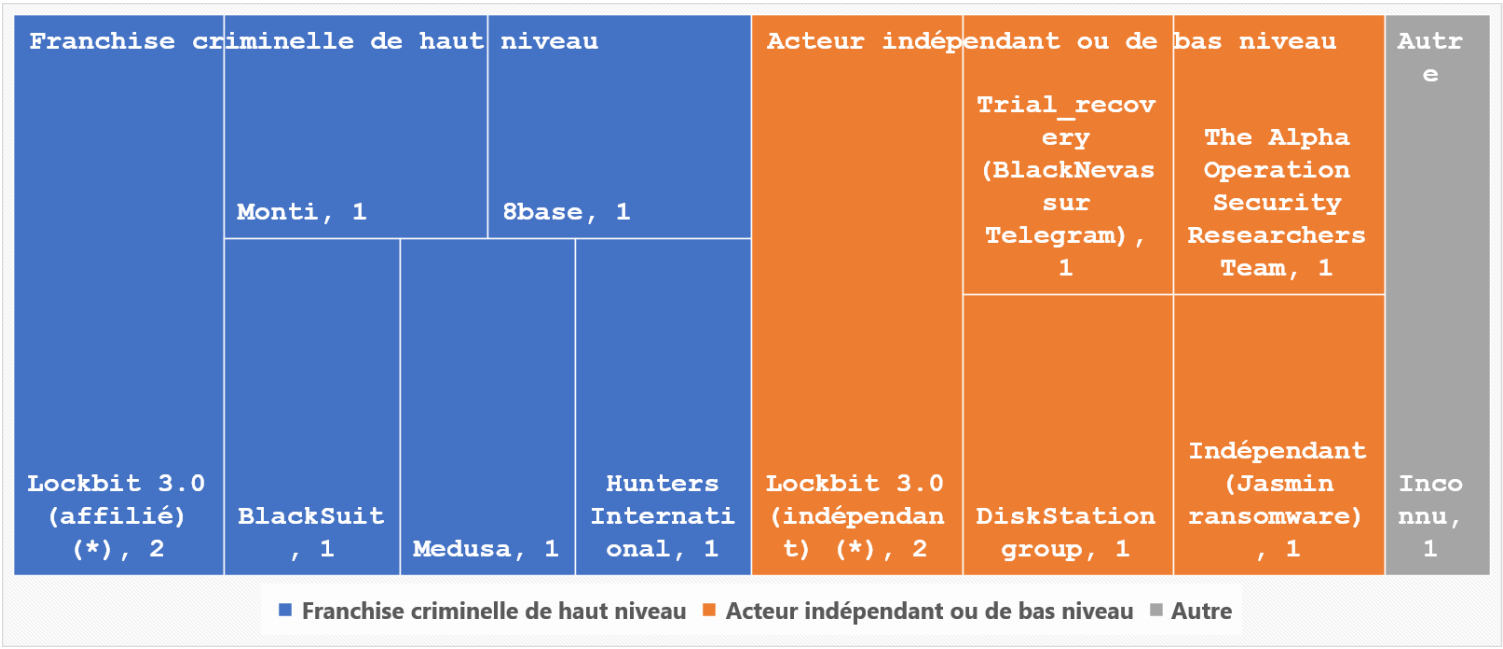
En pratique, Breizh Cyber est joignable :
> sur le site web breizhcyber.bzh
> au numéro d'urgence : 0 800 200 008 (appel gratuit)

La typologie des incidents montre la grande diversité des cas signalés à Breizh Cyber



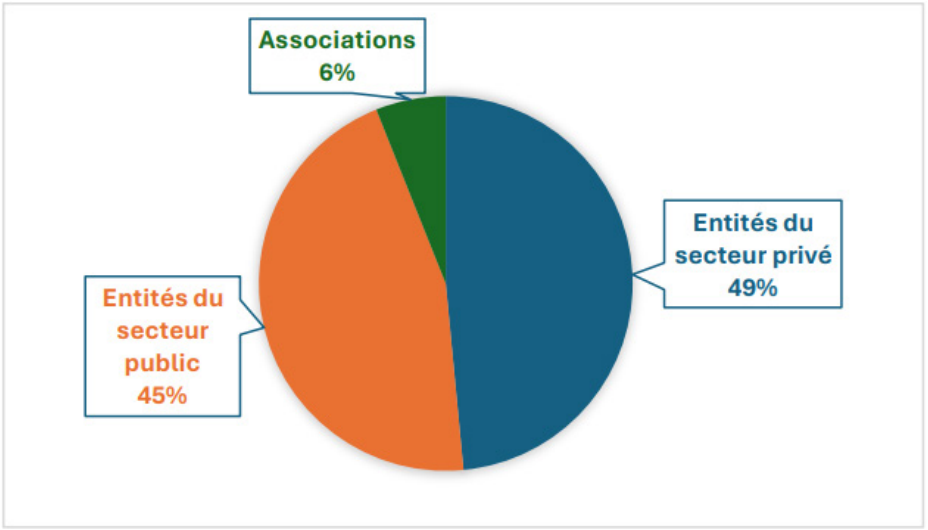
Type d'incident	Nombre
Compte non privilégié compromis	18
Hameçonnage	17
Rançongiciel	14
Chaine d'approvisionnement	8
Déni de service	7
Typosquattage et usurpation d'identité	7
Fraude	6
Compromission d'un site web	5
Défiguration	5
Autres	4
Comportement suspect d'un matériel	4
Faux positif	4
Maliciel	4
Ingénierie sociale	3
Compte privilégié compromis	2
Indisponibilité accidentelle	2
Vulnérabilité non corrigée	2
Exploitation d'une vulnérabilité	1
Tentatives de connexion	1
Total	114

Groupes criminels opérateurs de rançongiciel ayant fait des victimes en Bretagne



Définitions :
- attaque par simple extorsion : l'attaquant chiffre des données et demande rançon pour la clé de déchiffrement
- attaque par double extorsion : l'attaquant chiffre et exfiltre des données, avec menace de publication ou de vente des données volées si la rançon n'est pas payée
- indépendant : acteur criminel qui opère de manière autonome, développe ou acquiert ses propres outils et ne partage pas les revenus générés avec un groupe criminel.
- affilié : acteur criminel qui utilise les ressources fournies par le groupe criminel auquel il est affilié avec qui il partage les revenus souvent via un modèle ransomware-as-a-service (RaaS). Un acteur criminel peut être affilié à plusieurs franchises criminelles.

Profil des victimes d'incidents



Sources : Breizh Cyber


Région
BRETAGNE
Breizh Cyber