PANORAMA DE LA MENACE RANSOMWARE 2025

par le CERT-XMCO

We deliver cybersecurity

Plus de **7 300** tentatives d'extorsion par ransomware revendiquées en 2025 à l'international, dont **173** opérations criminelles contre des entités françaises.

Une instrumentalisation régulière des groupes cybercriminels par des **acteurs étatiques russes, chinois, iraniens et nord-coréens** à des fins diverses.

Un écosystème cybercriminel qui demeure **résilient** malgré les opérations des forces de l'ordre et les tentatives de **déstabilisations internes**.

Direction de la publication : XMCO
Conception : plusdebleu.com
Date de publication : Septembre 2026
Crédit photo : AdobeStock

Avant-propos

OBJECTIFS DU PANORAMA DE LA MENACE RANSOMWARE

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.

PRÉAMBULE DU PANORAMA DE LA MENACE RANSOMWARE

L'année 2025 a confirmé l'ancrage durable de la menace ransomware dans le paysage cyber, tant par la diversité des groupes actifs que par la sophistication et l'adaptabilité de leurs modes opératoires. Certains collectifs, à l'image de Qilin et de TheGentlemen, se sont distingués par leur omniprésence et leur capacité à maintenir une pression constante sur les organisations, à l'international comme en France. L'analyse de leurs activités criminelles, de leur victimologie et de leurs méthodes d'extorsion met ainsi en évidence des tendances qui dépassent le seul cadre de l'année 2025 et constituent des indicateurs précieux pour appréhender l'évolution de la menace en 2026 et dans les années à venir.

Les événements observés en 2026 viennent renforcer ces enseignements et illustrent la continuité, mais également l'amélioration, des stratégies employées par les groupes de ransomware. Le retour de Cl0p, notamment à travers le ciblage actif d'instances PTC Windchill et FlexPLM, rappelle que l'exploitation de vulnérabilités demeure un vecteur d'intrusion privilégié. Parallèlement, la menace ne se limite plus à des groupes cybercriminels indépendants : la distribution de Medusa ransomware par un sous-groupe associé au cluster nord-coréen Lazarus, ainsi que la recrudescence d'attaques par ransomware menées par des proxies étatiques iraniens, illustrent la porosité croissante entre cybercriminalité et intérêts étatiques.

Dans ce contexte, l'étude des groupes de ransomware observés en 2025 constitue un socle indispensable pour comprendre les dynamiques de cette menace pour les organisations françaises à moyen et long terme. L'identification des acteurs, de leurs cibles, des vulnérabilités exploitées, de leurs éventuelles affiliations étatiques, ainsi que de leurs mécanismes d'extorsion permet de dégager des constantes tout en anticipant leurs évolutions. Les enseignements tirés de 2025 doivent être considérés non comme un bilan figé, mais comme une base d'analyse prospective : les tendances déjà observées, confirmées ou amplifiées en 2026, appellent à maintenir une vigilance durable et à intégrer ces indicateurs dans les stratégies de prévention, de détection et de réponse aux incidents ransomware pour les années à venir.

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.

Sommaire

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.

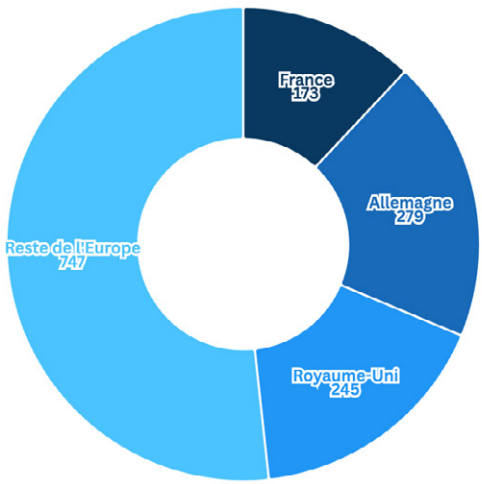
2025 - UNE ANNÉE PROLIFIQUE POUR LES GROUPES DE RANSOMWARE

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 60,16%, 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)



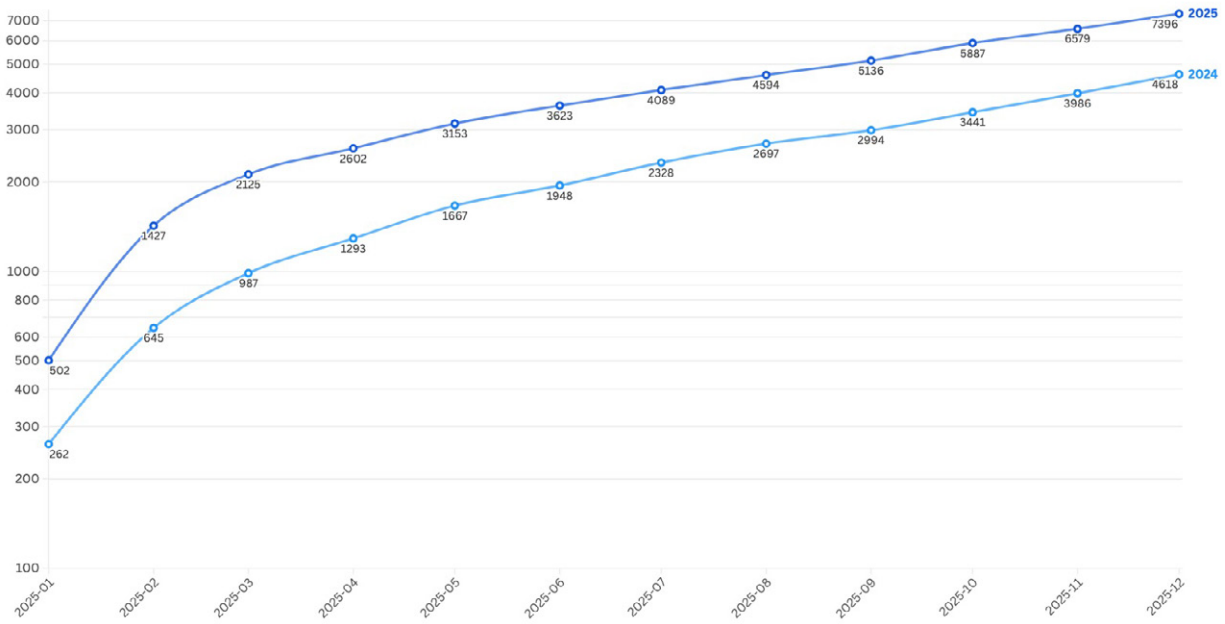
L'intensification des attaques par ransomware, s'illustrant par l'augmentation significative des attaques revendiquées sur les sites des groupes criminels, pourrait paradoxalement refléter la stagnation des paiements de rançon par leurs victimes : les cybercriminels multiplieraient les victimes ciblées 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 économiques 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].

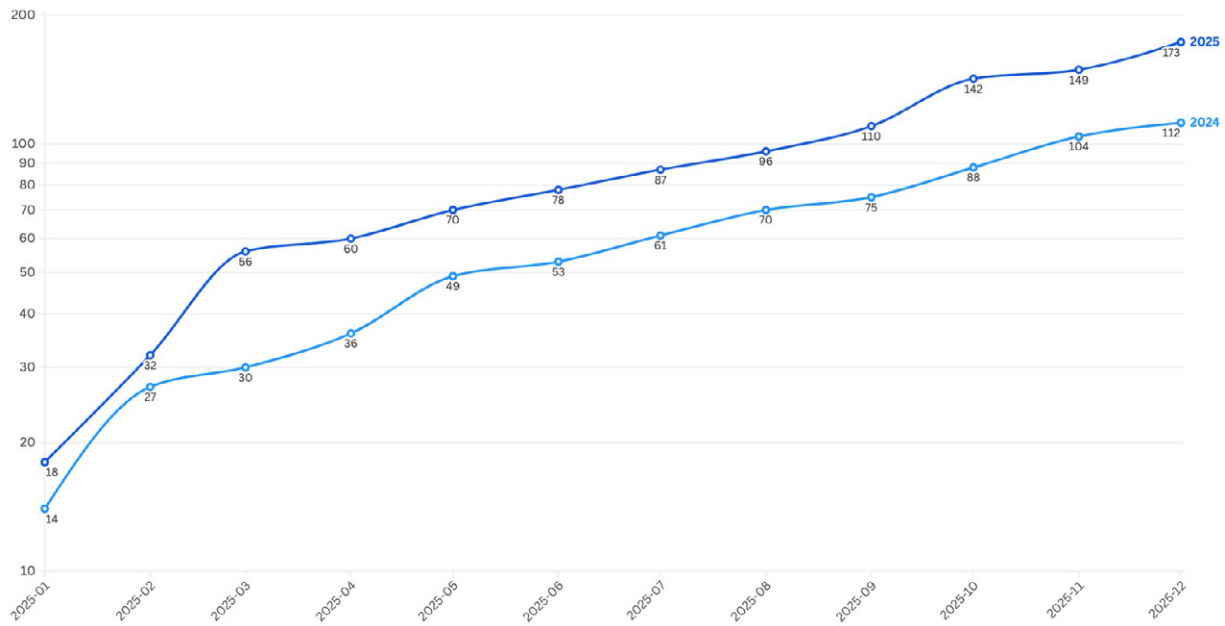
ÉVOLUTION CUMULATIVE DES ATTAQUES PAR RANSOMWARE REVENDIQUÉES À L'INTERNATIONAL EN 2025

(source : données internes du CERT-XMCO)



ÉVOLUTION CUMULATIVE DES ATTAQUES PAR RANSOMWARE REVENDIQUÉES EN FRANCE EN 2025

(source : données internes du CERT-XMCO)



LES ENTREPRISES FRANÇAISES SONT-ELLES DES CIBLES PRIVILÉGIÉES POUR LES ACTEURS CRIMINELS ?

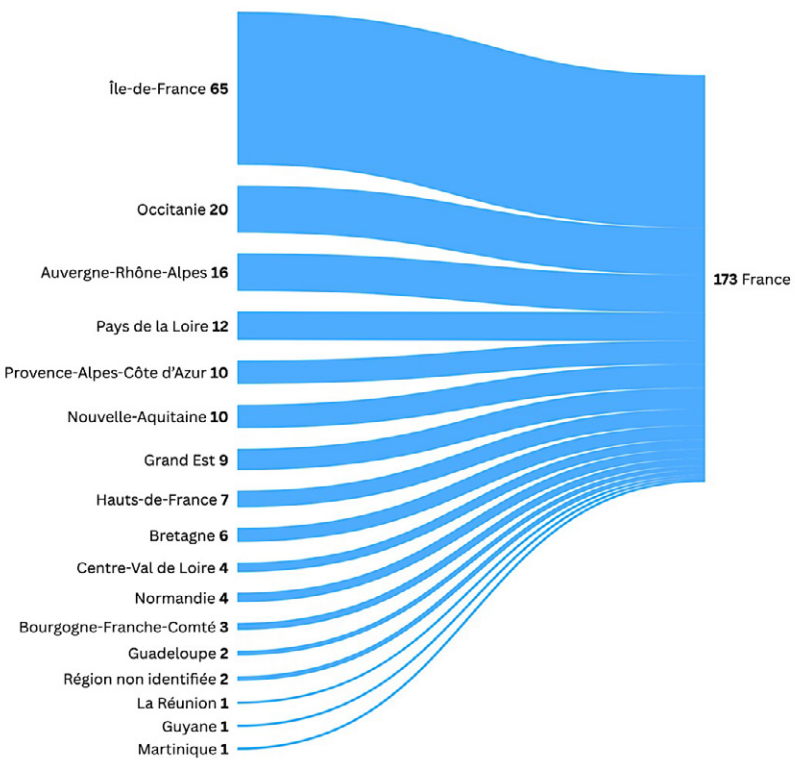
Tout au long de l'année 2025, les entreprises françaises ont été ciblées par des acteurs criminels aux motivations financières. Le CERT-XMCO a été en mesure d'identifier et qualifier 173 entités localisées en France et victimes de groupes criminels disposant d'un site vitrine de revendication. En amont 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.

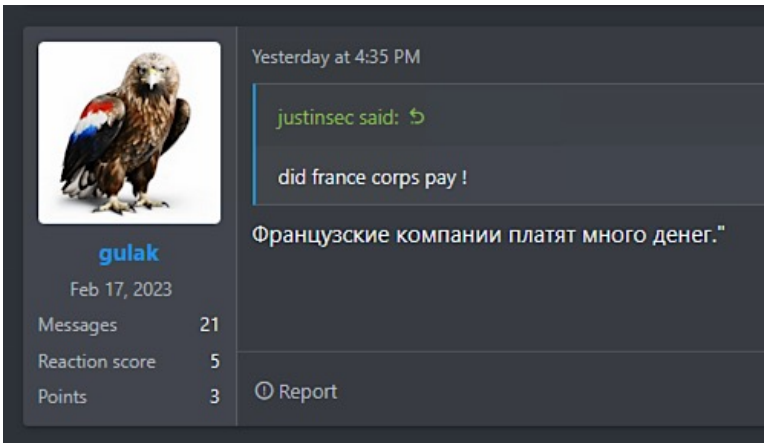
La répartition géographique des attaques par ransomware a tendance à se concentrer en Île-de-France, disposant d'une forte concentration économique et d'une densité d'entreprises. **Les régions françaises d'outre-mer ne sont pour autant pas épargnées par les extorsions cybercriminelles**, comme en témoigne 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)

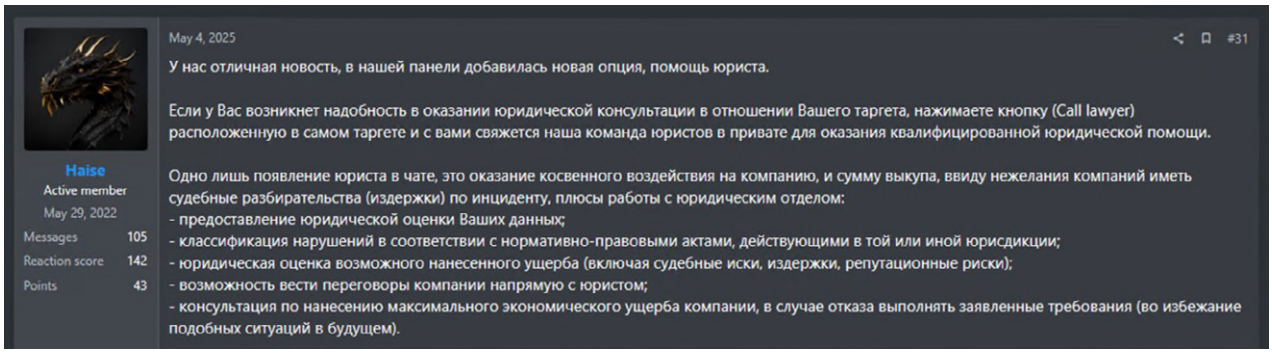


Les tentatives d'extorsion par ransomware signalées en France en 2025 semblent, pour la majorité d'entre elles, motivées par des objectifs financiers. En raison de son poids économique au sein de l'Europe, la France constitue une cible particulièrement attractive pour les cybercriminels, cherchant à 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.



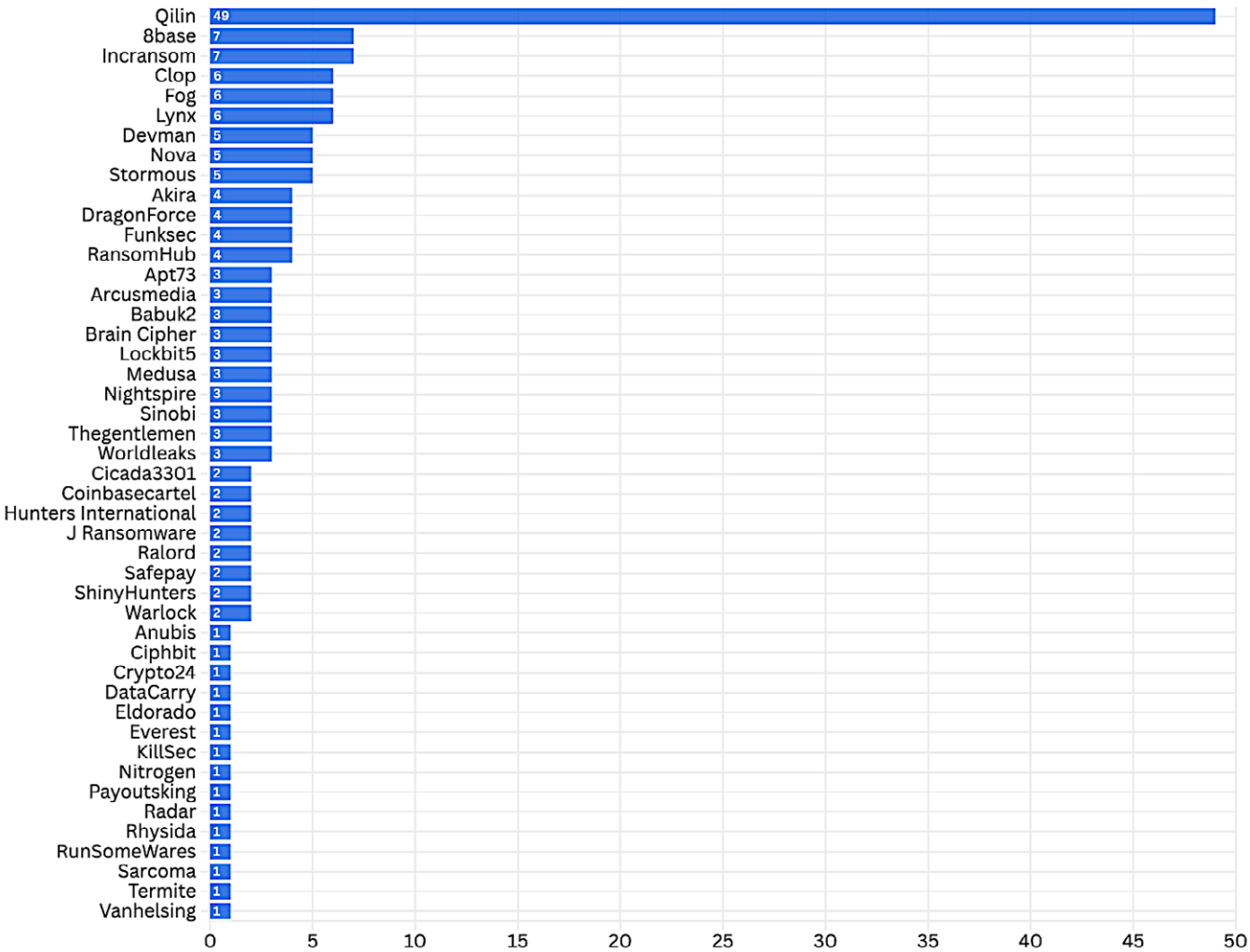
L'administrateur du groupe Qilin met à disposition un service d'assistance juridique auprès de ses affiliés (source : CERT-XMCO)

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 et qualification des données : 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 ».

