Harvest-Now-Decrypt-Later : Protéger vos Données DSI

> La menace HNDL est active dès aujourd'hui : adversaires collectent vos données chiffrées pour déchiffrer demain. Checklist DSI et mesures immédiates.

La menace Harvest-Now-Decrypt-Later (HNDL) — littéralement « collecter maintenant, déchiffrer plus tard » — est la raison pour laquelle la préparation post-quantique n'est pas une question d'avenir mais d'urgence présente. Contrairement à la plupart des cybermenaces qui nécessitent d'être actives pour causer des dommages, le HNDL fonctionne sur un horizon temporel inversé : l'attaque se produit aujourd'hui, les dommages se matérialisent dans 5 à 10 ans. Des acteurs étatiques — et peut-être déjà certains groupes criminels bien dotés — interceptent et stockent en masse des communications chiffrées avec les algorithmes actuels RSA et ECC, en attendant de disposer d'un ordinateur quantique suffisamment puissant pour les déchiffrer. Pour un DSI dont la mission est de protéger les données de son organisation, cette réalité change fondamentalement l'équation temporelle de la gestion des risques : il ne suffit plus de s'assurer que vos données sont sécurisées aujourd'hui. Il faut s'assurer qu'elles le resteront pendant toute la durée de leur cycle de vie utile.

Comprendre la mécanique du Harvest-Now-Decrypt-Later

Comment fonctionne l'attaque

Le HNDL exploite une propriété fondamentale des algorithmes à clé publique actuels : le texte chiffré ne révèle rien sur le contenu si la clé privée est inconnue, mais il contient toute l'information nécessaire pour déchiffrer le contenu une fois la clé privée connue ou recalculée.

Concrètement, un attaquant HNDL :

Intercepte des flux de réseau chiffrés (trafic TLS, VPN, échanges de fichiers chiffrés) et les enregistre dans des systèmes de stockage massif.

Stocke ces données chiffrées pendant des années, en attendant de disposer d'un ordinateur quantique suffisamment puissant.

Une fois le CRQC disponible, utilise l'algorithme de Shor pour recalculer la clé privée RSA ou ECC correspondant à la clé publique visible dans les échanges interceptés.

Déchiffre l'ensemble des communications stockées depuis des années.

La sophistication de cette attaque réside dans sa temporalité : l'interception est passive (et donc indétectable), le déchiffrement est différé, et les dommages surviennent longtemps après les faits.

Un plan d'affaires dérobé aujourd'hui peut encore avoir une valeur compétitive stratégique dans 7 ans.

Pourquoi Perfect Forward Secrecy n'est pas suffisant

Un DSI averti pourrait objecter : « nous utilisons TLS 1.3 avec Perfect Forward Secrecy (PFS), ce qui signifie que chaque session génère des clés éphémères — l'interception d'une session n'expose pas les autres ». C'est partiellement juste. Le PFS protège effectivement contre la compromission de la clé de session après coup, dans le cas d'une attaque classique.

Mais face à un CRQC, le PFS ne protège pas si l'algorithme d'échange de clés éphémères est lui-même vulnérable. TLS 1.3 utilise ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) pour l'échange de clés — et ECDHE est précisément l'un des algorithmes que l'algorithme de Shor peut casser. Autrement dit : l'attaquant HNDL enregistre l'intégralité de l'échange TLS, incluant le handshake ECDHE. Avec un CRQC, il peut recalculer la clé de session ECDHE éphémère et déchiffrer la session complète.

La seule protection efficace contre le HNDL dans TLS est d'utiliser un algorithme d'échange de clés post-quantique (ML-KEM) dès maintenant — même hybride. Les sessions établies après le déploiement de ML-KEM ne seront pas déchiffrables par un futur CRQC, car ML-KEM ne dépend pas de la factorisation ou du logarithme discret.

Qui pratique le HNDL et depuis quand ?

Les États-nations : les acteurs principaux

Le programme PRISM révélé par Edward Snowden en 2013 a montré que la NSA interceptait massivement du trafic internet — y compris chiffré. Le programme BULLRUN, également révélé par Snowden, documentait les efforts de la NSA pour affaiblir et contourner les algorithmes de chiffrement. Qu'il s'agisse de la NSA, du GCHQ britannique, de la Direction Technique de la DGSE française, du GRU ou du PLA chinois, les grandes agences de

renseignement disposent des capacités d'interception massive et des infrastructures de stockage nécessaires à une stratégie HNDL.

