

Retour d'expérience :

Du hack à l'affaire d'état



Tobias Bolliger | Conseiller juridique Xplain AG
tobias.bolliger@xplain.ch

Stephan Bischof | Directeur général Xplain AG
stephan.bischof@xplain.ch

Agenda

Congrès Suisse d'Informatique Policière 2026

00 À propos de nous

L'entreprise, les produits et les clients

01 L'attaque

Que s'est-il passé en mai 2023 ?

02 Gestion de crise

Les 72 premières heures en état d'exception

03 Médias & affaire d'état

Du darknet à la décision du Conseil fédéral

04 Audit & reconstruction

Audit du code source, gel des livraisons, rétablissement

05 Traitement des suites 2024

Analyse OFCS, PFPDT, mesures

06 Lessons Learned

Ce que l'incident a réellement appris



À propos de nous

Xplain AG



Xplain développe **depuis 2000** avec quelque 60 collaborateurs des applications spécialisées pour :

- Police
 - Ministères publics
 - Tribunaux
 - Exécution des peines et mesures
 - Offices des migrations
- au niveau **fédéral, cantonal et communal**.

Xplain n'héberge **aucune** donnée client et n'a pas accès aux systèmes en production. Le logiciel fonctionne sur l'infrastructure des clients.





L'attaque

Samedi matin, fin mai 2023 – PLAY Ransomware, Double Extortion

"Nous avons été piratés – tous les systèmes chiffrés."

CEO Xplain AG par téléphone à ses plus proches collaborateurs

PLAY Ransomware

Double Extortion : chiffrement + menace de fuite

Actif depuis 2022, nombreuses victimes dans le monde

907 GB

volume de données publié

14 jours

minuterie darknet avant la fuite



Gestion de crise

Les **72 premières heures** – BCM comme base, communication comme clé

1

H. 0–6 | Détection & isolation

CEO alerte l'équipe. Serveurs hors ligne. Plan de reprise activé. Le BCM fonctionne – le véritable marathon ne fait que commencer.

2

H. 6–24 | OSINT & SOMAS

Tor, GitHub, forums de fuite parcourus. PLAY identifié. Sauvegardes, plan de reprise, etc.

3

H. 24–48 | Autorités & assurance

Plainte pénale déposée auprès de la police cantonale bernoise. Matériel informatique séquestré. NCSC, fedpol, OFDF, assurance cyber informés. Premiers rapports de situation.

4

H. 48–72 | Préparation de la communication

Courriers clients. FAQ médias élaborée. Récit défini : **aucune rançon, transparence totale**, faits plutôt que spéculation.



Du darknet aux gros titres

Juin 2023 – 1,3 million de fichiers – 1,3 million de fichiers rendus publics

Mi-juin 2023 : PLAY publie 907 Go – des documents opérationnels de la Confédération et des cantons sont accessibles publiquement. Des centaines d'articles dans les médias en deux

Pourquoi les médias ont été si rapidement informés :

Semaines auparavant : un grand groupe de presse suisse avait lui-même été victime de PLAY. La rédaction d'investigation surveillait quotidiennement le forum de fuite darknet du groupe depuis lors.

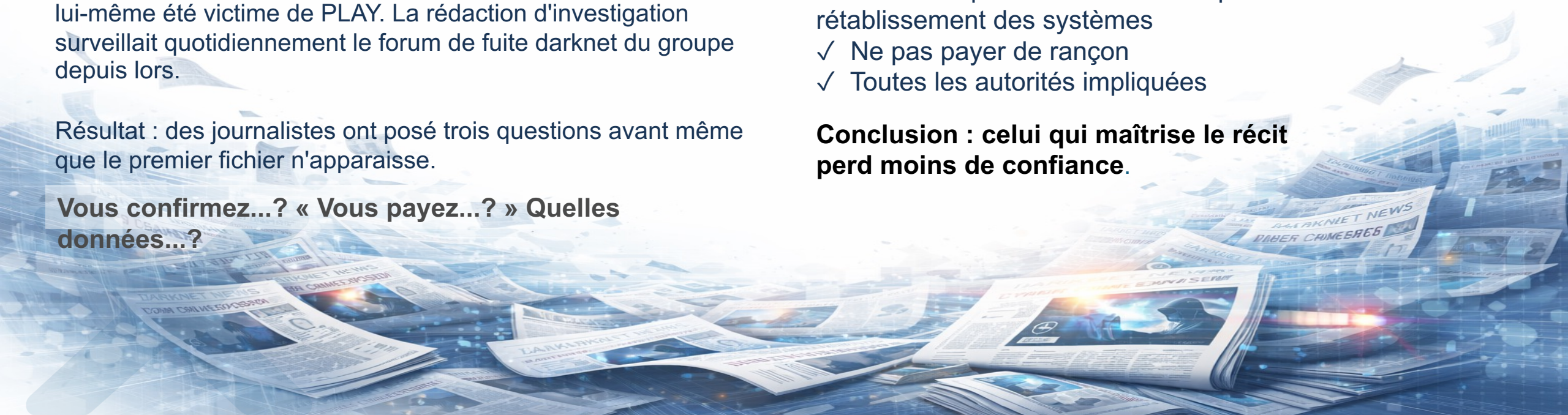
Résultat : des journalistes ont posé trois questions avant même que le premier fichier n'apparaisse.