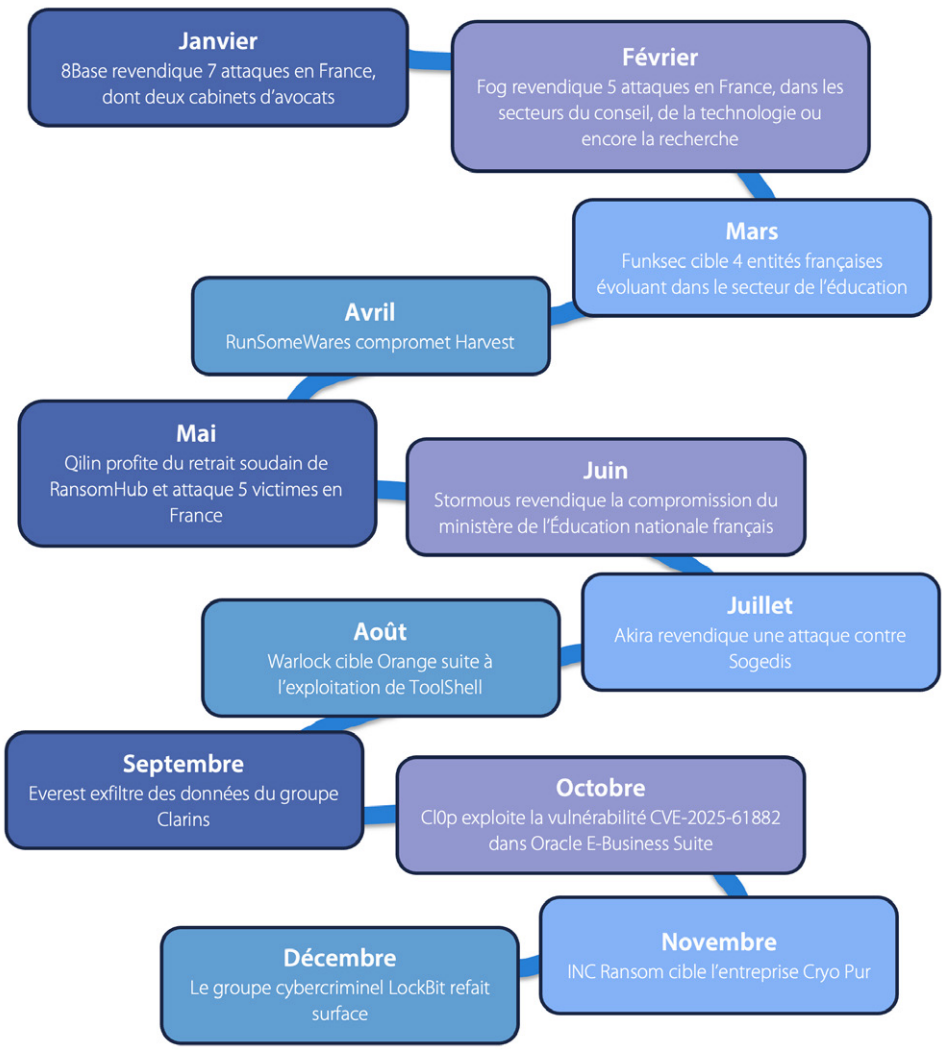
Certains collectifs criminels ont cherché à se distinguer en revendiquant des opérations aux résultats manifestement exagérés, à l'instar de Stormous et Funksec, des groupes historiquement connus pour

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.



1. LES CAPACITÉS DES GROUPES DE RANSOMWARE EN 2025

1.1 DES TACTIQUES, TECHNIQUES ET PROCÉDURES EN CONSTANTE AMÉLIORATION

1.1.1 LE DÉTOURNEMENT DES INFRASTRUCTURES CLOUD

En 2025, les groupes d'attaquants ont continuellement amélioré leurs modes opératoires, de l'accès initial jusqu'au chiffrement ou à l'exfiltration des données. Parmi les évolutions notables des tactiques, techniques et procédures (TTPs) déployées par les attaquants cette année, **le CERT-XMCO alerte sur le détournement progressif des infrastructures cloud par les opérateurs de ransomware**, ces derniers abusant de manière croissante des mauvaises configurations de services et ciblant des *API* exposées. En janvier, Halcyon signalait une cyberattaque au cours de laquelle des acteurs malveillants avaient détourné des clefs de type SSE-C pour chiffrer les données présentes au sein de *buckets Amazon S3* et exiger une rançon [12]. En utilisant un en-tête spécifiquement conçu, les attaquants étaient parvenus à chiffrer les données avec une clef AES-256 générée sur mesure et stockée localement par les cybercriminels. Il n'existe pas à ce jour de méthode publiquement documentée permettant de récupérer les données chiffrées.

En août, c'est au tour de Microsoft d'avertir sur des attaques contre des environnements cloud conduites par le mode opératoire Storm-0501, le *cluster* étant suspecté d'avoir collaboré avec plusieurs collectifs de ransomware, dont Embargo [13]. Lors de cette campagne, les cybercriminels auraient eu recours à la compromission de plusieurs domaines *Active Directory* et de locataires *Entra* en exploitant des failles de sécurité dans les déploiements *Microsoft Defender*. Les attaquants avaient ensuite désactivé les solutions de sécurité et volé des données sensibles à partir des comptes Azure Storage, puis tenté de détruire les instantanés de stockage, les points de restauration, les coffres-forts *Recovery Services* et les comptes de stockage.

1.1.2 LE CONTOURNEMENT DES SOLUTIONS EDR ET DES SCHÉMAS D'EXTORSION ÉVOLUTIFS

Le contournement des solutions de sécurité *EDR* a été un enjeu central pour les attaquants en 2025. À la suite de leur adoption massive par les organismes publics et privés, de nombreux cybercriminels ont commencé à considérer les *EDR* comme un obstacle majeur au cours de leurs attaques. Pour parvenir à les esquiver, plusieurs *clusters* ont développé des outils dédiés, tels que *EDRKillShifter* ou *AvNeutralizer*, tandis que d'autres se sont appuyés sur diverses techniques artisanales : la compromission de périphériques *IoT* observée lors d'une attaque d'Akira, ou encore l'exploitation d'une erreur dans le processus de mise à jour d'un *EDR* via une technique dite *Bring Your Own Installer* par Babuk [14] [15]. **En 2025, les groupes de ransomware ont démontré leur capacité de résilience en s'adaptant techniquement aux stratégies mises en place par les entreprises visant à limiter la portée de leurs attaques.** L'une des tendances majeures émergentes réside dans l'abandon progressif du chiffrement des données au profit de leur seule exfiltration. Ce mode opératoire se révèle moins lourd pour les attaquants, beaucoup plus discret et actionnable. Pour faire face aux politiques de non-paiement des rançons, certains groupes ont aussi recours à la mise en vente des données volées, conjointement aux tentatives d'extorsion auprès de leurs victimes.

L'année 2025 a également été marquée par la détection d'une quatrième souche de ransomware capable de contourner le processus de démarrage sécurisé UEFI. Référencée HybridPetya, cette souche est en mesure de compromettre les systèmes basés sur *UEFI* via l'exploitation d'une faille de sécurité référencée CVE-2024-7344. En contournant le processus de démarrage sécurisé, le ransomware démarre l'infection au niveau du firmware et peut compromettre un système même après un nettoyage complet de l'OS, complexifiant considérablement la réponse à incident [16]. Des souches antérieures, disposant de capacités d'infection similaires, avaient déjà servi des objectifs politiques via le sabotage d'infrastructures stratégiques.

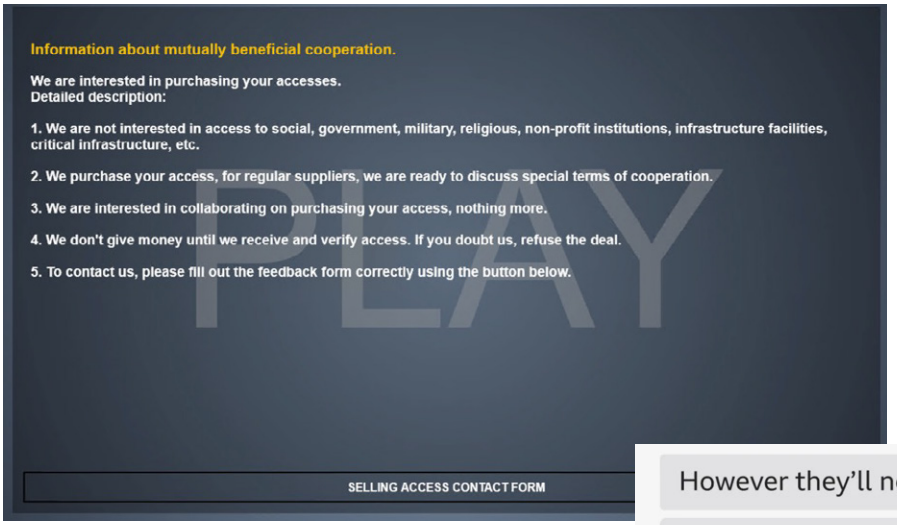
C'est notamment le cas de la souche NotPetya qui avait été distribuée à grande échelle en Ukraine en 2017, provoquant plus de 10 milliards de dollars de dommages [17].

1.1.3 L'EXPLOITATION DES FAIBLESSES HUMAINES PAR LES CYBERCRIMINELS

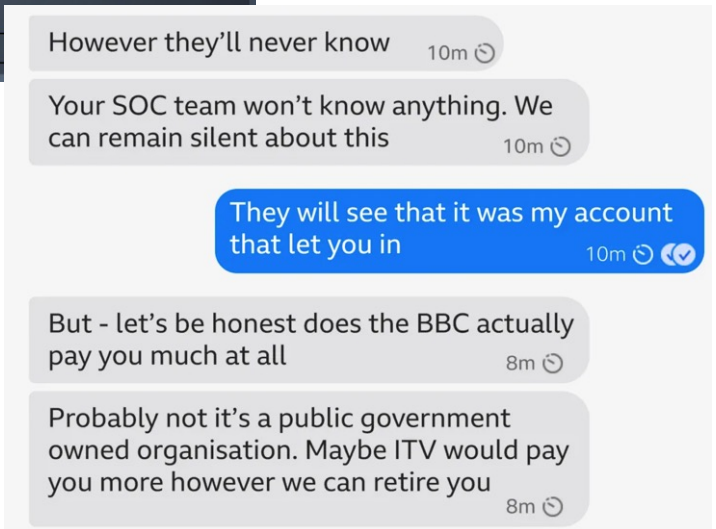
En 2025, les groupes de ransomware ont eu de plus en plus recours à des *insiders* (employés, prestataires, sous-traitants) au sein des entreprises ciblées. Contre une rétribution financière, ces derniers ont transmis aux attaquants un accès légitime aux systèmes informatiques de l'entreprise, permettant aux opérateurs de ransomware de contourner les mécanismes de sécurité et de réduire drastiquement le risque de détection et le délai de compromission.

Grâce à leur connaissance de l'environnement interne ciblé, les insiders facilitent les activités d'extorsion des cybercriminels, tout en limitant les coûts et efforts techniques déployés par les attaquants [18] [19]. À l'image de Sarcoma au mois de février, qui proposait une rémunération aux salariés prêts à partager des identifiants ou des informations réseau, plusieurs collectifs cybercriminels ont ainsi tenté de recruter des insiders en 2025.

Plus tard dans l'année, le collectif Scattered Lapsus$ Hunters s'est également illustré par le recrutement d'un employé au sein de la société de cybersécurité CrowdStrike, permettant aux attaquants d'accéder au réseau de l'entreprise en échange de 25 000 dollars [20]. En septembre, la BBC avait déjà alerté sur ces risques dans un article détaillant la tentative de corruption de l'un de ses employés par le groupe cybercriminel Medusa [21].



Page de contact dédiée aux insiders sur le site du groupe de ransomware Play (source : CERT-XMCO)



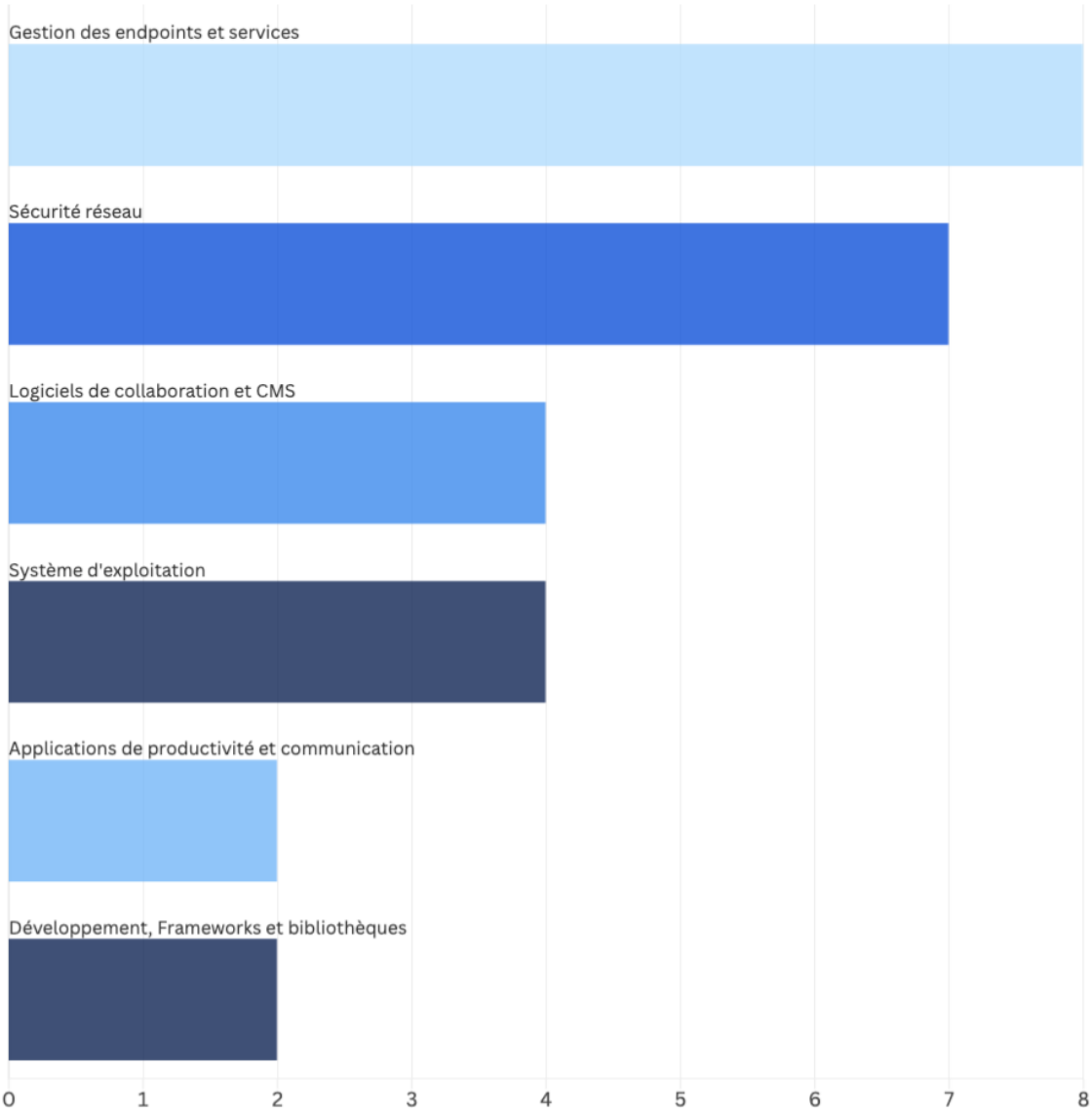
Tentative de recrutement d'un insider au sein de la BBC par le groupe Medusa (source : BBC)

1.2 ÉTAT DES LIEUX DES VULNÉRABILITÉS EXPLOITÉES PAR LES OPÉRATEURS DE RANSOMWARE

En 2025, les groupes de ransomware ont ponctuellement eu recours à l'identification et l'exploitation de failles de sécurité afin de faciliter la conduite de leurs opérations d'extorsion. Ces vulnérabilités leur ont permis d'accéder à des informations sensibles, de manipuler des données, d'élever leurs privilèges, de contourner des solutions de sécurité, voire de prendre le contrôle des instances ciblées.

VUE D'ENSEMBLE DES TECHNOLOGIES CIBLÉES PAR LES GROUPES DE RANSOMWARE

(source et qualification des données : CERT-XMCO)



1.2.1 ACCÈS INITIAL : DES VULNÉRABILITÉS AFFECTANT DES TECHNOLOGIES EXPOSÉES SUR INTERNET

Les services VPN et les technologies de type Managed File Transfer (MFT) ou Content Management System (CMS) ont été des cibles privilégiées pour les opérateurs de ransomware en 2025. Les vulnérabilités affectant Fortinet FortiOS / FortiProxy, SonicWall SMA / SonicOS montrent les risques liés aux équipements de sécurité et d'accès distant exposés sur Internet, souvent ciblés pour obtenir un accès initial ou persistant aux réseaux d'entreprise par les opérateurs de ransomware. À titre d'illustration, le CERT-XMCO documentait en mars 2025 l'exploitation de failles de sécurité (CVE-2024-55591 et CVE-2025-24472) au sein des instances Fortinet par une nouvelle souche de ransomware nommée SuperBlack [22].

1.2.2 PERSISTANCE ET ÉVASION : DES VULNÉRABILITÉS AFFECTANT DES PROCESSUS ET OUTILS LÉGITIMES

Une fois qu'ils ont pris pied au sein du réseau ciblé, les attaquants cherchent à prendre le contrôle total du système tout en limitant les risques d'être détectés. Ce mode opératoire explique donc le ciblage répété des outils de gestion d'endpoints, le détournement de processus natifs au système d'exploitation ou bien encore le détournement d'infrastructure virtuelle. Les groupes de ransomware ont exploité des vulnérabilités affectant des composants légitimes comme Windows Common Log File System, le Linux kernel ou des pilotes vulnérables afin d'obtenir des privilèges élevés et contourner les mécanismes de sécurité. En février 2025, Microsoft avait identifié cinq failles de sécurité affectant le pilote Paragon Partition Manager BioNTdrv.sys, dont l'une d'entre elles, référencée CVE-2025-0289, avait été exploitée comme 0-day par des groupes de ransomware non spécifiés [23].