> ⚡ **Retour terrain**
>
> Dans mes missions d'audit, je rencontre régulièrement la même configuration à risque : des règles de firewall héritées depuis 5 à 10 ans, que personne n'ose supprimer par crainte de casser quelque chose. J'ai développé une méthode de nettoyage progressive — analyser les logs de connexion sur 90 jours, identifier les règles sans trafic, les désactiver sans supprimer pendant 30 jours, puis valider avec les équipes métier. Sur un parc de 340 règles dans un groupe logistique, nous en avons supprimé 218 sans incident.

La Chine est particulièrement identifiée comme acteur HNDL par les agences de renseignement occidentales. Dans un rapport de 2023, la NSA estimait que la Chine investissait massivement dans la collecte de données chiffrées en prévision de la disponibilité de CRQC. Les secteurs ciblés prioritairement : la défense, l'aérospatiale, les technologies de pointe, la pharmacie, l'énergie nucléaire et l'industrie militaire.

Les groupes criminels organisés

Le HNDL par des acteurs non étatiques reste aujourd'hui moins probable — il nécessite des capacités d'interception réseau (accès aux câbles sous-marins, aux points d'échange internet) qui dépassent les moyens de la plupart des groupes criminels. Mais cette barrière pourrait diminuer si des services HNDL « as-a-service » apparaissaient sur des marchés criminels — permettant à des acteurs moins dotés de louer des capacités de stockage HNDL et de revendre les données déchiffrées ultérieurement.

À RETENIR

Points clés à retenir

La menace HNDL est active maintenant : des adversaires collectent probablement déjà vos données chiffrées.

Le Perfect Forward Secrecy ne protège pas contre le HNDL si l'échange de clés est ECDHE — seul ML-KEM protège.

Les secteurs les plus ciblés : défense, santé, finance, énergie, industrie de pointe, R&D.

Le risque HNDL est proportionnel à la valeur des données sur 10 ans, pas sur 1 an.

Mesures immédiates : déployer ML-KEM dans TLS, activer PFS partout, raccourcir les durées de vie des clés.

Le RGPD impose de protéger les données selon l'état de l'art — inclut désormais le risque PQC.

Quelles données sont ciblées en priorité ?

L'équation valeur × durée de vie

Le risque HNDL est le produit de la valeur des données et de leur durée de vie utile. Une donnée qui vaut un million d'euros mais devient obsolète dans six mois présente un risque HNDL limité. Une donnée de valeur moyenne mais qui conserve sa pertinence pendant 15 ans est une cible HNDL de premier ordre.

La politique de classification de l'information ISO 27001 doit intégrer une dimension temporelle : pour chaque classe de données, quelle est la durée de vie utile de la confidentialité ?

Les données à risque HNDL élevé

Propriété intellectuelle industrielle : brevets en cours, formules, processus de fabrication. Dans l'industrie pharmaceutique, les données de R&D d'un médicament en développement ont une valeur compétitive de 10 à 20 ans.

Données de défense et d'armement : plans de systèmes d'armes, capacités militaires, positionnement de forces. Ces données peuvent rester sensibles des décennies.

Données diplomatiques et négociations stratégiques : positions de négociation dans des fusions-acquisitions, des contrats d'armement, des accords commerciaux.

Données de santé : les données médicales individuelles ont une durée de vie de protection couvrant toute la vie de la personne concernée — leur exposition via HNDL crée un risque RGPD structurel.

Infrastructure critique : cartographies réseau d'OIV/OSE, schémas SCADA, plans de résilience. Cette information peut être exploitée pour des attaques futures contre des infrastructures dont la configuration n'a pas changé.

Données financières stratégiques : résultats financiers non publiés, plans d'investissement, informations sur les fusions en préparation. L'exploitation différée d'informations financières constitue un délit d'initié différé.

Clés cryptographiques et secrets d'authentification : si des clés privées RSA ou des secrets partagés sont transmis chiffrés sur le réseau, leur interception aujourd'hui permet leur compromission future — compromettant rétroactivement tous les systèmes qu'ils protégeaient.