Vous confirmez...? « Vous payez...? » Quelles données...?

Notre stratégie de communication :

- ✓ Confirmer l'attaque, pas de spéculation
- ✓ Communiquer de manière transparente sur le rétablissement des systèmes
- ✓ Ne pas payer de rançon
- ✓ Toutes les autorités impliquées

Conclusion : celui qui maîtrise le récit perd moins de confiance.



L'affaire d'État

28 juin 2023 – Le Conseil fédéral crée la cellule de crise PSK-D

Pour la première fois dans l'histoire suisse: état-major de crise politico-stratégique
Fuite de données (**PSK-D**) sous la direction du Département des finances.

Mesures immédiates de la Confédération

Protocoles d'urgence internes à la Confédération activés. Systèmes concernés isolés.

Audit du code source

L'OFCS scelle le code source de Xplain.
Examen complet de chaque historique de commit.

Lignes de communication

Lignes unifiées pour la Confédération, les cantons et tous les fournisseurs IT.

Gel des livraisons

Aucune livraison jusqu'à ce qu'un audit externe confirme « aucune porte dérobée ».

Vérification des contrats

Révision de l'ensemble des contrats des fournisseurs IT de la Confédération.

Conséquences financières

Les clients gèlent les factures. Pression sur la liquidité jusqu'en novembre 2023.



Audit & reconstruction

Été à novembre 2023 – sous le regard de la Confédération et de l'OFCS

Chaque historique de commit, chaque script Jenkins, chaque artefact de build examiné de manière forensique. Seul le sceau «aucune porte dérobée» a ouvert la voie.

Juin/juil. 2023

Examen forensique

Auditeurs internes et externes. Chaque historique de commit, scripts Jenkins, artefacts.

Août 2023

Enquête administrative

Le Conseil fédéral ordonne la mise au point complète de toutes les circonstances.

Nov. 2023

Rapport final & autorisation

Verdict : infrastructure reconstruite, processus traçables. Gel des livraisons levé.

**8 février 2024 : résultat annuel 2023 à l'équilibre.
Aucun départ non souhaité de collaborateurs.**



Traitement des suites 2024

Analyse OFCS, PFPDT & enquête administrative

7 mars 2024 : l'OFCS présente les chiffres. 2 mai 2024 : le PFPDT et l'enquête administrative sont publiés.

1'300'000

fichiers volés au total

65'000

provenant d'autorités fédérales (5 %)

Points critiques (PFPDT / enquête administrative) :

- * Formulations contractuelles peu claires côté Confédération
- * Routines de suppression insuffisantes chez Xplain
- * Aucune autorisation «need-to-know» appliquée

Titre médias : chaîne d'erreurs chez la Confédération et le fournisseur

Mesures (toutes mises en œuvre avant le rapport) :

- ✓ Autorisations need-to-know dans tous les processus de support
- ✓ Politiques de suppression obligatoires introduites
- ✓ Formation protection des données pour tous les collaborateurs
- ✓ Vérifications de conformité auditées en externe



Enquêtes pénales pas encore clôturées

Nouveau niveau de maturité

Zero Trust, auditabilité & transparence comme ADN



Domaine d'action	Ce qui a été mis en œuvre
Architecture Zero Trust	MFA, moindre privilège, réseaux segmentés, surveillance continue
Processus auditables	SOC 2 Type II annuel, contrôles CIS Benchmark automatisés
Résilience financière	Ligne de crédit de secours, assurance cyber, scénario de gel des livraisons intégré à la planification de liquidité
Garantie de confiance	Classification stricte des données, need-to-know, politiques de suppression

2024 : Chapters Group acquiert Xplain.



Leçons apprises

Quatre enseignements – directement tirés de la pratique

1

Le BCM n'est que la phase 1

Le rétablissement informatique ne fait que lancer le marathon juridique, de surveillance et de communication.

→ Créer un chapitre distinct After-Action et Legal Track dans le manuel BCM.

2

La transparence protège la réputation

Des rapports de situation ouverts maintiennent le récit sous contrôle propre. Communication proactive = nettement moins de pertes de clients.

→ Préparer un guide de communication avec des niveaux d'escalade.

3

La résilience financière et structurelle nécessite une préparation

La pression sur les liquidités survient souvent des semaines après l'attaque – les clients gèlent les factures.

→ Mettre en place dès aujourd'hui une ligne de crédit de secours, une assurance cyber et une planification de liquidité.

4

Les collaborateurs sont le facteur clé

La charge psychologique dure plus longtemps que le ticket d'incident.

→ Désigner une personne de confiance, communiquer honnêtement. Programmes de résilience : jusqu'à -30 % de rotation.

La sécurité n'est pas un état –
c'est un processus.

Celui qui l'a traversé –
est xperienced.



Stephan Bischof | Xplain AG
stephan.bischof@xplain.ch

Tobias Bolliger | Xplain AG
tobias.bolliger@xplain.ch