1.2.3 MONÉTISATION DE L'ATTAQUE : DES VULNÉRABILITÉS AU SEIN DE SOLUTIONS AUX DONNÉES SENSIBLES

En 2025, les groupes de ransomware ont exploité certaines technologies connues pour héberger des informations sensibles. Cette démarche est conduite afin de maximiser les possibilités d'extorsion sur les victimes. Il n'est dès lors pas surprenant que les attaquants ciblent les services hébergeant des données financières, RH, juridiques, ou bien encore des documents susceptibles d'intégrer des propriétés intellectuelles. Les solutions manipulant des données sensibles, comme Oracle E-Business Suite, Veritas Backup Exec et Gladinet CentreStack, constituent des cibles privilégiées pour les acteurs malveillants. Leurs compromissions ont facilité des tentatives d'extorsion menées par divers opérateurs de ransomware, dont Cl0p et ShinyHunters [24] [25].

Phase de l'attaque	Technologies privilégiées par les attaquants	Exemples de technologies détournées
Accès initial	VPN MFT CMS	Fortinet FortiOS / FortiProxy SonicWall SMA / SonicOS Craft CMS
Persistance et évasion	Système d'exploitation Logiciels de sécurité	Windows CLFS Linux kernel Howyar UEFI Application Reloader Baidu Antivirus Velociraptor
Monétisation de l'attaque	Applications de productivité, de communication	Oracle E-Business Suite Veritas Backup Exec Gladinet CentreStack

VULNÉRABILITÉS EXPLOITÉES EN 2025 PAR DES OPÉRATEURS DE RANSOMWARE

(source et qualification des données : CERT-XMCO)

Références CVE	Technologies ciblées	Dommages associés	Groupes de ransomware	Exploitatées comme 0-day	Références
CVE-2023-22527	Atlassian Confluence	Prise de contrôle du système	LockBit Black ELPACO-team	NON	DFIR Report [24] DFIR Report [25]
CVE-2024-57726 CVE-2024-57727 CVE-2024-57728	SimpleHelp RMM	Prise de contrôle du système Élévation de privilèges Divulgation d'informations	Akira DragonForce Play	NON	Field Effect [26] Sophos [27] et la CISA [28]
CVE-2025-0289	Paragon Partition Manager BioNTdrv.sys	Contournement de sécurité et prise de contrôle	Non spécifié	NON	Microsoft [29]
CVE-2025-24472 CVE-2024-55591	Fortinet FortiOS/FortiProxy	Contournement de sécurité	SuperBlack Qilin	**OUI** [28] [29]	ForeScout [30] Prodaft [31]
CVE-2025-29824	Windows CLFS	Élévation de privilèges	Storm-2460 (cluster proche des TTPs de RansomExx) et Play	**OUI** [32]	Microsoft [32] et Symantec [33]
CVE-2025-31324	SAP NETWEAVER Visual Composer	Prise de contrôle du système	BianLian et RansomEXX	**OUI** [35]	Reliaquest [34]
CVE-2025-32432	Craft CMS	Prise de contrôle du système	Minus	NON	Sekoia [35]
CVE-2021-27877 CVE-2021-27878	Veritas Backup Exec	Prise de contrôle du système	Non spécifié	NON	Google [36]
CVE-2025-49706 CVE-2025-49704 CVE-2025-53770 CVE-2025-53771	Microsoft SharePoint	Prise de contrôle du système Contournement de sécurité	Warlock, AK47 ransomware 4L4MD4R Ransomware	NON	Microsoft [37] CheckPoint [38] Unit42 [39]
CVE-2024-40766	SonicWall SMA SonicOS SSLVPN	Contournement de sécurité Déni de service	UNC6148 (cluster proche de World Leaks) Akira	NON	Google [40] SonicWall [41]
CVE-2025-8088	WinRAR	Prise de contrôle du système	RomCom	NON	ESET [42]
CVE-2024-7344	Howyar UEFI Application Reloader	Contournement de sécurité	HybridPetya	NON	ESET [43]
CVE-2024-51324	Baidu Antivirus	Contournement de sécurité	Warlock et DeadLock	NON	Sophos [44] Cisco Talos [45]
CVE-2025-61882 CVE-2025-61884	Oracle E-Business Suite	Prise de contrôle du système et divulgation d'information	ShinyHunters et Cl0p	NON	Oracle [46]
CVE-2025-10035	GoAnywhere Managed File Transfer	Prise de contrôle du système	Medusa	NON	Microsoft [47]
CVE-2025-6264	Velociraptor	Prise de contrôle du système Élévation de privilèges	Storm-2603 (aka Warlock)	NON	Cisco Talos [48]
CVE-2024-1086	Linux kernel	Élévation de privilèges	Ransomware non spécifié par la CISA	NON	SecurityAffairs [49]
CVE-2025-26633	Microsoft Management Console	Prise de contrôle du système Contournement de sécurité	EncryptHub	NON	Zscaler [50]
CVE-2025-55182	React Server Components	Prise de contrôle du système	Weaxor	NON	S-RM [51]
CVE Non spécifiée	Gladinet CentreStack	Dommage non spécifié	Cl0p	NON	Curated Intelligence [52]
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus	Prise de contrôle du système Contournement de sécurité	Non spécifié	**OUI** [55]	Google [36]
CVE-2019-6693	Fortinet FortiOS	Divulgation d'informations	Non spécifié	NON	Google [36]
CVE-2023-4966	Citrix NetScaler	Divulgation d'informations	Non spécifié	**OUI** [55]	Google [36]
CVE-2024-3400	Palo Alto PAN-OS GlobalProtect	Prise de contrôle du système	Non spécifié	**OUI** [56]	Google [36]
CVE-2025-31161	CrushFTP	Contournement de sécurité	Non spécifié	**OUI** [57]	Google [36]

1.3 UN ÉCOSYSTÈME CYBERCRIMINEL COMPÉTITIF S'ARTICULANT AUTOUR DE PROGRAMMES DE RAAS

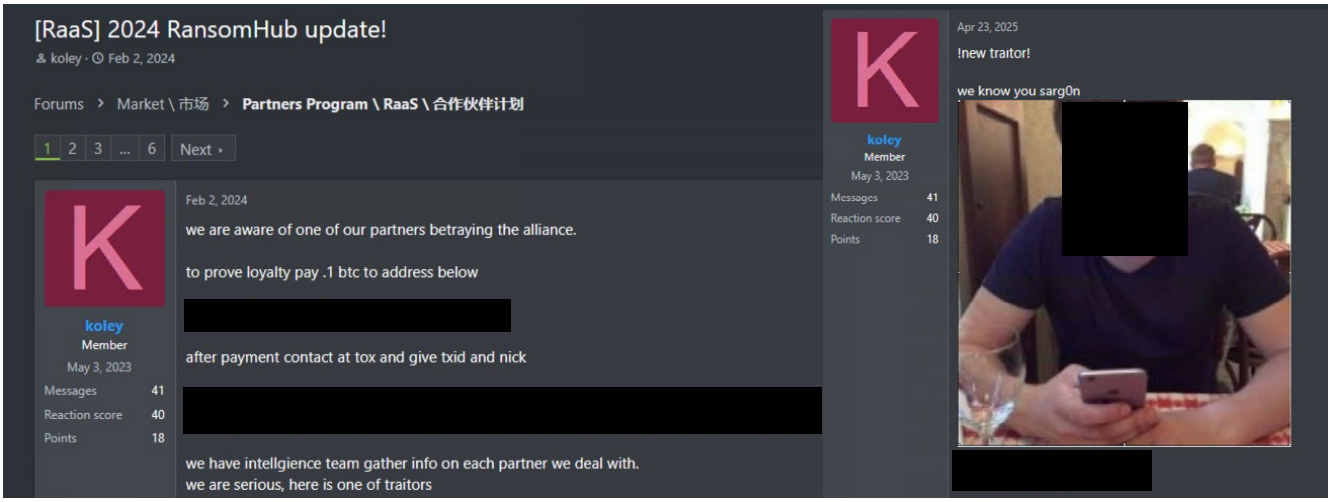
En 2025, l'écosystème des ransomware s'est caractérisé par des luttes internes entre collectifs criminels, conjuguées à des alliances opportunistes formées en réponse à l'intensification des actions des forces de l'ordre. **Des groupes criminels rivaux de type RaaS se sont ainsi confrontés pour prendre le contrôle des parts de marché, quand d'autres ont préféré s'allier afin de préserver leur réputation de stabilité auprès de leurs affiliés et recrues potentielles.**

1.3.1 LES LUTTES INTERNES À L'ÉCOSYSTÈME DES RANSOMWARE

L'écosystème cybercriminel est régulièrement traversé par des luttes internes : concurrence entre programmes de RaaS, exit scams entre développeurs et rivalités sur le pourcentage de rétribution des rançons. Les démantèlements ou opérations d'infiltrations policières soupçonnées [53] poussent certains affiliés à quitter un groupe pour en rejoindre un autre, ce qui **alimente la rivalité entre certains programmes de** *Ransomware-as-a-Service***, au sein desquels la réputation de performance devient centrale et provoque des dérives qui mettent en danger la sécurité de leurs membres** : fausses revendications d'attaques, leak de conversations internes du groupe, doxing de membres concurrents.

La disparition de RansomHub constitue sans doute l'épisode le plus significatif de l'année 2025. Avec plus de 840 victimes revendiquées entre les mois de février 2024 et de mars 2025, ce collectif cybercriminel qui proposait un programme de *Ransomware-as-a-Service* attractif pour ses affiliés était devenu le leader de l'écosystème cybercriminel, avant de disparaitre subitement en avril dernier.

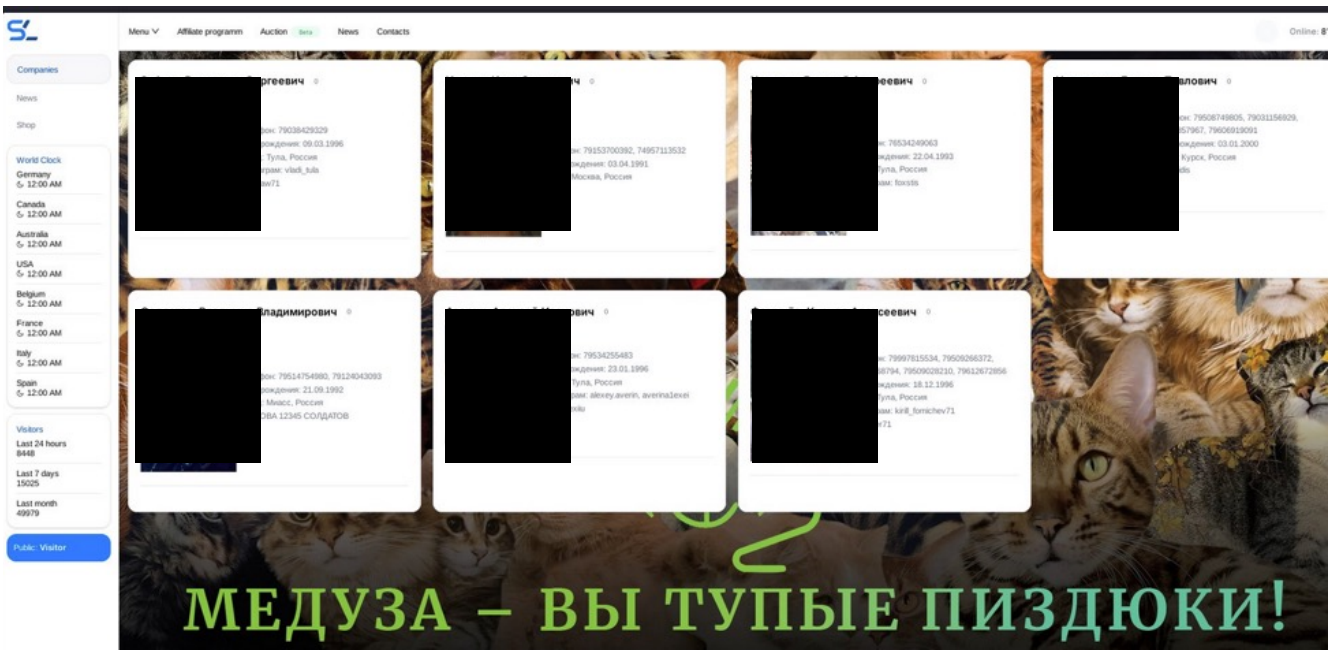
En l'espace de quelques mois, RansomHub avait réussi à s'illustrer par le développement d'EDRKillShifter, un outil destiné à désactiver les systèmes *EDR* en exploitant les pilotes vulnérables, et d'une *backdoor* nommée Betruger permettant aux affiliés du groupe d'élever leurs privilèges sur les machines compromises et de disposer de capacités avancées de collecte et d'exfiltration de données [54] [55]. L'essor de sa notoriété, conjugué à un afflux accéléré de nouveaux affiliés, a vraisemblablement accru la visibilité et la vulnérabilité du groupe. Les administrateurs de RansomHub ont, de leur propre aveu, affirmé avoir subi une infiltration par des chercheurs en cybersécurité en juin 2024, vraisemblablement à l'origine de la fuite de certains de ses affiliés vers d'autres programmes de ransomware [56].



L'administrateur de RansomHub attaque une partie de ses anciens affiliés à la suite de tensions internes (source : CERT-XMCO)

Les tentatives de déstabilisation subies par Medusa en 2025, initiées par d'autres groupes de ransomware, illustrent également combien la sécurité opérationnelle demeure un enjeu pour les affiliés de groupes cybercriminels. Dans ces environnements clandestins structurés autour de l'anonymat, d'une confiance limitée et de logiques de délégation, les vulnérabilités organisationnelles fragilisent les acteurs, perturbent les campagnes d'extorsion et sapent la réputation du collectif.
De tels épisodes soulignent que les menaces pesant à l'encontre de ces structures criminelles ne proviennent pas uniquement des autorités, mais également des groupes rivaux, prompts à exploiter ces défaillances pour affaiblir leurs adversaires, notamment via l'infiltration et la révélation publique de leur organisation interne.

Divulgation des conversations internes de Medusa par RansomedVC (source : CERT-XMCO)



Doxing opéré par Silent Ransomware contre les membres de Medusa (source : CERT-XMCO)

Les perturbations affectant RansomHub et Medusa ne constituent pas un épiphénomène. À l'issue de l'Opération Cronos, LockBit avait ainsi cédé son statut de leader du marché à RansomHub, qui l'a lui-même transmis à Qilin et DragonForce en 2025. Suivant cette logique naturelle, ces groupes aujourd'hui hégémoniques feront

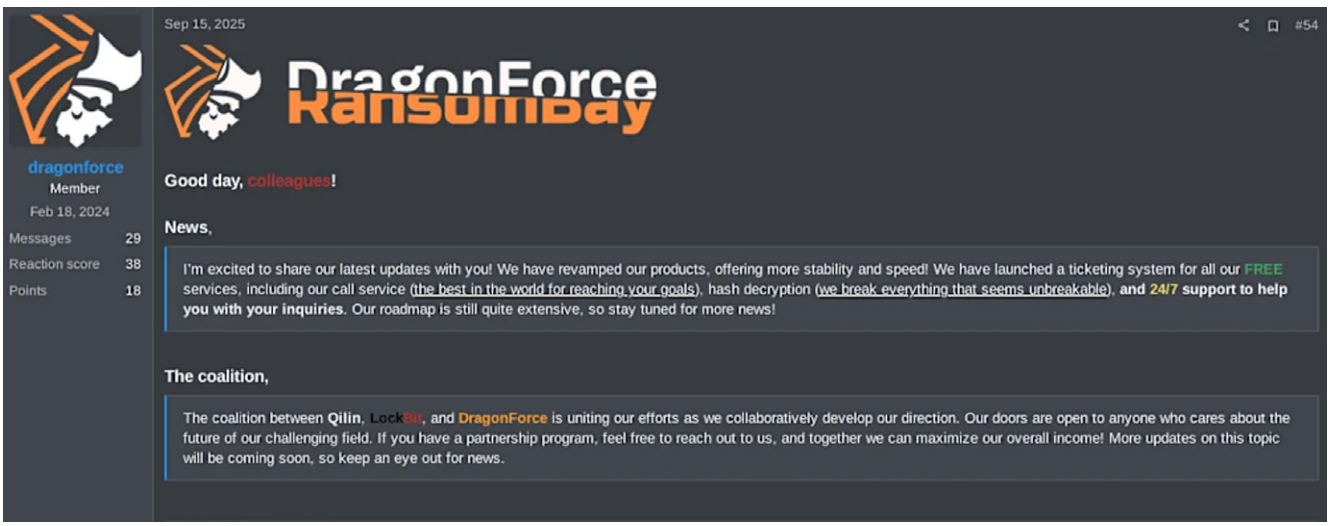
probablement à l'avenir l'objet de perturbations et seront remplacés par d'autres structures cybercriminelles.

Afin d'anticiper cette éventualité, **certains groupes de ransomware ont choisi de s'engager dans une forme de collaboration, parfois de façade, cherchant à optimiser leurs bénéfices par la mise en commun de certaines ressources et l'instauration progressive d'un climat de confiance**, sans pour autant exclure des intérêts parfois divergents.