Mesures immédiates : protéger dès aujourd'hui

1. Déployer ML-KEM dans TLS dès maintenant

C'est la mesure la plus impactante et la plus rapide à déployer. Configurer les serveurs web, reverse proxies et passerelles VPN pour proposer ML-KEM-768 (en mode hybride X25519+ML-KEM) en priorité dans la liste des groupes TLS. Les navigateurs modernes (Chrome 124+, Edge,

Firefox récent) négocieront automatiquement en ML-KEM hybride. Les clients anciens continueront avec ECDHE classique.

Impact : les sessions TLS négociées en ML-KEM ne pourront pas être déchiffrées par un CRQC futur — même si l'ensemble du trafic est enregistré aujourd'hui. C'est une protection HNDL directe et immédiate.

2. Activer le Perfect Forward Secrecy partout

Si vous utilisez encore des suites cipher TLS sans PFS (notamment dans des configurations héritées TLS 1.2 avec RSA key exchange non-ephemeral), migrez immédiatement vers des suites avec ECDHE ou DHE. Bien que le PFS classique ne protège pas contre un CRQC, il réduit la valeur du HNDL en limitant chaque capture à une session individuelle plutôt qu'à toutes les sessions d'un même serveur.

3. Réduire les durées de vie des clés et secrets

Les secrets à longue durée de vie sont les cibles HNDL les plus précieuses. Révisez la politique de rotation des clés :

Clés de chiffrement symétrique (AES) pour les bases de données : rotation tous les 12 mois maximum.

Certificats TLS de serveur : déjà limités à 90 jours (Let's Encrypt) ou 1 an par les CA publiques. Maintenez ce rythme.

Secrets de sessions VPN : activez la rotation automatique (IKEv2 rekeying) avec des intervalles de 4 heures maximum pour les connexions sensibles.

Clés API et secrets de services : rotation mensuelle pour les services critiques, trimestrielle pour les autres.

Mots de passe de service et comptes applicatifs : rotation semestrielle.

Le registre des risques ISO 27001 doit inclure une ligne dédiée au risque HNDL avec l'évaluation de la durée de vie des actifs les plus sensibles.

4. Chiffrement à longue durée de vie : passer au symétrique

Pour les données archivées à long terme (archives légales, données de R&D, historique médical), le chiffrement asymétrique est une mauvaise option sur le plan HNDL. Utilisez AES-256 pour chiffrer les données au repos — l'algorithme de Grover réduit sa sécurité effective à 128 bits, ce qui reste bien au-dessus des capacités de déchiffrement prévisibles. Si vous devez transmettre la clé AES pour un archivage chiffré à long terme, enveloppez-la avec ML-KEM plutôt qu'avec RSA.

5. Segmentation et minimisation des flux exposés

Tous les flux ne méritent pas la même attention HNDL. Identifiez les flux contenant des données à risque HNDL élevé et assurez-vous qu'ils passent exclusivement par des canaux ML-KEM. Segmentez le réseau pour isoler ces flux des communications ordinaires. L'approche Zero Trust — qui exige une authentification et un chiffrement pour chaque flux, même interne — est le cadre naturel pour implémenter cette segmentation.

Implications RGPD de la menace HNDL

L'obligation de sécurité selon l'état de l'art

L'article 32 du RGPD exige que les responsables de traitement mettent en œuvre des mesures techniques assurant un niveau de sécurité « approprié au risque », en tenant compte notamment « de l'état des techniques ». En 2026, l'état des techniques en matière de cryptographie évolue vers le post-quantique : les standards NIST sont finalisés, les navigateurs déploient ML-KEM, les agences gouvernementales recommandent la migration. Dans ce contexte, un responsable de traitement qui ne prend aucune mesure pour protéger des données à longue durée de vie contre le HNDL pourrait être considéré comme ne respectant pas l'état de l'art.

La politique DLP et de prévention de fuite de données doit intégrer la dimension HNDL : les mesures de prévention ne couvrent pas seulement le vol de données en clair, mais aussi la capture de données chiffrées en transit.

Durées de conservation et risque HNDL

Le RGPD impose la minimisation des données et la limitation des durées de conservation. Ces principes ont une résonance particulière dans le contexte HNDL : des données conservées longtemps créent un risque HNDL accru. La revue des durées de conservation doit intégrer une dimension post-quantique : est-il pertinent de conserver des données pendant 10 ans si elles seront potentiellement accessibles à un adversaire dans 7 ans ?