1.3.2 DE LA ***COOP*** AU ***REBRANDING*** – OU COMMENT FAIRE FACE AUX ACTIONS DES FORCES DE L'ORDRE

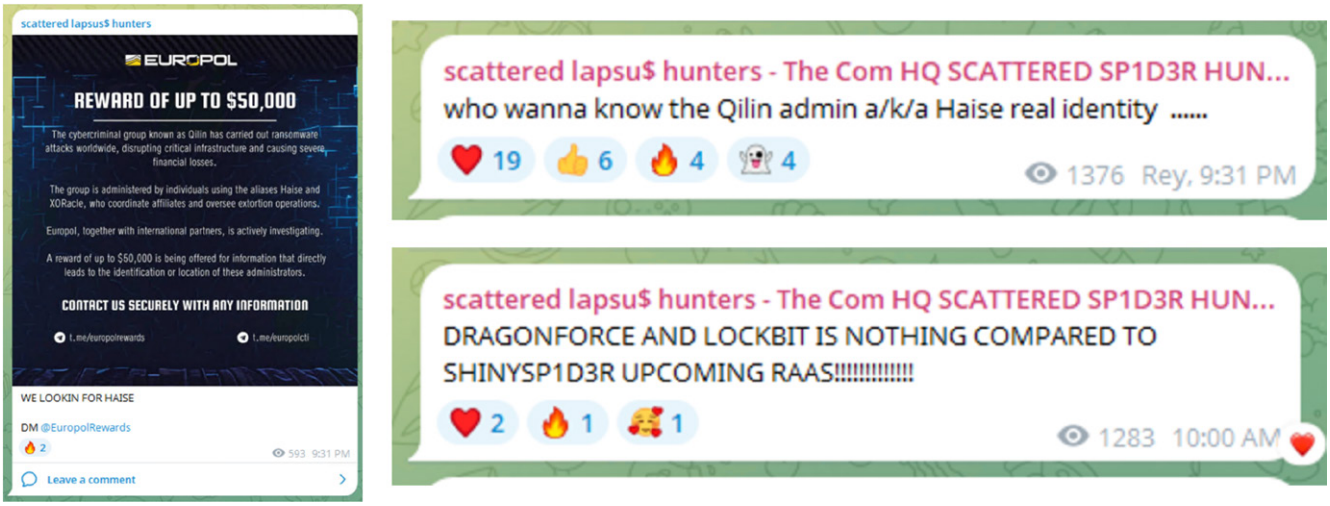
Afin de se prémunir contre les actions des forces de l'ordre et les tentatives de déstabilisation menées par des groupes concurrents, les opérateurs de ransomware ont ainsi élaboré diverses stratégies visant à renforcer leur résilience opérationnelle et à préserver la continuité de leurs activités illicites. **Certains groupes ont ainsi opté pour une stratégie de** *rebranding* **de leur programme de** *RaaS***, tandis que d'autres ont choisi de s'allier temporairement avec des groupes adverses.**

C'est dans cette logique que DragonForce, Qilin et LockBit ont annoncé en septembre dernier créer une nouvelle alliance destinée à dominer le paysage des programmes de *Ransomware-as-a-Service* [57] [58]. Cette annonce a été suivie de la publication d'une centaine de victimes sur le site vitrine de LockBit 5.0 durant le seul mois de décembre 2025. Bien que cette proactivité puisse être surestimée, elle traduit néanmoins la volonté du groupe de maintenir ses activités, nourrie par un sentiment de revanche à la suite des nombreuses opérations policières qui ont freiné son expansion au cours des deux dernières années.



Nouvelle alliance des collectifs DragonForce, Qilin et LockBit sur un forum en septembre 2025 (source : CERT-XMCO)

En fin d'année 2025, le CERT-XMCO a également noté l'évolution de la structure d'affiliation opérée par Lapsus$, Scattered Spider et ShinyHunters. Opérant jusqu'alors en cercle restreint, ce collectif cybercriminel, qui s'était illustré par la compromission médiatisée d'instances SalesForces au mois d'août, a cherché à développer son programme de *Ransomware-as-a-Service* en recrutant ses affiliés via Telegram et différentes marketplaces anglophones, tout en provoquant les collectifs cybercriminels concurrents [59].



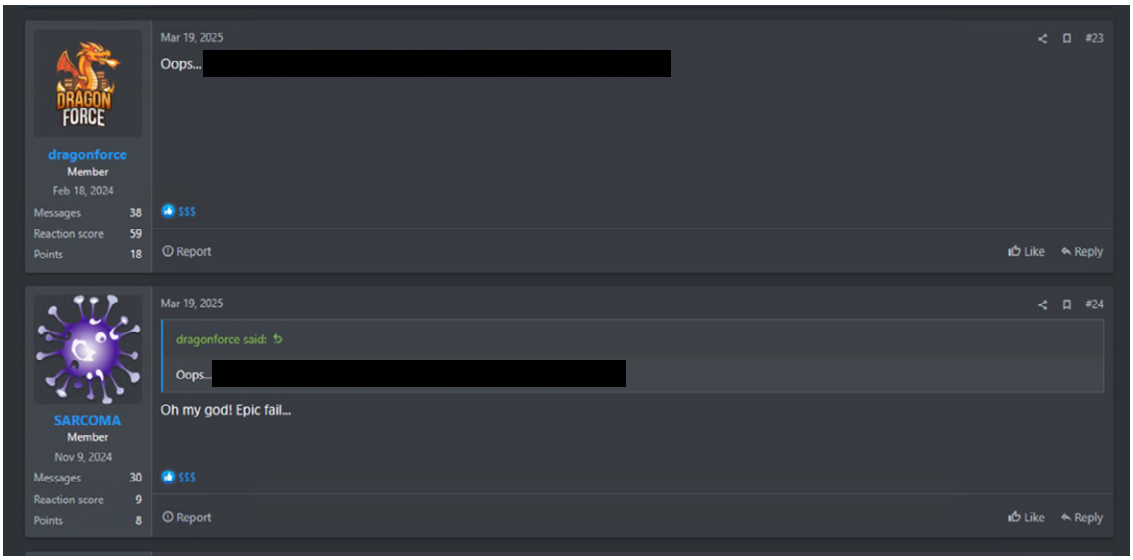
Scattered Lapsus$ Hunters usurpe une communication d' Europol pour provoquer Qilin (source : CERT-XMCO)

Les stratégies de *rebranding* adoptées par les groupes de ransomware sont intrinsèquement liées à la gestion de leur réputation au sein de l'écosystème cybercriminel. Une attaque particulièrement médiatisée, la divulgation de données internes, tels que le leak d'un source code ou l'exposition d'un affilié du groupe constituent autant d'événements susceptibles de ternir l'image d'un collectif criminel auprès de ses effectifs, de ses partenaires et de ses victimes. **Le** *rebranding* **d'un groupe permet alors d'absoudre la réputation compromise du groupe, en se présentant sous une nouvelle identité plus attractive, car anonyme et gage de sécurité opérationnelle.**

En avril dernier, les chercheurs de Group-IB ont signalé le *rebranding* du collectif criminel Hunters International sous le nom de World Leaks [60]. Cette démarche s'expliquerait a posteriori par des actions menées par les forces de l'ordre à l'encontre des cybercriminels, ainsi que par une volonté de simplifier leur mode opératoire, ce dernier s'appuyant désormais sur des mécaniques d'exfiltrations de données uniquement. Actifs depuis le mois d'octobre 2023, certains administrateurs du groupe étaient déjà soupçonnés d'être issus de l'ancien collectif prolifique Hive, contrairement aux déclarations du groupe lui-même.

À titre d'exemple, l'administrateur de Mamona RIP et BlackLock (aka Eldorado), connu sous le pseudonyme «$$$», s'est illustré ces dernières années par plusieurs tentatives de rebranding successives, la plus récente consistant en la création de la marque GLOBAL GROUP, présentée comme l'itération la plus mature de son programme RaaS [61] [62].

Différentes erreurs de sécurité opérationnelle ont permis de confirmer que l'opérateur contrôlait les trois souches de ransomware susmentionnées et ont desservi le groupe au profit de collectifs concurrents. En dépit des fonctionnalités successivement proposées au sein GLOBAL GROUP, Black Lock et Mamona, l'opérateur a durablement terni sa réputation auprès de ses affiliés.



DragonForce opère un défacement du site vitrine de Mamona ransomware (source : CERT-XMCO)

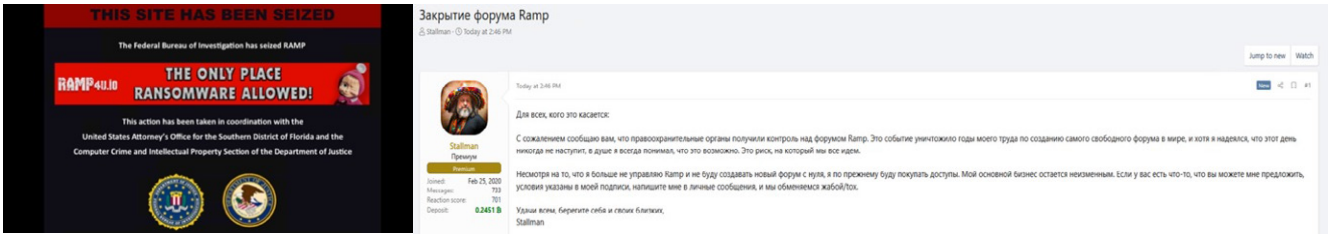
1.4 RÉFLEXIONS SUR L'ÉVOLUTION DES MODES OPÉRATOIRES FACE AUX FORCES DE L'ORDRE

En 2026, **le CERT-XMCO s'attend à une continuité des modes opératoires employés par les groupes de ransomware**, dans une logique de résilience vis-à-vis de la pression exercée par les forces de l'ordre au cours de l'année passée et ayant résulté sur la saisie de plusieurs services de type « Bulletproof hosting » (*BPH*) stratégiques pour opérer leurs attaques, ainsi qu'à l'arrestation de multiples opérateurs de programmes *RaaS*. Afin d'assurer une relative sécurité opérationnelle, ces acteurs pourraient tendre vers une structuration en cercle encore plus restreint, dans le but de réduire les risques d'infiltration et de préserver la confidentialité de leurs opérations. En fin d'année 2025, certains groupes effectuaient déjà une sélection drastique de leurs affiliés, ces derniers nécessitant désormais un garant, des ressources financières établies et de faire montre d'une proactivité effective lors du début de la collaboration.

1.4.1 LE RÔLE JOUÉ PAR LES MESSAGERIES CHIFFRÉES

Les plateformes du *Deep/Dark web*, couplées aux diverses messageries disposant d'un mécanisme de chiffrement ou d'une garantie de confidentialité des données, telles que Telegram, Signal, TOX ou encore Session, continueront probablement d'être des outils privilégiés de communication pour les administrateurs de ransomware avec leurs affiliés et leurs potentielles cibles. Ainsi, il est probable que **l'organisation de ces collectifs criminels évoluant au sein de cercles restreints continuera de représenter un enjeu majeur afin de surveiller leurs activités**, dans un contexte de diffusion d'informations trompeuses destinées à leurrer les forces de l'ordre et les chercheurs en cybersécurité [63] 1.3.1.

Saisie des sites criminels Cracked et Nulled en janvier 2025 [64] / Saisie du site criminel XSS en juillet 2025 [65]



Saisie du site criminel RAMP en janvier 2026 et communiqué de l'administrateur sur XSS [66]

Durant l'année 2026, **les cybercriminels continueront de s'appuyer régulièrement sur des insiders**, chargés de faciliter l'accès initial et l'exfiltration de données d'intérêt au sein des organismes compromis [67] [68]. Contrairement à la recherche de vulnérabilités techniques de type *0-day*, nécessitant des ressources techniques et financières importantes, **la corruption d'employés ou de sous-traitants s'avère beaucoup moins coûteuse et moins complexe à mettre en œuvre que la découverte et la militarisation de failles techniques**. Dès lors, l'obtention d'un accès légitime par les attaquants auprès d'un employé ou d'un prestataire, contacté directement par l'intermédiaire de messageries mobiles chiffrées, facilitera le contournement d'une grande partie des défenses techniques aujourd'hui mises en place dans les organisations 1.1.3.

2. UNE VICTIMOLOGIE TOUJOURS MOTIVÉE PAR LE GAIN FINANCIER ?

En 2025, les campagnes d'attaques par ransomware ont évolué bien au-delà des cadres traditionnels du cybercrime motivé par l'appât du gain. Si la logique financière demeure le moteur dominant de la plupart des opérateurs et affiliés de ransomware, les investigations menées en 2025 par divers acteurs de la cybersécurité ont mis en évidence une tendance plus nuancée : certains modes opératoires exploitant des souches de ransomware semblent poursuivre des objectifs pluriels, à la croisée du crime organisé, de l'espionnage, de l'action d'influence, voire dans certains cas spécifiques : du sabotage.

Cette évolution marque une transformation profonde dans l'analyse de la victimologie des groupes de ransomware, révélant que certaines opérations obéissent à des considérations davantage politiques et idéologiques, et non plus seulement économiques. Les campagnes menées l'an dernier et documentées par le service Yuno du CERT-XMCO illustrent cette diversification des motivations.

- Le cluster *RomCom* s'est distingué par des opérations de vols de données contre diverses entités stratégiques évoluant dans des pays européens et nord-américains, laissant supposer un intérêt pour la collecte de renseignements et la perturbation de structures perçues comme hostiles à la Russie.

- De même, le collectif de ransomware *Warlock*, ayant opéré des attaques concomitantes à des groupes étatiques chinois, s'est illustré en 2025 par des opérations mêlant vol de données, campagnes d'espionnage et publication sélective de documents, brouillant la frontière entre le cybercrime et les opérations d'influence chinoises.

- Quant à *Handala*, un proxy iranien déjà connu pour ses agissements au Moyen-Orient, ses attaques récentes en 2025 ont directement visé des infrastructures critiques en Israël et aux États-Unis, avec des impacts politiques qui dépassent largement la simple recherche du profit.

L'année passée, la Russie, la Chine, la Corée du Nord et l'Iran ont été régulièrement mentionnés par les chercheurs en Cyber Threat Intelligence (CTI) comme des environnements où l'activité cybercriminelle bénéficie d'une relative tolérance, évoluant dans une zone grise, voire parfois sous la supervision tacite d'agences étatiques, leur permettant dans certains cas de disposer d'outils offensifs sans engagement officiel – un mécanisme souvent qualifié de *plausible deniability*.

Les groupes de ransomware actifs dans ces environnements sont ainsi soumis à des logiques de stratégies étatiques dans le cadre de leurs opérations, qu'il s'agisse du choix des cibles, du calendrier des opérations, de la publication sélective de données dérobées ou des priorités fixées au regard des enjeux politiques d'intérêt pour l'État parrain.

Il convient toutefois de souligner que ces corrélations ne suffisent pas à démontrer un contrôle direct exercé par les instances étatiques, sans néanmoins nier les connexions existantes entre elles et les groupes concernés. Les analyses publiées en 2025 mettent plutôt en évidence une récurrence de convergences d'intérêt, une juxtaposition temporelle des attaques avec des contextes géopolitiques, ainsi que des modes opératoires suggérant des motivations plurielles, parfois trompeuses.

Les liens présumés entre les opérateurs de ransomware et les structures gouvernementales russes, chinoises, iraniennes et nord-coréennes restent dès lors difficiles à établir formellement, en raison du cloisonnement et de la complexité technique de l'écosystème cybercriminel étudié. Néanmoins, **la répétition de ces signaux dans les rapports publics de sociétés de cybersécurité plaide pour une lecture prudente, mais critique : le ransomware ne doit plus être envisagé exclusivement comme un phénomène économique**, mais aussi comme un instrument au service de stratégies d'influence.

2.1 DES CLUSTERS CRIMINELS QUI PARTICIPENT À L'EFFORT DE GUERRE RUSSE EN UKRAINE

La notion de *krysha* (en russe : *крыша*), signifiant littéralement « toit » en langue russe, est un concept historique clé pour appréhender les rapports de force entre l'écosystème cybercriminel et les autorités russes [69]. Cette *krysha* désigne une protection informelle d'une structure criminelle par un représentant de l'État russe en échange d'une rétribution, généralement financière [70].

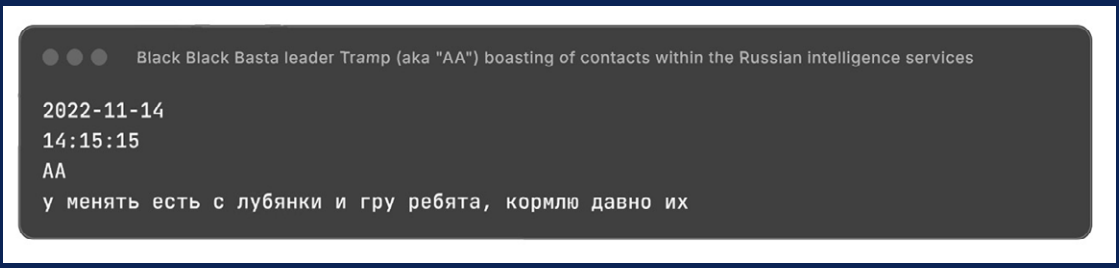
Ce système offre aux cybercriminels disposant de relations au sein des structures de force russes une protection contre d'éventuels poursuites judiciaires. La désagrégation de l'Union soviétique en 1991 a favorisé l'émergence d'un environnement propice à la criminalité organisée, où certains acteurs du monde informatique se sont orientés vers le piratage et le carding, consolidant le lien entre cybercriminalité et intérêts russes [71].

La perméabilité entre les activités de cybercriminalité et les opérations d'espionnage soutenues par le Kremlin s'est accentuée à la suite du lancement de l'invasion militaire russe en Ukraine en février 2022 [72] [73]. En contrôlant des structures cybercriminelles, déjà partiellement détournées depuis 2014, les services de renseignement russes ont pu exploiter leurs ressources techniques et humaines afin de faciliter les campagnes d'espionnage et complexifier l'attribution des attaques russes poursuivant des objectifs de sabotage ou de désinformation [74] [75] [76].

De leur côté, les groupes de ransomware opérant depuis la *Communauté des États Indépendants* ont été contraints de collaborer avec les autorités russes pour poursuivre leurs activités criminelles en parallèle d'une participation à l'effort de guerre sur le front ukrainien, leur évitant par la même occasion les risques d'une extradition vers les pays ciblés par leurs attaques. Les cas d'Evil Corp et de Conti témoignent des relations troubles entretenues avec les autorités russes [77].

BLACK BASTA LEAK

Parmi les groupes de ransomware actifs cette année, les opérateurs de BlackBasta ont été publiquement épinglés en février 2025 pour avoir eu recours à une *krysha*. À la suite de tensions internes, un individu connu sur Telegram sous le nom ExploitWhispers a décidé de publier les communications internes du collectif criminel, représentant 197 000 messages et menant à l'identification de liens entre le leader de BlackBasta, Oleg Nefedov (connu sous les pseudonymes *GG* et *AA*), et les autorités russes. Cette *krysha* pourrait lui avoir permis d'échapper à une arrestation en Arménie survenue en juin 2024 [139] [146] [147] [148] [150] [151]. En dépit des actions menées par les forces de l'ordre contre les membres de BlackBasta, ce collectif demeure actif en début d'année 2026, comme en témoigne la récente exploitation de la CVE-2025-68947 affectant un driver Windows par un opérateur du collectif criminel [149].



Extrait de conversation entre les opérateurs de BlackBasta :
« J'ai des hommes à moi à la Lubyanka et au GRU, ça fait longtemps que je les entretiens. » (sources : LeMagIt et Der Spiegel)

RomCom

Ce groupe d'attaquants, connu pour ses liens historiques avec les souches de ransomware Cuba, Industrial Spy et Team Underground, serait opéré par l'unité militaire russe n°29155, chargée des opérations offensives sur des réseaux informatiques pour le compte du GRU [152] [153] [154]. En 2025, le CERT-XMCO a observé les opérations d'espionnage du groupe en Europe et en Amérique du Nord, incluant la diffusion ponctuelle de SocGholish, un malware issu d'une infrastructure de type *Malware-as-a-Service*, employé pour exfiltrer des informations sensibles appartenant à des organisations stratégiques. Afin de conduire ses opérations offensives, RomCom aurait par ailleurs exploité la faille de sécurité CVE-2025-8088, vulnérabilité *0-day* affectant WinRAR [155].

Qilin

Le groupe Qilin s'est illustré en mars 2025 par la compromission du ministère des Affaires étrangères ukrainien. Cette variante de ransomware, déjà employée en février par le mode opératoire étatique nord-coréen Moonstone Sleet, laisse envisager une coopération récurrente entre acteurs cybercriminels et autorités russes dans le contexte du conflit ukrainien [156] [157].

Compromission du ministère ukrainien des Affaires étrangères par Qilin (source : CERT-XMCO)

2.2 DES CLUSTERS CRIMINELS INTÉGRÉS À L'ÉCOSYSTÈME « HACK FOR HIRE » EN CHINE

Comme la Russie, la République Populaire de Chine est soupçonnée d'avoir régulièrement instrumentalisé des groupes criminels au cours des dernières années, une pratique qui s'est poursuivie en 2025 [78] [79]. Le recours aux souches de ransomware a probablement permis à Pékin d'obfusquer l'origine et les motivations de diverses campagnes d'attaques.

2.2.1 LE CAS RÉVÉLATEUR DE LA SOCIÉTÉ CHINOISE SICHUAN SILENCE

Suivant cette approche, différentes structures privées pourraient opérer au bénéfice de l'État chinois, en conformité avec le cadre juridique national, tout en maintenant une marge d'autonomie dans la conduite de leurs activités. Le cas de l'affaire I-S00N en témoigne : cette entreprise a conduit des opérations d'espionnage en 2024 pour le compte du ministère de la Sécurité publique chinois [80] [81] [82]. Il est dès lors envisageable que des activités cybercriminelles aient été orchestrées par des entreprises privées sous contrat avec le gouvernement chinois, comme en atteste l'imposition de sanctions par le département du Trésor américain à l'encontre de **la société de cybersécurité chinoise Sichuan Silence, accusée d'avoir déployé une version du ransomware Ragnarok contre de nombreuses entités internationales** en avril 2020 [83].

En 2025, l'instrumentalisation du cybercrime en Chine est une tendance qui semble s'être poursuivie. En témoigne l'identification en février d'une campagne d'attaques à l'encontre d'une entreprise asiatique spécialisée dans les services informatiques via la distribution de *RA World* conjointement à une variante personnalisée de PlugX (aussi connu comme Korplug), associée au *cluster* Fireant. Cette souche avait été observée lors d'une précédente opération d'espionnage chinoise menée contre le ministère des Affaires étrangères d'un pays d'Europe du Sud [84]. En février 2025, deux rapports émanant d'Orange Cyberdéfense et de Trend Micro mettent en évidence une campagne d'attaques utilisant le chiffreur nouvellement référencé sous le nom de NailaoLocker [85] [86]. Les opérateurs ciblent alors des organisations à travers plusieurs régions du monde, dont des entreprises européennes évoluant dans le domaine de la santé. Cette opération, non associée à un mode opératoire spécifique, avait bénéficié du concours d'outils populaires chez les groupes APT sinophones, tels que ShadowPad et PlugX, ainsi que d'un botnet ou un réseau de type Operational Relay Box (ORB) destiné à complexifier la détection des serveurs *C2*.

2.2.2 UN ENVIRONNEMENT NORMATIF AU SERVICE DES AMBITIONS DE PÉKIN

Ces différentes opérations témoignent d'une stratégie globale menée par les autorités chinoises, destinée à obtenir un avantage comparatif sur les puissances étatiques concurrentes à Pékin, au-devant desquelles les États-Unis. Depuis 2021, la logique de conflictualité cyber opérée par la Chine s'est appuyée sur l'entrée en vigueur du projet *Regulation on the Management of Network Product Security Vulnerabilities (RSMV)*, dans le prolongement direct de la *Cybersecurity Law* de 2017, qui constitue un instrument juridique stratégique permettant à l'État chinois d'encadrer la découverte, la gestion et la divulgation des vulnérabilités informatiques au profit des intérêts du gouvernement [87] [88] [89].

Ce cadre réglementaire confère aux services de sécurité chinois un accès privilégié et anticipé à des vulnérabilités critiques, susceptibles d'être par la suite exploitées pour répondre aux objectifs politiques et économiques formulés par Pékin. **La RMSV constitue dès lors un habillage légal à une politique de rétention et de valorisation stratégique des vulnérabilités informatiques.** Ce maillon fonctionnel s'accompagne d'autres corpus juridiques, à l'instar de la *National Security Law* de 2015, destinés à transformer toute organisation ou individu en un soutien des activités de sécurité nationale chinoise [90] [91]. La RMSV semble alors s'inscrire

pleinement dans la doctrine de fusion civilo-militaire (en chinois : 军民融合), pouvant se résumer sous la forme suivante : le secteur privé découvre des vulnérabilités, l'État assure la captation légale de ces failles, puis les services de sécurité les exploitent.

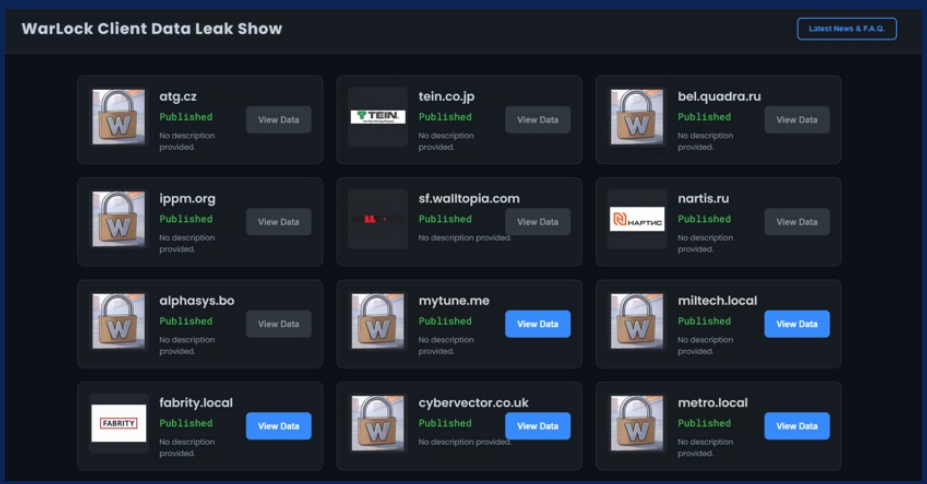
Warlock

En juillet 2025, Microsoft a publié un bulletin de sécurité sur l'exploitation de 2 failles de sécurité affectant Microsoft SharePoint et référencées CVE-2025-49704 et CVE-2025-49706. Chainées sous le nom de *ToolShell*, ces vulnérabilités désormais corrigées auraient permis à des groupes d'attaquants parrainés par l'État chinois de collecter des informations stratégiques sur diverses entités publiques et privées à l'international [158].

Lors des activités de réponse à incident, les chercheurs de Microsoft ont identifié trois *clusters* distincts exploitant les failles susmentionnées. Les deux premiers, documentés sous les noms de Linen Typhoon et Violet Typhoon (aka APT31) seraient directement opérés par les autorités chinoises, tandis que le troisième, référencé Storm-2603 (cluster ayant distribué le ransomware Warlock), est soupçonné d'être contrôlé par des acteurs sinophones aux motivations plurielles, expliquant son exploitation antérieure des souches Babuk et Lockbit Black [159].

Le recours à des solutions criminelles de type *Malware-as-a-Service* par Storm-2603 pourrait indiquer une victimologie motivée par des objectifs financiers, néanmoins, le groupe est suspecté d'être basé en Chine et d'opérer des attaques conjointes à d'autres acteurs sinophones soupçonnés d'être parrainés par l'État chinois. Cette coordination expliquerait ainsi l'exploitation des failles de sécurité *0-day* affectant Microsoft SharePoint et l'identification d'échantillons présentant des caractéristiques propres aux groupes APT chinois. L'exploitation coordonnée de la chaîne de vulnérabilités ToolShell ouvre la voie à une analyse plus large de la militarisation des failles 0-day dans l'écosystème cyber chinois.

La mise en œuvre simultanée des vulnérabilités CVE-2025-49704 et CVE-2025-49706 par le groupe Warlock, soupçonné d'être implanté en Chine et animé par des motivations essentiellement financières, ainsi que par des acteurs de type APT bénéficiant d'un parrainage étatique chinois, suggère l'existence d'une capacité offensive partagée autour de ToolShell. Cette convergence est cohérente avec le cadre de gestion et de contrôle des vulnérabilités instauré par la réglementation chinoise RMSV. Les opérateurs de Warlock semblent toujours actifs en février 2026, comme en témoigne leur récente exploitation de la CVE-2026-23760 affectant SmarterMail [160] [161]



Site opéré parWarlock pour revendiquer ses attaques (source : CERT-XMCO)

2.3 DES CLUSTERS CRIMINELS INFLUENCÉS PAR LES GARDIENS DE LA RÉVOLUTION ISLAMIQUE (IRGC)

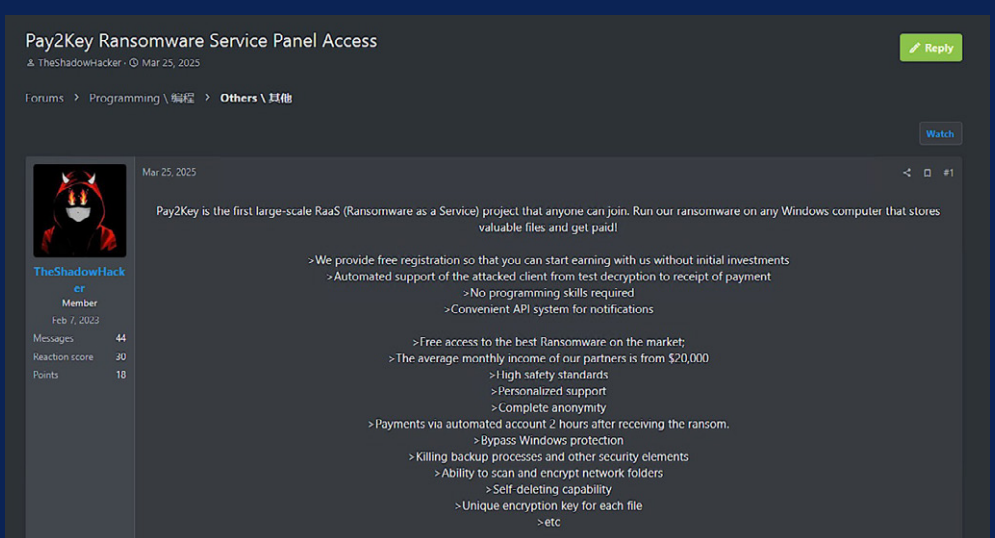
En 2025, l'Iran a intensifié l'instrumentalisation des groupes de ransomware comme vecteurs de politique étrangère, combinant motivations financières et idéologiques pour déstabiliser ses adversaires, en particulier l'État d'Israël et les États-Unis dans un contexte de tensions accrues au Moyen-Orient.

2.3.1 DES OPÉRATIONS D'INFLUENCE IRANIENNES CONDUITES PAR L'INTERMÉDIAIRE DE PROXYS CRIMINELS

Comme en Chine, l'Iran pourrait s'appuyer sur des proxys criminels prenant l'apparence d'entreprises IT pour mener ses campagnes d'attaques. Le régime iranien est ainsi soupçonné d'employer l'entreprise privée Emennet Pasargad et divers proxys cybercriminels pour revendiquer des opérations de sabotage ciblant ses adversaires régionaux et pour mener des activités d'influence dans le reste du monde. Depuis plusieurs années, l'Iran s'appuierait sur des modes opératoires issus de la cybercriminalité afin de brouiller l'attribution de ses opérations et de préserver un déni plausible des attaques [92] [93] [94] [95].

Pay2Key

En juillet, Morphisec a publié une analyse sur le groupe de *Ransomware-as-a-Service* Pay2Key (aussi nommé Pay2Key.I2P). En apparence motivé par des objectifs financiers, ce groupe est soupçonné de mener des opérations partisanes pour le compte de Téhéran contre les États-Unis et Israël, dont le regain d'activité au sein de l'écosystème cybercriminel pourrait coïncider avec la situation conflictuelle au Moyen-Orient au cours des derniers mois [162].
Les investigations menées par Morphisec ont notamment permis d'établir que le programme Pay2Key disposait de liens avec le mode opératoire APT Fox Kitten, lui aussi parrainé par l'Iran, ainsi qu'avec la souche de ransomware Mimic.
Le programme de *RaaS* Pay2Key.I2P a été promu sur des forums criminels russophones et sinophones depuis février 2025. Sur ce laps de temps, Morphisec estime que le groupe criminel aurait obtenu 51 rançons payées, démontrant l'efficacité de ses opérateurs, dont la victimologie se concentre sur des cibles occidentales.



Promotion du ransomware Pay2Key sur un forum cybercriminel (source : CERT-XMCO)

2.3.2 UNE APPROCHE DE LA GUERRE NON CONVENTIONNELLE BASÉE SUR LA NOTION DE « GUERRE DOUCE »

La notion de «guerre douce» a été introduite par les autorités iraniennes après la réélection de Mahmoud Ahmadinejad en 2009 [96]. Ce terme désigne l'approche iranienne de la guerre non conventionnelle reposant sur la manipulation de l'information et la guerre psychologique, plutôt que sur un affrontement militaire direct. Ce paradigme pourrait expliquer l'instrumentalisation fréquente des proxys criminels, à l'instar des groupes de ransomware, par les autorités iraniennes et en particulier le Corps des gardiens de la révolution islamique (IRGC).

Charlie Hebdo avait ainsi été victime de la conduite de cette approche de «guerre douce» en janvier 2023. La cyberattaque, intervenue à la suite de la publication par le journal de caricatures sur le régime de Téhéran, avait été opérée par le groupe Holy Souls et attribuée par Microsoft à la société iranienne *Emennet Pasargad* coordonnée par l'IRGC [97] [98] [99]. Cette opération sous faux-drapeau avait entrainé le défacement de la page d'accueil du site web du journal et le vol des données personnelles de 200 000 clients.

En août 2024, la CISA, le FBI et le DC3 avaient conjointement publié un avis de sécurité sur les activités criminelles menées par des groupes APT associés à l'Iran [100]. Leur rapport mettait en avant **la collaboration des groupes affiliés à Téhéran avec des opérateurs de ransomware, les incitant à cibler des organisations aux États-Unis, en Azerbaïdjan, aux Émirats Arabes Unis et en Israël**.

L'Iran était déjà soupçonné par la CISA d'avoir collaboré avec les opérateurs des *RaaS* NoEscape, Ransomhouse et ALPHV/BlackCat [101]. Le mode opératoire APT Pioneer Kitten (aussi connu comme UNC757, Parisite et Lemon Sandstorm) était notamment suspecté par la CISA d'avoir facilité des attaques par ransomware en monétisant les accès initiaux obtenus au sein d'organisations internationales évoluant dans les secteurs de la santé, de la finance, de l'enseignement, et à l'administration gouvernementale [101].

Plus tard en octobre 2024, la CISA publiait un avis de sécurité alertant de nouveau sur le parrainage d'opérations cybercriminelles par l'Iran via la mise en vente di'dentifiants de connexion volés sur des *marketplaces* criminelles. En agissant comme courtiers d'accès initiaux pour des groupes criminels, les opérateurs iraniens ont facilité la distribution de souches de ransomware contre des entités américaines stratégiques.

Vente d'accès volés sur une plateforme cybercriminelle par un faux profil iranien

Profil identifié sur un forum par le CERT-XMCO via l'adresse TOX divulguée par la CISA dans son avis de sécurité

2.4 DES CLUSTERS CRIMINELS AU CŒUR DE LA STRATÉGIE DE RÉSILIENCE DU RÉGIME NORD-CORÉEN

Au cours des dernières années, la Corée du Nord s'est distinguée par la mise en œuvre d'une diversité de modes opératoires destinée à assurer le financement du régime de Kim Jong-un, ainsi qu'à soutenir le projet politique de Pyongyang relatif à la réunification de la péninsule coréenne ; objectif étroitement lié au développement de son programme nucléaire et balistique [102]. Pour faire face à ses limites structurelles, l'État nord-coréen a historiquement exploité des ressources cybercriminelles par procuration, impliquant notamment les programmes de ransomware, permettant de surcroît de confondre une partie de ses opérations avec celles d'autres groupes d'attaquants [103].

2.4.1 UN CIBLAGE RÉPÉTÉ DES PLATEFORMES DE CRYPTOMONNAIES

Depuis plus de 10 ans, les modes opératoires APTs Kimsuky, Lazarus et Andariel ont exploité les tactiques, techniques et procédures traditionnellement associées aux collectifs cybercriminels. En dépit des tentatives d'obfuscation de leurs opérations, les acteurs nord-coréens ont été accusés d'avoir détourné plusieurs milliards de dollars au cours des dernières années. En 2024, l'Organisation des Nations Unies a enquêté sur les cyberattaques commises par la Corée du Nord et estime qu'elles sont susceptibles d'avoir rapporté 3 milliards de dollars au régime nord-coréen entre 2017 et 2023 [104]. La même année, Elliptic a signalé un détournement supplémentaire de 235 millions de dollars en cryptoactifs par un groupe nord-coréen non spécifié, via la compromission de la plateforme indienne WazirX [105]. Dans le prolongement de ces attaques, la plateforme d'échange de cryptomonnaies Bybit a été victime d'une opération cybercriminelle en février 2025, attribuée à des acteurs étatiques nord-coréens et ayant conduit au détournement de plus de 400 000 Ether, pour une valeur estimée à environ 1,5 milliard de dollars [106]. Cet incident, considéré comme le plus important vol de cryptomonnaies jamais documenté, démontre la volonté du régime d'inscrire ces activités dans **une stratégie de long terme visant à contourner les sanctions internationales et à générer des ressources financières durables pour le régime nord-coréen**.