Pour certaines catégories (données médicales, archives judiciaires), les durées de conservation sont imposées par la loi et ne peuvent être raccourcies. Dans ces cas, la protection post-quantique du stockage (chiffrement AES-256 des données au repos, accès via ML-KEM) devient d'autant plus critique.

Notification de violation et HNDL

Si une organisation découvre qu'elle a été victime d'une interception massive de données chiffrées (HNDL présumé), est-elle tenue de notifier la CNIL et les personnes concernées ? La réponse n'est pas encore tranchée par la jurisprudence ou les lignes directrices du EDPB. Mais si les données chiffrées interceptées concernent des données personnelles et que les algorithmes de chiffrement utilisés sont connus pour être vulnérables à un CRQC imminent, l'argument que « les données sont chiffrées donc non exposées » pourrait ne pas suffire. Consultez votre DPO et votre conseil juridique pour anticiper cette question.

Checklist HNDL pour les DSI : actions par priorité

Actions immédiates (0-3 mois)

☐ Activer ML-KEM hybride dans la configuration TLS de tous les serveurs exposés (mise à jour OpenSSL + configuration Nginx/Apache).

☐ Vérifier que PFS (ECDHE) est activé sur toutes les connexions TLS — désactiver les suites non-PFS résiduelles.

☐ Identifier les 5 à 10 flux réseau les plus sensibles (forte valeur, longue durée de vie) et vérifier leur protection.

☐ Inventorier les clés et secrets à durée de vie supérieure à 3 ans — planifier leur rotation.

☐ Former le RSSI et les architectes sécurité aux concepts de base du HNDL et de la cryptographie post-quantique.

Actions à court terme (3-12 mois)

☐ Réaliser l'inventaire cryptographique complet du SI (certificats, clés, configurations protocolaires).

☐ Intégrer le risque HNDL dans le registre des risques ISO 27001 avec cotation et plan de traitement.

☐ Mettre à jour la politique de cryptographie (A.8.24) pour inclure les exigences PQC.

☐ Mettre à jour la politique de classification de l'information pour inclure la durée de vie de confidentialité.

☐ Évaluer les HSM actuels pour leur compatibilité PQC — lancer les appels d'offres de remplacement si nécessaire.

☐ Inclure des clauses PQC dans les nouveaux contrats fournisseurs et sous-traitants.

☐ Briefer le COMEX et le conseil d'administration sur la menace HNDL et le programme de migration PQC.

Actions à moyen terme (1-3 ans)

☐ Lancer le pilote PKI hybride (ML-DSA + ECDSA).

☐ Migrer les VPN critiques vers IKEv2 + ML-KEM.

☐ Remplacer le chiffrement RSA/ECC des archives à long terme par AES-256.

☐ Déployer ML-KEM dans les accès SSH aux systèmes critiques (OpenSSH 9.0+).

☐ Intégrer les exigences PQC dans les analyses d'impact sur la vie privée (AIPD/DPIA) pour les nouveaux traitements.

Cas sectoriels : adapter la protection HNDL à votre contexte

Santé et pharmaceutique

Le risque HNDL est maximal dans ce secteur. Les données de R&D pharmaceutique (séquences génétiques, résultats d'essais cliniques) peuvent valoir des milliards et rester stratégiques 20 ans. Les données patients (DSP, dossiers médicaux) sont protégeables pendant toute la vie. Priorité absolue à la migration ML-KEM sur les connexions portant des données de R&D, et au chiffrement AES-256 des archives patients. Le cadre de l'analyse d'impact métier (BIA) doit intégrer le scénario de déchiffrement HNDL des données R&D comme scénario de sinistre majeur.

Finance et assurance

Le risque HNDL dans la finance porte principalement sur les données de trading, les stratégies d'investissement et les informations sur les fusions-acquisitions en préparation. Les flux de trading haute fréquence, s'ils sont interceptés et déchiffrés, pourraient permettre à un adversaire de reconstruire des stratégies algorithmiques propriétaires. Priorité à la migration ML-KEM sur les connexions vers les systèmes de trading et les plateformes de gestion d'actifs.

Industrie et défense

C'est le secteur le plus ciblé par le HNDL étatique. Les plans de conception d'armements, les caractéristiques de performance, les secrets de fabrication — autant d'informations qui conservent une valeur stratégique sur des décennies. L'ANSSI recommande aux industriels de défense de traiter le HNDL comme une priorité opérationnelle immédiate, au même titre que les menaces APT actuelles. Les systèmes d'information classifiés sont soumis à des règles spécifiques — consultez l'ANSSI pour les systèmes de niveau Diffusion Restreinte et supérieur.