2.4.2 UNE STRATÉGIE D'INFILTRATION CONSOLIDÉE DES ENTREPRISES STRATÉGIQUES OCCIDENTALES

À cet égard, Pyongyang déploie des **stratégies d'infiltration ciblant des entreprises européennes et nord-américaines**, en cherchant à positionner clandestinement ses agents à des postes susceptibles d'être exercés en télétravail [107] [108] [109]. Cette approche offre la perspective d'un accès progressif à des informations sensibles, tout en ayant la possibilité de générer des ressources financières complémentaires. Conjointement, ces mêmes acteurs recourent ponctuellement à la mise en place de **faux entretiens de recrutement via des plateformes professionnelles**, telles que LinkedIn, dans le but de cibler des individus évoluant dans des secteurs stratégiques, à l'image des NTIC et de la BITD [110] [111]. À cela s'ajoutent des attaques sophistiquées ciblant des chaines d'approvisionnement logicielles (*supply chain attack*). Ces compromissions épidémiques, reposant sur l'infection en amont de projets collaboratifs, de dépôts publics GitHub, ou bien encore d'outils légitimes populaires, permettraient à la Corée du Nord de répondre aux intérêts politiques et financiers du régime de Pyongyang via le détournement en cascade d'actifs en cryptomonnaies ou la collecte d'informations sensibles [112] [113] [114] [115].

2.4.3 LES RAAS COMME INSTRUMENT COMPLÉMENTAIRE DES AMBITIONS DE PYONGYANG

En 2025, les groupes d'attaquants rattachés au *Reconnaissance General Bureau*, au ministère de la Sécurité du

Peuple ou encore à la *Korean People's Army*, ont continué d'opérer ces activités, combinant espionnage industriel et détournement d'actifs financiers. Bien que la Corée du Nord soit soupçonnée d'avoir régulièrement recours à des opérations d'extorsion par ransomware, basées tantôt sur des souches de malware conçues en interne, tantôt sur le détournement de programmes de type *Ransomware-as-a-Service*, ces activités malveillantes n'en restent pas moins secondaires au regard de l'ensemble des activités cybercriminelles commanditées par le régime politique de Kim Jong-un. **En début d'année 2026, l'appareil étatique nord-coréen semble poursuivre la mobilisation des diverses capacités cybercriminelles afin de générer des ressources financières** [116] [117].

Moonstone Sleet

En mars 2025, Microsoft a publié une alerte sur le détournement du ransomware Qilin par le groupe nord-coréen Moonstone Sleet (aussi nommé Storm-1789) lors de multiples attaques [163]. Ce groupe APT, mû par des objectifs financiers et politiques, s'en serait servi pour viser des organisations actives dans les NTIC, le domaine éducatif ainsi que dans la base industrielle de défense. Selon Bitdefender, l'instrumentation de ce programme de *RaaS* par Moonstone Sleet expliquerait une soudaine augmentation des victimes sud-coréennes revendiquées sur le site du collectif criminel Qilin en 2025 [164] [165] [166].

Pour rappel, Moonstone Sleet est un groupe d'attaquants étatique qui a déjà eu recours à la distribution de ransomware lors d'attaques précédentes. En avril 2024, Microsoft signalait déjà la diffusion d'une souche de ransomware personnalisée, baptisée FakePenny. Cette dernière avait permis Moonstone Sleet de poursuivre des objectifs financiers via la demande d'un paiement de rançon.

Demande de rançon de Moonstone Sleet (source : Microsoft)

ScarCruft

En août 2025, les chercheurs de S2W ont signalé l'exploitation d'un ransomware par le mode opératoire nord-coréen ScarCruft (aka APT37). Historiquement documenté pour ses attaques ciblées contre des personnalités de premier plan et contre des structures gouvernementales, le *cluster* ScarCruft aurait eu recours à une nouvelle souche nommée VCD pour attaquer des utilisateurs sud-coréens afin de détourner des actifs financiers [167].

Le recours à ce mode opératoire contraste avec les activités d'espionnage historiquement associées au groupe ScarCruft, soupçonné d'être contrôlé par le ministère de la Sécurité d'État nord-coréen. En août 2023, ce groupe d'attaquants avait fait l'actualité suite à la découverte d'une *backdoor* lui étant attribuée au sein des systèmes informatiques de *Mashinostroyeniya*, un organisme industriel russe, spécialisé dans le secteur des missiles balistiques intercontinentaux [168]. En février 2024, ce même groupe avait cherché à distribuer une *backdoor* dans un logiciel utilisé par les représentations consulaires russes [169].

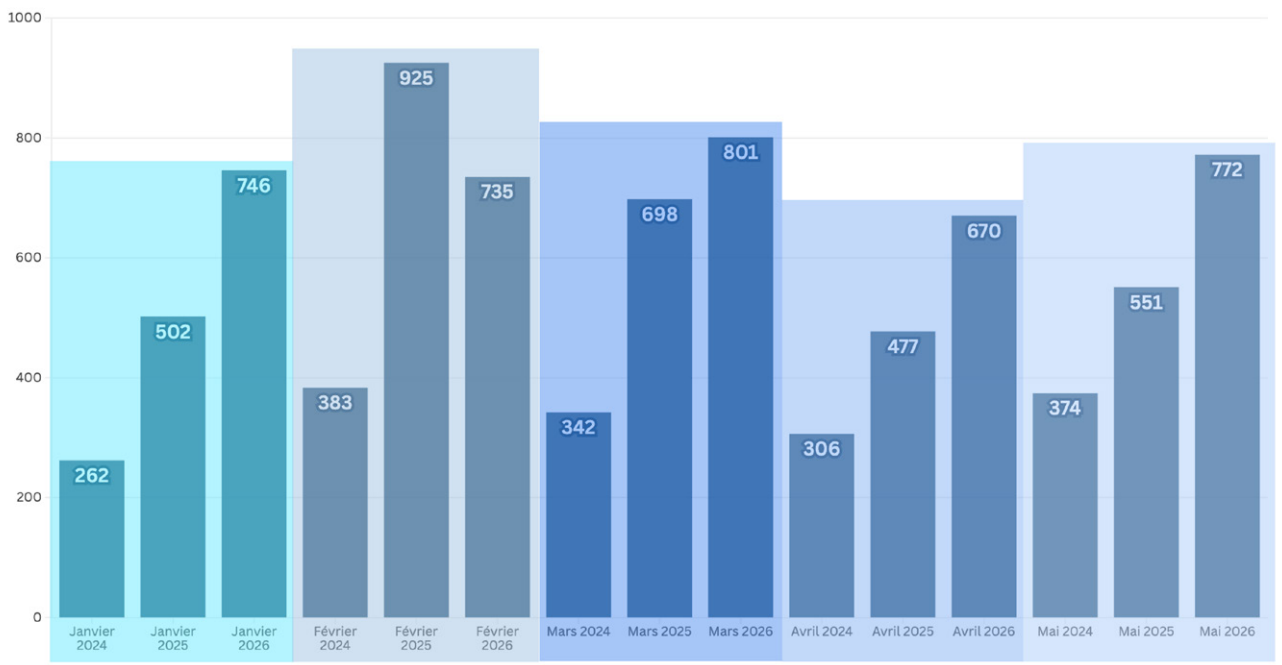
L'instrumentalisation de *RaaS* et l'exploitation de souches de ransomware personnalisées témoignent de la transversalité des opérations associées aux menaces *APTs* nord-coréennes, impliquant espionnage politique, influence et extorsion financière, ayant toutes les trois pour finalité de maintenir la dynastie Kim au pouvoir et d'assurer l'unification de la péninsule coréenne via la mise en oeuvre du programme nucléaire nord-coréen.

3. LES PERSPECTIVES DES OPÉRATEURS DE RANSOMWARE EN 2026

3.1 VERS UNE AUGMENTATION EXPONENTIELLE DES TENTATIVES D'EXTORSION EN 2026 ?

Le recours aux revendications d'attaque continue d'être une méthode largement employée par l'écosystème cybercriminel dans sa grande majorité. Ce mode opératoire, au-delà de provoquer un dommage réputationnel pour ses victimes, vise aussi à attirer l'attention des autres acteurs malveillants, dans la perspective d'une collaboration durable ou bien de l'accès à des ressources partagées en cercle restreint [118]. **Avec une augmentation de 2 778 victimes revendiquées à l'international entre 2024 et 2025, le CERT-XMCO présume que les groupes de ransomware revendiqueront un nombre croissant d'attaques en 2026.**

Cette perspective semble se confirmer en début d'année. Le mois de février 2025 constitue une exception, en raison des revendications de plus de 300 victimes par le groupe Cl0p. Celles-ci pourraient être liées à l'exploitation de la vulnérabilité zero-day CVE-2024-50623 affectant les produits Cleo, survenue en décembre 2024. Ces observations initiales devront être confirmées au cours des prochains mois de 2026, bien que les premiers relevés de l'année permettent d'émettre l'hypothèse d'une **augmentation exponentielle des tentatives d'extorsion des groupes de ransomware en France comme à l'international**.



COMPARAISON MENSUELLE DES ATTAQUES PAR RANSOMWARE REVENDIQUEES (2024-2026)
(source : données internes du CERT-XMCO)

À l'issue d'une année 2025 marquée par diverses opérations des forces de l'ordre destinées à démanteler les groupes prolifiques et à fragiliser les ressources de type *MaaS*, l'écosystème cybercriminel a été forcé de se réorganiser, prouvant par la même occasion la résilience des acteurs le composant, comme en témoigne la résurgence de SystemBC [119]. **Les groupes fragilisés par les opérations de police, à l'instar de Phobos, BlackBasta et BlackSuit, ont rapidement laissé leur place à des outsiders tels que Qilin et DragonForce, devenant omniprésents dans le paysage des RaaS en 2026.**

3.2 VERS UN CONTEXTE GÉOPOLITIQUE FAVORABLE POUR LES OPÉRATEURS DE RANSOMWARE ?

Les opérateurs de ransomware ont continué de prospérer en 2025, en dépit des nombreuses opérations policières ayant mené à des arrestations, des extraditions et aux démantèlements d'infrastructures malveillantes. Leur capacité d'adaptation s'est en grande partie appuyée sur un contexte géopolitique favorable, marqué par des zones de non-coopération judiciaire et des tensions internationales, leur offrant des espaces de refuge et facilitant la poursuite de leurs activités criminelles.

Suivant cette logique, la poursuite du conflit armé en Ukraine constituera en 2026 un frein aux actions menées contre le cybercrime. Une part importante des groupes de *Ransomware-as-a-Service* restant composée d'acteurs opérant depuis la Communauté des États Indépendants, ce positionnement géographique leur a permis d'échapper aux tentatives d'arrestation et d'extradition.
Les opérateurs de ransomware continueront de s'appuyer sur des environnements institutionnels peu propices à l'engagement de poursuites judiciaires, susceptibles d'expliquer une porosité grandissante des frontières entre les acteurs à motivation financière et ceux opérant à des fins d'espionnage ou d'influence stratégique.
Dans un contexte géopolitique dégradé, ces acteurs vont tirer parti des tensions accrues pour brouiller davantage la lecture de leurs motivations et de leurs commanditaires. Cette porosité étant désormais plus aisément documentée, certains groupes pour lesquels on observait jusque-là un simple alignement semblent aujourd'hui laisser supposer un niveau accru de coordination avec l'État iranien qui les soutient, tels que BQT. Lock ou Handala Hack.

- **Dans ce contexte, l'État russe pourrait faciliter la poursuite et le parrainage d'opérations cybercriminelles en 2026.** Cette complaisance pourrait expliquer le ciblage de certaines instances gouvernementales stratégiques par des acteurs russophones aux motivations financières, tels que RomCom et Qilin, ayant ciblé des organismes stratégiques l'année passée. En février 2026, la Direction nationale de la cybersécurité de la Roumanie a alerté sur l'instrumentalisation des groupes cybercriminel par la Russie, faisant suite à des attaques par ransomware ayant compromis des infrastructures stratégiques du secteur de l'énergie, telles que celles de Conpet et Oltenia Energy Complex [118].

- **Au Moyen-Orient, l'Iran semble toujours s'appuyer sur des ressources cybercriminelles pour mener des actions de sabotage et de désinformation contre ses adversaires politiques**, comme en témoigne l'instrumentalisation de Handala Hack par le groupe APT iranien Void Manticore ou bien encore le détournement du RaaS Chaos dans le cadre d'une opération sous faux drapeau menée par MuddyWater [119] [120].

- **En 2026, le financement de l'appareil étatique nord-coréen devrait continuer de reposer sur des activités cybercriminelles, notamment la diffusion de souches de ransomware.** En février, un sous-groupe affilié au groupe nord-coréen Lazarus a ainsi été identifié dans le cadre d'une campagne d'extorsion reposant sur le modèle de *Ransomware-as-a-Service (RaaS)* Medusa, visant principalement des organisations du secteur de la santé ainsi que des structures à but non lucratif, majoritairement situées aux États-Unis [121] [122].

Ainsi, le recours à des ressources cybercriminelles permet à des instances étatiques de mener des opérations clandestines tout en ayant la possibilité d'en nier la responsabilité. La sous-traitance des activités offensives étatiques à des groupes criminels, prenant parfois l'apparence d'entreprises privées légales, est une tendance qui avait déjà été documentée dans le Bilan des activités Yuno 2024 du CERT-XMCO et qui reste susceptible de se poursuivre sur l'année 2026 [123].

3.3 VERS UNE INDUSTRIALISATION DES ATTAQUES CIBLANT LA SUPPLY CHAIN LOGICIELLE ?

En 2025, les consultants du CERT-XMCO ont noté un ciblage répétitif des chaînes d'approvisionnement logicielles des entreprises par les opérateurs de ransomware, facilitant ainsi des compromissions de grande ampleur. Des collectifs tels que Cl0p, ShinyHunters et TeamPCP ont illustré trois variantes d'une même stratégie d'extorsion de données : respectivement basées sur l'identification de failles chez fournisseurs de confiance, sur la compromission d'environnements d'entreprises par détournement d'identité, ou encore sur l'utilisation abusive de solutions open source.

3.3.1 L'IDENTIFICATION DE FAILLES DE SÉCURITÉ PAR CL0P

Au cours des dernières années, Cl0p s'est illustré par l'identification et l'exploitation de plusieurs failles de sécurité 0-day au sein de solutions de transfert de fichiers sécurisées largement répandues au sein d'environnements d'entreprise. Cl0p constitue un cas d'école des groupes de ransomware ciblant activement la chaîne d'approvisionnement logicielle de ses victimes afin d'accéder à d'importants volumes de données réparties dans de nombreuses organisations. Actif depuis 2019, ce collectif cybercriminel est responsable de vastes campagnes d'attaques par supply chain, documentées dans une section dédiée de ce rapport. Ce mode opératoire devrait être de nouveau éprouvé en 2026.

3.3.2 LE DÉTOURNEMENT D'IDENTITÉ PAR SHINYHUNTERS

La perspective d'une industrialisation des attaques par ransomware basées sur la supply chain logicielle en 2026 s'appuie également sur le cas du groupe ShinyHunters, dont le modèle d'extorsion utilisé en 2025 a tiré profit d'une large intégration des *SaaS*, des jetons à privilèges excessifs et de la confiance humaine de ses victimes. Ainsi, lorsqu'une unique plateforme tierce dispose d'un accès à des environnements tels que Salesforce, Gainsight ou encore Zendesk, la compromission d'un seul jeu d'identifiants par ShinyHunters a entraîné l'exposition de volumes significatifs de données internes l'année passée [132] [133] [134].

3.3.3 LA COMPROMISSION DE SOLUTIONS OPEN SOURCE PAR TEAMPCP

L'industrialisation des attaques par ransomware basées sur la *supply chain* logicielle semble déjà se poursuivre en début d'année 2026 comme en témoigne le cas du mode opératoire TeamPCP. Ce *cluster*, disposant de liens potentiels avec le groupe cybercriminel LAPSUS$, s'est illustré par la compromission du scanner de vulnérabilités open-source Trivy, permettant ensuite aux attaquants d'injecter du code malveillant directement dans les processus des organisations qui reposaient sur des pipelines CI/CD, qui s'exécutaient sans systématiquement vérifier que le code source avait été modifié, résultant sur l'infection de la bibliothèque Python LiteLLM, KICS, ou bien encore du paquet PyPI de Telnyx [135] [136] [137] [138].

Dimension	Cl0p	ShinyHunters	TeamPCP
Vecteur d'attaque	Vulnérabilité logicielle	Détournement de comptes SaaS	Injection de code malveillant dans des projets open source
Mécanisme de redondance	Exploitation d'une faille dans un logiciel d'entreprises populaire, disposant de centaines de clients	Détournement de comptes privilégiés dans des solutions SaaS : accès à de multiples tenants	Compromission d'une dépendance initiale menant à la distribution de versions malveillantes à tous ses utilisateurs

4. PANORAMA MENSUEL DES ATTAQUES PAR RANSOMWARE SIGNALÉES EN FRANCE 2025

4.1.1 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 [170].

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.

4.1.2 FÉVRIER

14 attaques revendiquées par les groupes de ransomware en février 2025			
Localisation régionale	**Entité française 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 [171] [172] [173].

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.

4.1.3 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'exacerbé la pression exercée [174].

4.1.4 AVRIL

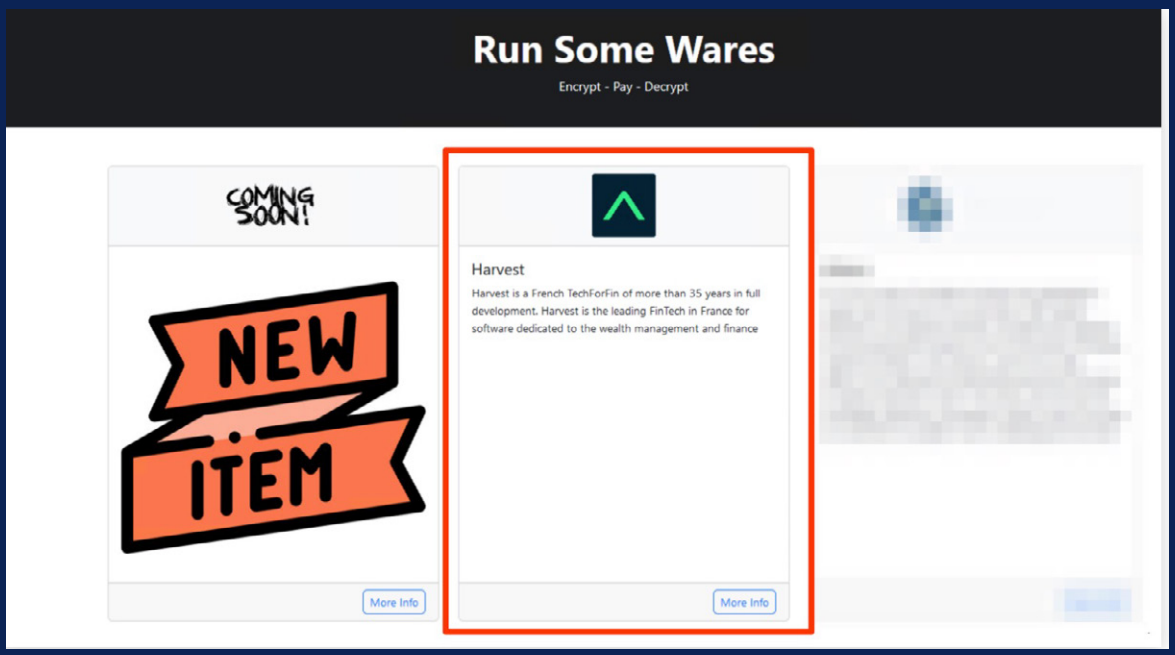
4 attaques revendiquées par les groupes de ransomware en avril 2025			
Localisation régionale	**Taille de l'entité ciblée**	**Secteur d'activités**	**Groupe de ransomware**
Ile-de-France	Non spécifiée	Société civile	Nightspire
Centre-Val de Loire	Microentreprise	Secteur public	Nightspire
Ile-de-France	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 [175].

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)

4.1.5 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

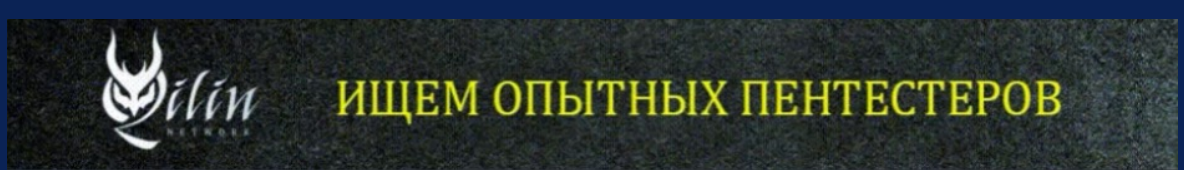
Avec plus de 1 200 victimes à son actif, Qilin est un programme criminel opéré selon un modèle de *Ransomware-as-a-Service (RaaS)*, principalement motivé par des objectifs financiers et ciblant ses victimes de manière largement opportuniste. Ce groupe a été activement documenté par le CERT-XMCO au cours 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 [176].

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 [177] [178] [179].

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)

4.1.6 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 [180].

Déclaration du collectif Stormous sur Telegram (source : LeMagIt)

4.1.7 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 [181] [182] [183].

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.

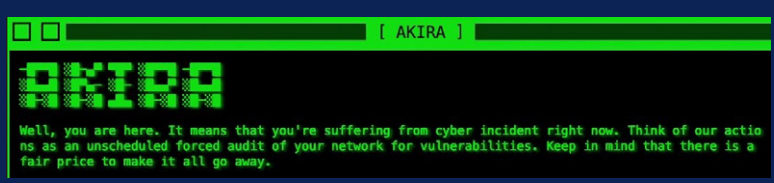


Illustration d'une note de rançon d'Akira (source : LeMagIt)

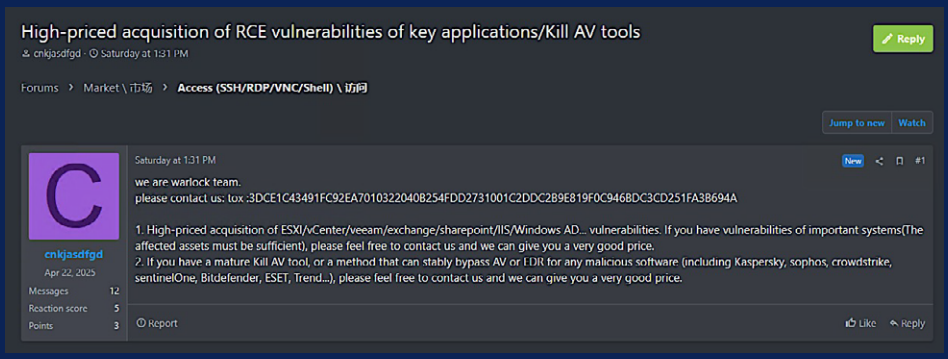
4.1.8 AOÛT

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 [184] [185] [186].

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 [187].



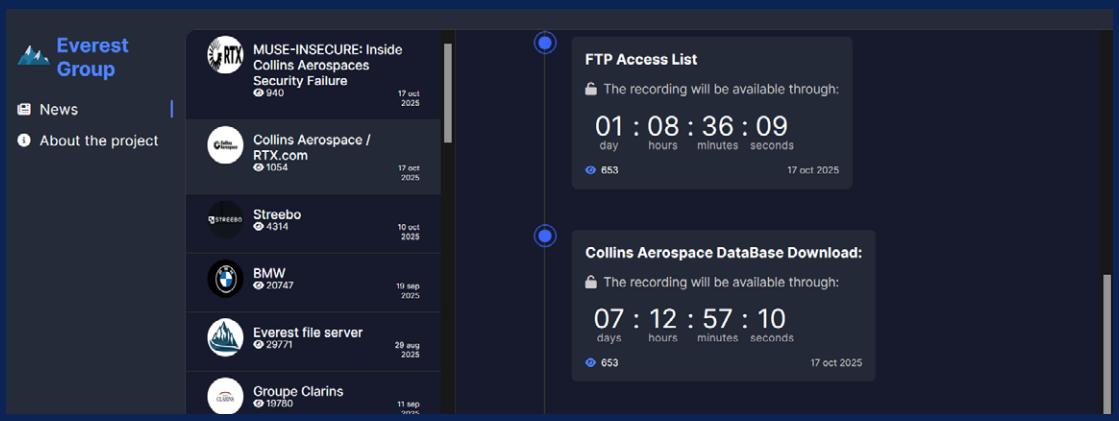
Achat de failles de sécurité par l'administrateur de Warlock (source : CERT-XMCO)

4.1.9 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 [191]. 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.



Revendication de l'attaque contre Collins Aerospace par Everest (source : CERT-XMCO)

4.1.10 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

Suite

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.

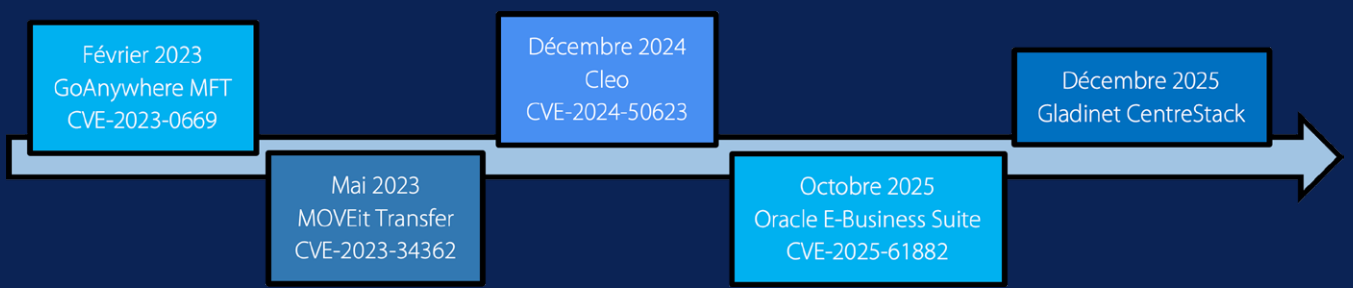
Le collectif de ransomware Cl0p est connu pour cibler les solutions d'entreprise. Par le passé, ce groupe cybercriminel a opéré plusieurs campagnes de vol de données via l'identification et le détournement de vulnérabilités affectant Accellion FTA, GoAnywhere MFT, MOVEit Transfer ainsi que les produits Cleo [192] [193] [194].

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 [195].

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



4.1.11 NOVEMBRE

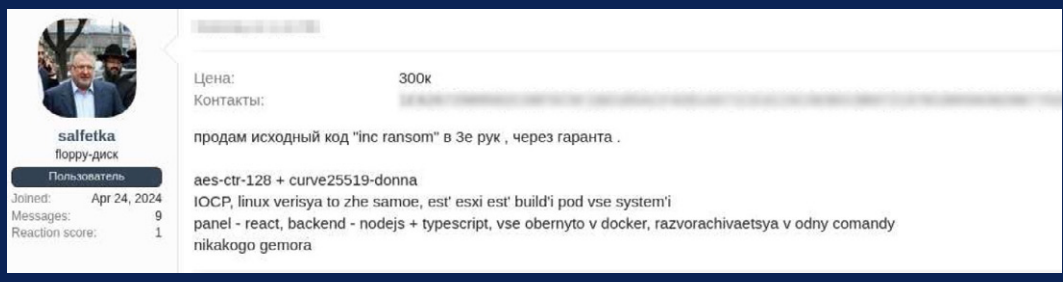
7 attaques revendiquées par les groupes de ransomware en novembre 2025			
Localisation régionale	**Taille de l'entité ciblée**	**Secteur d'activités**	**Groupe de ransomware**
Ile-de-France	ETI	Fabrication	Qilin
Ile-de-France	Microentreprise	Energie	Incransom
Auvergne-Rhône-Alpes	Grande entreprise	Fabrication	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 [199] [200]. 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 [197] [198].

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 [204] [205]. 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 [206] [207] [208]. 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 [201] [202] [203].

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 [209]. 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 [210].



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

4.1.12 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 [196]. 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.

5. 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.

5. BIBLIOGRAPHIE

[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-whitepapers/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] Halcyon, «Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C,» 13 01 2025. [En ligne]. Available: https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c

[13] Microsoft, « Storm-0501's evolving techniques lead to cloud-based ransomware,» 27 08 2025. [En ligne]. Available: https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

[14] S-RM, «Camera off: Akira deploys ransomware via webcam,» 05 03 2025. [En ligne]. Available: https://www.s-rminform.com/latest-thinking/camera-off-akira-deploys-ransomware-via-webcam

[15] L. M. Informatique, «L'EDR de SentinelOne neutralisé pour installer une variante du ransomware Babuk,» 07 05 2025. [En ligne]. Available: https://www.lemondeinformatique.fr/actualites/lire-l-edr-de-sentinelone-neutralise-pour-installer-une-variante-du-ransomware-babuk-96790.html

[16] ESET, « Introducing HybridPetya: Petya/NotPetya copycat with UEFI Secure Boot bypass,» 12 09 2025. [En ligne]. Available: https://www.welivesecurity.com/en/eset-research/introducing-hybridpetya-petya-notpetya-copycat-uefi-secure-boot-bypass/

[17] T. Wired, «The Untold Story of NotPetya, the Most Devastating Cyberattack in History,» 22 08 2018. [En ligne]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[18] CheckPoint, «Cyber Criminals Are Recruiting Insiders in Banks, Telecoms, and Tech,» 19 12 2025. [En ligne]. Available: https://blog.checkpoint.com/research/cyber-criminals-are-recruiting-insiders-in-banks-telecoms-and-tech

[19] DarkReading, «Cybercriminals Court Traitorous Insiders via Ransom Notes,» 04 02 2025. [En ligne]. Available: https://www.darkreading.com/threat-intelligence/cybercriminals-traitorous-insiders-ransom-notes?utm_source=chatgpt.com

[20] TechCrunch, «CrowdStrike fires 'suspicious insider' who passed information to hackers,» 21 11 2025. [En ligne]. Available: https://techcrunch.com/2025/11/21/crowdstrike-fires-suspicious-insider-who-passed-information-to-hackers/

[21] BBC, «'You'll never need to work again': Criminals offer reporter money to hack BBC,» 29 09 2025. [En ligne]. Available: https://www.bbc.com/news/articles/c3w5n903447o

[22] ForeScout, «New Ransomware Operator Exploits Fortinet Vulnerability Duo,» 13 03 2025. [En ligne]. Available: https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/

[23] SecurityAffairs, «Ransomware gangs exploit a Paragon Partition Manager BioNTdrv.sys driver zero-day,» 01 03 2025. [En ligne]. Available: https://securityaffairs.com/174789/cyber-crime/ransomware-gangs-paragon-partition-manager-biontdrv-sys-driver-zero-day-attacks.html

[24] BleepingComputer, «Oracle patches EBS zero-day exploited in Clop data theft attacks,» 05 10 2025. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/oracle-patches-ebs-zero-day-exploited-in-clop-data-theft-attacks/

[25] BleepingComputer, «Oracle silently fixes zero-day exploit leaked by ShinyHunters,» 14 10 2025. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/oracle-silently-fixes-zero-day-exploit-leaked-by-shinyhunters/

[26] D. Report, «Confluence Exploit Leads to LockBit Ransomware,» 24 02 2025. [En ligne]. Available: https://thedfirreport.com/2025/02/24/confluence-exploit-leads-to-lockbit-ransomware/

[27] D. Report, «Another Confluence Bites the Dust: Falling to ELPACO-team Ransomware,» 19 05 2025. [En ligne]. Available: https://thedfirreport.com/2025/05/19/another-confluence-bites-the-dust-falling-to-elpaco-team-ransomware/

[28] F. Effect, «Not-so-SimpleHelp exploits enabling deployment of Sliver backdoor,» 06 02 2025. [En ligne]. Available: https://fieldeffect.com/blog/field-effect-mitigates-not-so-simplehelp-exploits-enabling-deployment-of-backdoors

[29] Sophos, «DragonForce actors target SimpleHelp vulnerabilities to attack MSP, customers,» 27 05 2025. [En ligne]. Available: https://www.sophos.com/en-us/blog/dragonforce-actors-target-simplehelp-vulnerabilities-to-attack-msp-customers

[30] CISA, «#StopRansomware: Play Ransomware,» 04 06 2025. [En ligne]. Available: https://www.ic3.gov/CSA/2025/250604.pdf.

[31] SecurityAffairs, « Ransomware gangs exploit a Paragon Partition Manager BioNTdrv.sys driver zero-day,» 01 03 2025. [En ligne]. Available: https://securityaffairs.com/174789/cyber-crime/ransomware-gangs-paragon-partition-manager-biontdrv-sys-driver-zero-day-attacks.html

[32] Tenable, « CVE-2024-55591: Fortinet Authentication Bypass Zero-Day Vulnerability Exploited in the Wild,» 14 01 2025. [En ligne]. Available: https://www.tenable.com/blog/cve-2024-55591-fortinet-authentication-bypass-zero-day-vulnerability-exploited-in-the-wild

[33] Tenable, « CVE-2024-55591: Fortinet Authentication Bypass Zero-Day Vulnerability Exploited in the Wild,» 14 01 2025. [En ligne]. Available: https://www.tenable.com/blog/cve-2024-55591-fortinet-authentication-bypass-zero-day-vulnerability-exploited-in-the-wild