Énergie et infrastructures critiques

La cartographie des réseaux SCADA, les schémas des centrales, les protocoles de communication des systèmes de contrôle — ces informations gardent leur pertinence des décennies. Un adversaire qui dispose aujourd'hui d'une capture du trafic chiffré d'un réseau SCADA pourrait, dans 7 ans, comprendre la topologie complète d'une infrastructure critique et planifier une attaque physique ou cyber avec une précision redoutable.

Liens avec les référentiels de conformité

La protection contre le HNDL s'intègre dans les référentiels de conformité existants :

ISO 27001 A.8.24 : politique de cryptographie — inclure explicitement les algorithmes post-quantiques et les exigences de protection HNDL.

ISO 27001 A.8.12 : prévention de la fuite de données — étendre la DLP au chiffrement des données en transit pour limiter l'exposition HNDL.

NIS 2 Article 21 : mesures de sécurité pour les OIV/OSE — la migration PQC est une mesure de sécurité appropriée à inclure dans le plan de conformité NIS 2.

DORA (finance) : résilience opérationnelle numérique — les risques HNDL doivent apparaître dans les analyses de risque ICT sous DORA.

RGPD Article 32 : sécurité du traitement selon l'état de l'art — inclure la protection HNDL pour les données personnelles à longue durée de vie.

Le Référentiel Général de Sécurité (RGS) de l'ANSSI est en cours de mise à jour pour intégrer les exigences post-quantiques — suivez son évolution pour les systèmes d'information des administrations et collectivités.

FAQ

Comment savoir si mes données ont déjà été interceptées dans le cadre d'une attaque HNDL ?

Il est généralement impossible de le savoir avec certitude. L'interception passive de flux réseau ne laisse pas de traces dans les systèmes de la victime — contrairement à une intrusion qui déclenche des alertes SIEM ou laisse des artefacts. Les indices indirects peuvent être une anomalie dans les logs de routeurs en bordure, une alerte de renseignement sur des comportements d'acteurs étatiques ciblant votre secteur, ou une notification de partenaires ou de services gouvernementaux. La réponse pratique : assumez que vos flux non protégés par ML-KEM ont potentiellement été interceptés, et agissez en conséquence.

La menace HNDL concerne-t-elle aussi les données au repos (bases de données, sauvegardes) ?

Le HNDL classique cible les données en transit — les flux réseau interceptables. Mais il existe un risque similaire pour les données au repos si elles sont chiffrées avec des algorithmes asymétriques vulnérables. Par exemple, une base de données dont la clé de chiffrement est enveloppée avec RSA-2048 dans un fichier de sauvegarde accessible à un attaquant pourrait être déchiffrée une fois un CRQC disponible. La protection des données au repos doit utiliser AES-256 pour le chiffrement des données elles-mêmes, et ML-KEM pour la protection des clés de chiffrement.

Quelle est la différence entre HNDL et le vol de données classique ?

Le vol de données classique vise des données en clair ou déchiffre les données en temps réel (l'attaquant accède au système où les données sont déchiffrées). Le HNDL capture des données chiffrées sans pouvoir les lire immédiatement, en pariant sur la disponibilité future d'un CRQC. Le HNDL est donc indétectable (pas d'accès au système cible), passif (capture de flux réseau en dehors du périmètre de la victime), et différé dans ses effets. Cela le rend fondamentalement différent dans sa gestion : vous ne pouvez pas réagir après coup, vous devez prévenir maintenant.

Est-il trop tard si je n'ai pas encore déployé ML-KEM ?

Non, il n'est pas trop tard. Les données transmises après le déploiement de ML-KEM seront protégées contre le HNDL futur. Le déploiement de ML-KEM dans TLS prend quelques jours techniques — c'est l'une des migrations de sécurité les plus rapides à implémenter pour son niveau de protection. Chaque jour de délai expose davantage de données sensibles. Commencez par les serveurs hébergeant les données les plus sensibles et étendez progressivement à l'ensemble du SI.

Sources

ANSSI CERT-FR — Publications et alertes

MITRE ATT&CK — Framework des techniques d'attaque

CISA — Advisories de cybersécurité