[34] ForeScout, «New Ransomware Operator Exploits Fortinet Vulnerability Duo,» 13 03 2025. [En ligne].
Available: https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/
[35] Prodaft, «Threat actors are actively exploiting Fortigate vulnerabilities (CVE-2024-21762, CVE-2024-55591, and others) to deploy Qilin ransomware.,» 06 06 2025. [En ligne].
Available: https://x.com/PRODAFT/status/1930959948810264845
[36] Microsoft, « Exploitation of CLFS zero-day leads to ransomware activity,» 08 04 2025. [En ligne]. A
Available: https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity.
[37] Microsoft, « Exploitation of CLFS zero-day leads to ransomware activity,». [En ligne].
Available: https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/, 08 04 2025
[38] Symantec, «Ransomware Attackers Leveraged Privilege Escalation Zero-day,» 07 05 2025. [En ligne].
Available: https://www.security.com/threat-intelligence/play-ransomware-zero-day
[39] Rapid7, «Active exploitation of SAP NetWeaver Visual Composer CVE-2025-31324,» 28 04 2025. [En ligne].
Available: https://www.rapid7.com/blog/post/2025/04/28/etr-active-exploitation-of-sap-netweaver-visual-composer-cve-2025-31324/
[40] Reliaquest, «ReliaQuest Uncovers New Critical Vulnerability in SAP NetWeaver,» 15 08 2025. [En ligne].
Available: https://reliaquest.com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/
[41] Sekoia, « The Sharp Taste of Mimo'lette: Analyzing Mimo's Latest Campaign targeting Craft CMS,» 27 05 2025. [En ligne].
Available: https://blog.sekoia.io/the-sharp-taste-of-mimolette-analyzing-mimos-latest-campaign-targeting-craft-cms/
[42] Google, «Ransomware Under Pressure: Tactics, Techniques, and Procedures in a Shifting Threat Landscape,» 16 03 2026. [En ligne].
Available: https://cloud.google.com/blog/topics/threat-intelligence/ransomware-ttps-shifting-threat-landscape/?hl=en
[43] 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/
[44] 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/
[45] U. P. Alto, «Project AK47: Uncovering a Link to the SharePoint Vulnerability Attacks,» 05 08 2025. [En ligne].
Available: https://unit42.paloaltonetworks.com/ak47-activity-linked-to-sharepoint-vulnerabilities/
[46] Google, «Ongoing SonicWall Secure Mobile Access (SMA) Exploitation Campaign using the OVERSTEP Backdoor,» 16 07 2025. [En ligne].
Available: https://cloud.google.com/blog/topics/threat-intelligence/sonicwall-secure-mobile-access-exploitation-overstep-backdoor
[47] SonicWall, «Gen 7 and newer SonicWall Firewalls – SSLVPN Recent Threat Activity,» 04 08 2025. [En ligne].
Available: https://www.sonicwall.com/support/notices/gen-7-and-newer-sonicwall-firewalls-sslvpn-recent-threat-activity/kA1VN0000000RDG0A2
[48] ESET, « Update WinRAR tools now: RomCom and others exploiting zero-day vulnerability,» 11 08 2025. [En ligne].
Available: https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/
[49] ESET, « Introducing HybridPetya: Petya/NotPetya copycat with UEFI Secure Boot bypass,» 12 09 2025. [En ligne].
Available: https://www.welivesecurity.com/en/eset-research/introducing-hybridpetya-petya-notpetya-copycat-uefi-secure-boot-bypass/
[50] Sophos, «GOLD SALEM's Warlock operation joins busy ransomware landscape,» 17 09 2025. [En ligne].
Available: https://www.sophos.com/en-us/blog/gold-salems-warlock-operation-joins-busy-ransomware-landscape/
[51] C. Talos, «New BYOVD loader behind DeadLock ransomware attack,» 09 12 2025. [En ligne].
Available: https://blog.talosintelligence.com/byovd-loader-deadlock-ransomware/
[52] Oracle, «Oracle Security Alert Advisory - CVE-2025-61882,» 04 10 2025. [En ligne].
Available: https://www.oracle.com/security-alerts/alert-cve-2025-61882.html
[53] Microsoft, « Investigating active exploitation of CVE-2025-10035 GoAnywhere Managed File Transfer vulnerability,» 06 10 2025. [En ligne].
Available: https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed-file-transfer-vulnerability/
[54] C. Talos, «Velociraptor leveraged in ransomware attacks,» 09 10 2025. [En ligne].
Available: https://blog.talosintelligence.com/velociraptor-leveraged-in-ransomware-attacks/
[55] SecuirtyAffairs, « Old Linux Kernel flaw CVE-2024-1086 resurfaces in ransomware attacks,» 31 10 2025. [En ligne].
Available: https://securityaffairs.com/184076/security/old-linux-kernel-flaw-cve-2024-1086-resurfaces-in-ransomware-attacks.html
[56] Zscaler, «Zscaler Threat Hunting Discovers and Reconstructs a Sophisticated Water Gamayun APT Group Attack,» 25 11 2025. [En ligne].
Available: https://www.zscaler.com/blogs/security-research/water-gamayun-apt-attack
[57] S-RM, «React2Shell used as initial access vector for Weaxor ransomware deployment,» 16 12 2025. [En ligne].
Available: https://www.s-rminform.com/latest-thinking/react2shell-used-as-initial-access-vector-for-weaxor-ransomware-deployment
[58] C. Intelligence, «Clop ransomware targets Gladinet CentreStack in data theft attacks,» 18 12 2025. [En ligne].
Available: https://www.linkedin.com/posts/curatedintelligence_psa-incident-responders-from-the-curated-activity-7407480091133231104-C6hv/
[59] Microsoft, « Threat actor DEV-0322 exploiting ZOHO ManageEngine ADSelfService Plus,» 08 11 2021. [En ligne].
Available: https://www.microsoft.com/en-us/security/blog/2021/11/08/threat-actor-dev-0322-exploiting-zoho-manageengine-adselfservice-plus/
[60] Wiz, «Critical vulnerabilities in NetScaler ADC exploited in-the-wild: everything you need to know,» 06 07 2025. [En ligne].
Available: https://www.wiz.io/blog/critical-vulnerabilities-netscaler-adc-exploited-in-the-wild-cve-2025-5777
[61] Volexity, « Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400),» 12 04 2024. [En ligne].
Available: https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/
[62] CrushFTP, «CVE-2025-31161: CrushFTP vulnerability analysis and mitigation,» 03 04 2025. [En ligne].
Available: https://www.wiz.io/vulnerability-database/cve/cve-2025-31161
[63] Lemonde.fr, «Revealed: Group 78, the secret US task force fighting cybercriminals,» 16 10 2025. [En ligne].
Available: https://www.lemonde.fr/en/pixels/article/2025/10/16/revelations-on-group-78-the-secret-us-task-force-that-fights-cybercriminals_6746474_13.html
[64] ESET, « Shifting the sands of RansomHub's EDRKillShifter,» 26 03 2025. [En ligne].
Available: https://www.welivesecurity.com/en/eset-research/shifting-sands-ransomhub-edrkillshifter/
[65] Symantec, «RansomHub: Attackers Leverage New Custom Backdoor,» 20 03 2025. [En ligne].
Available: https://www.security.com/threat-intelligence/ransomhub-betruger-backdoo
[66] Group-IB, «Ransomware debris: an analysis of the RansomHub operation,» 30 04 2025. [En ligne].
Available: https://www.group-ib.com/blog/ransomware-debris/

[67] L. M. Informatique, «DragonForce, Qilin et Lockbit forment un cartel du cybercrime,» 10 10 2025. [En ligne]. Available: https://www.lemondeinformatique.fr/actualites/lire-dragonforce-qilin-et-lockbit-forment-un-cartel-du-cybercrime-98137.html
[68] DarkReading, «Ransomware Gang Goes Full 'Godfather' With Cartel,» 04 02 2026. [En ligne]. Available: https://www.darkreading.com/cyber-risk/ransomware-gang-full-godfather-cartel
[69] Resecurity, «Trinity of Chaos: The LAPSUS$, ShinyHunters, and Scattered Spider Alliance Embarks on Global Cybercrime Spree,» 25 09 2025. [En ligne]. Available: https://www.resecurity.com/blog/article/trinity-of-chaos-the-lapsus-shinyhunters-and-scattered-spider-alliance-embarks-on-global-cybercrime-spree
[70] Group-IB, «The beginning of the end: the story of Hunters International,» 02 04 2025. [En ligne]. Available: https://www.group-ib.com/blog/hunters-international-ransomware-group/
[71] Eclecticiq, «GLOBAL GROUP: Emerging Ransomware-as-a-Service, supporting AI driven negotiation and mobile control panel for their affiliates,» 15 07 2025. [En ligne]. Available: https://blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service
[72] Intrinsec, « Global Group: ransomware rebranding stories,» 30 10 2025. [En ligne]. Available: https://www.intrinsec.com/global-group-ransomware-rebranding-stories/
[73] Rapid7, «The Post-RAMP Era: Allegations, Fragmentation, and the Rebuilding of the Ransomware Underground,» 25 02 2025. [En ligne]. Available: https://www.rapid7.com/blog/post/tr-post-ramp-allegations-fragmentation-ransomware-underground-rebuild/
[74] Europol, «Law enforcement takes down two largest cybercrime forums in the world,» 30 01 2025. [En ligne]. Available: https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world
[75] Europol, «Key figure behind major Russian-speaking cybercrime forum targeted in Ukraine,» 23 07 2025. [En ligne]. Available: https://www.europol.europa.eu/media-press/newsroom/news/key-figure-behind-major-russian-speaking-cybercrime-forum-targeted-in-ukraine
[76] HackRead, «Russian Cybercrime Platform RAMP Forum Seized by FBI,» 28 01 2026. [En ligne]. Available: https://hackread.com/russian-cybercrime-ramp-forum-seized-fbi/
[77] FalconFeeds.com, «SLSH Posted Recruitment Offers for Insider Access to Corporate Networks,» 30 01 2026. [En ligne]. Available: https://x.com/FalconFeedsio/status/2017179170229678253
[78] B. Computer, «Coinbase confirms insider breach linked to leaked support tool screenshots,» 03 02 2026. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/coinbase-confirms-insider-breach-linked-to-leaked-support-tool-screenshots/
[79] Wikipedia, «крыша,» [En ligne]. Available: https://en.wiktionary.org/wiki/%D0%BA%D1%80%D1%8B%D1%88%D0%B0
[80] D. Center, «ГРУ Эволюция, методы, кризис,» 12 09 2025. [En ligne]. Available: https://gru.dossier.center/
[81] Intel471, «Why Russia is a Hotbed of Cybercrime,» 24 09 2024. [En ligne]. Available: https://www.intel471.com/blog/why-russia-is-a-hotbed-of-cybercrime
[82] R. Future, «Dark Covenant 3.0: Controlled Impunity and Russia's Cybercriminals,» 23 10 2025. [En ligne]. Available: https://www.recordedfuture.com/research/dark-covenant-3-controlled-impunity-and-russias-cybercriminals
[83] T. Insider, «Hidden Bear: The GRU hackers of Russia's most notorious kill squad,» 31 05 2025. [En ligne]. Available: https://theins.ru/en/inv/281731
[84] T. Insider, «Hidden Bear: The GRU hackers of Russia's most notorious kill squad,» 31 05 2025. [En ligne]. Available: https://theins.ru/en/inv/281731
[85] TRM, «Nine Emerging Groups Shaping the Ransomware Landscape,» 06 10 2025. [En ligne]. Available: https://www.trmlabs.com/resources/blog/nine-emerging-groups-shaping-the-ransomware-landscape
[86] BleepingComputer, «RedCurl cyberspies create ransomware to encrypt Hyper-V servers,» 26 03 2025. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/redcurl-cyberspies-create-ransomware-to-encrypt-hyper-v-servers/
[87] R. Future, « Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine,» 31 01 2023. [En ligne]. Available: https://www.recordedfuture.com/research/dark-covenant-2-cybercrime-russian-state-war-ukraine
[88] Virtual-Routes, « Pharos Report No. 3: Ransomware's New Masters: How States Are Hijacking Cybercrime,» 23 04 2025. [En ligne]. Available: https://virtual-routes.org/pharos-report-no-3-ransomwares-new-masters-how-states-are-hijacking-cybercrime/
[89] SentinelOne, «ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware,» 26 06 2024. [En ligne]. Available: https://www.sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/
[90] O. Cyberdéfense, «The hidden network: How China unites state, corporate, and academic assets for cyber offensive campaigns,» 24 11 2024. [En ligne]. Available: https://www.orangecyberdefense.com/global/blog/cert-news/the-hidden-network-how-china-unites-state-corporate-and-academic-assets-for-cyber-offensive-campaigns
[91] R. Future, « Attributing I-SOON: Private Contractor Linked to Multiple Chinese State-sponsored Groups,» 20 03 2024. [En ligne]. Available: https://www.recordedfuture.com/fr/research/attributing-i-soon-private-contractor-linked-chinese-state-sponsored-groups
[92] Unit42, «Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns,» 23 02 2024. [En ligne]. Available: https://unit42.paloaltonetworks.com/i-soon-data-leaks/
[93] D. o. t. T. O. o. F. A. Control, « Treasury Sanctions Cybersecurity Company Involved in Compromise of Firewall Products and Attempted Ransomware Attacks,» 10 12 2024. [En ligne]. Available: https://home.treasury.gov/news/press-releases/jy2742
[94] Symantec, «China-linked Espionage Tools Used in Ransomware Attacks,» 13 02 2025. [En ligne]. Available: https://www.security.com/threat-intelligence/chinese-espionage-ransomware
[95] O. Cyberdéfense, «Faites connaissance avec NailaoLocker: un ransomware distribué en Europe par les backdoors ShadowPad et PlugX,» 27 02 2025. [En ligne]. Available: https://www.orangecyberdefense.com/fr/insights/blog/faites-connaissance-avec-nailaolocker-un-ransomware-distribue-en-europe-par-les-backdoors-shadowpad-et-plugx.
[96] T. Micro, «Updated Shadowpad Malware Leads to Ransomware Deployment,» 20 02 2025. [En ligne]. Available: https://www.trendmicro.com/en_us/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html
[97] Intrinsec, « China : Vulnerabilities as a strategic resource,» 24 10 2024. [En ligne]. Available: https://www.intrinsec.com/china-vulnerabilities-as-a-strategic-resource/
[98] Flashpoint, «How China's "Walled Garden" is Redefining the Cyber Threat Landscape,» 30 01 2026. [En ligne]. Available: https://flashpoint.io/blog/chinas-walled-garden-redefining-cyber-threat-landscape/
[99] Wikipedia, «China National Vulnerability Database,» 06 02 2026. [En ligne]. Available: https://en.wikipedia.org/wiki/China_National_Vulnerability_Database?utm_source=chatgpt.com

[100] Wikipedia, «National Security Law of the People's Republic of China,» 06 02 2026. [En ligne].
Available: https://en.wikipedia.org/wiki/National_Security_Law_of_the_People%27s_Republic_of_China
[101] Sekoia, « A three beats waltz: The ecosystem behind Chinese state-sponsored cyber threats,» 13 11 2024. [En ligne].
Available: https://blog.sekoia.io/a-three-beats-waltz-the-ecosystem-behind-chinese-state-sponsored-cyber-threats/
[102] Carnegie, «Iran's Cyber Threat: Espionage, Sabotage, and Revenge,» 04 01 2018. [En ligne].
Available: https://carnegieendowment.org/research/2018/01/irans-cyber-threat-espionage-sabotage-and-revenge?lang=en
[103] U. D. o. Treasury, « Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity,» 14 09 2022. [En ligne].
Available: https://home.treasury.gov/news/press-releases/jy0948
[104] NCSC, «UK and allies expose Iranian state agency for exploiting cyber vulnerabilities for ransomware operations,» 20 09 2022. [En ligne].
Available: https://www.ncsc.gov.uk/news/uk-and-allies-expose-iranian-state-agency-for-exploiting-cyber-vulnerabilities-for-ransom-operations
[105] Sekoia, « Iran Cyber Threat Overview,» 05 06 2023. [En ligne].
Available: https://blog.sekoia.io/iran-cyber-threat-overview/
[106] R. Future, « Social Engineering Remains Key Tradecraft for Iranian APTs,» 20 03 2022. [En ligne].
Available: https://www.recordedfuture.com/research/social-engineering-remains-key-tradecraft-for-iranian-apts
[107] Microsoft, « L'Iran responsable des attaques contre Charlie Hebdo,» 02 02 2023. [En ligne].
Available: https://www.microsoft.com/fr-fr/security/security-insider/emerging-threats/iran-responsible-for-charlie-hebdo-attacks
[108] U. D. o. t. T. O. o. F. A. Control, « Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election,» 28 11 2021. [En ligne].
Available: https://home.treasury.gov/news/press-releases/jy0494
[109] C. Point, «Spotlight on Iranian Cyber Group Emennet Pasargad's Malware,» 14 11 2024. [En ligne].
Available: https://blog.checkpoint.com/research/spotlight-on-iranian-cyber-group-emennet-pasargads-malware/
[110] CISA, « Joint Statement from CISA, FBI, DC3 and NSA on Potential Targeted Cyber Activity Against U.S. Critical Infrastructure by Iran,» 30 06 2025. [En ligne].
Available: https://www.cisa.gov/news-events/news/joint-statement-cisa-fbi-dc3-and-nsa-potential-targeted-cyber-activity-against-us-critical
[111] CISA, «Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations,» 28 08 2025. [En ligne].
Available: https://www.cisa.gov/sites/default/files/2024-08/aa24-241a-iran-based-cyber-actors-enabling-ransomware-attacks-on-us-organizations_0.pdf
[112] R. Future, « North Korea's Cyber Strategy,» 23 06 2023. [En ligne].
Available: https://www.recordedfuture.com/research/north-koreas-cyber-strategy
[113] CISA, « Guidance on the North Korean Cyber Threat,» 23 06 2020. [En ligne].
Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a
[114] TheGuardian, «Cyber-attacks by North Korea raked in $3bn to build nuclear weapons, UN monitors suspect,» 08 02 2024. [En ligne].
Available: https://www.theguardian.com/world/2024/feb/08/cyber-attacks-by-north-korea-raked-in-3bn-to-build-nuclear-weapons-un-monitors-suspect
[115] Elliptic, «$235 million lost by WazirX in North Korea-linked breach,» 18 06 2024. [En ligne].
Available: https://www.elliptic.co/blog/235-million-lost-by-wazirx-in-north-korea-linked-breach
[116] TRM, «The Bybit Hack: Following North Korea's Largest Exploit,» 26 02 2025. [En ligne].
Available: https://www.trmlabs.com/resources/blog/the-bybit-hack-following-north-koreas-largest-exploit
[117] O. o. P. A. U.S, « Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes,» 30 06 2025. [En ligne].
Available: https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote
[118] BBC, «Amazon blocks 1,800 job applications from suspected North Korean agents,» 23 12 2025. [En ligne].
Available: https://www.bbc.com/news/articles/c3e0kw80wwzo
[119] Microsoft, « Jasper Sleet: North Korean remote IT workers' evolving tactics to infiltrate organizations,» 30 06 2025. [En ligne].
Available: https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/
[120] SentinelOne, «Contagious Interview | North Korean Threat Actors Reveal Plans and Ops by Abusing Cyber Intel Platforms,» 04 09 2025. [En ligne].
Available: https://www.sentinelone.com/labs/contagious-interview-threat-actors-scout-cyber-intel-platforms-reveal-plans-and-ops/
[121] T. H. News, «North Korean Threat Actors Deploy COVERTCATCH Malware via LinkedIn Job Scams,» 07 09 2024. [En ligne].
Available: https://thehackernews.com/2024/09/north-korean-threat-actors-deploy.html
[122] Google, «DPRK Adopts EtherHiding: Nation-State Malware Hiding on Blockchains,» 16 10 2025. [En ligne].
Available: https://cloud.google.com/blog/topics/threat-intelligence/dprk-adopts-etherhiding
[123] Aikido, «Malware hiding in plain sight: Spying on North Korean Hackers,» 31 03 2025. [En ligne].
Available: https://www.aikido.dev/blog/malware-hiding-in-plain-sight-spying-on-north-korean-hackers
[124] Socket, «Inside the GitHub Infrastructure Powering North Korea's Contagious Interview npm Attacks,» 2025, 26 11. [En ligne].
Available: https://socket.dev/blog/north-korea-contagious-interview-npm-attacks
[125] Socket, «Another Wave: North Korean Contagious Interview Campaign Drops 35 New Malicious npm Packages,» 25 06 2025. [En ligne].
Available: https://socket.dev/blog/north-korean-contagious-interview-campaign-drops-35-new-malicious-npm-packages
[126] Symantec, «North Korean Lazarus Group Now Working With Medusa Ransomware,» 24 02 2026. [En ligne].
Available: https://www.security.com/threat-intelligence/lazarus-medusa-ransomware
[127] R. Future, «PurpleBravo's Targeting of the IT Software Supply Chain,» 21 01 2026. [En ligne].
Available: https://www.recordedfuture.com/research/purplebravos-targeting-it-software-supply-chain
[128] Google, «Ransomware Under Pressure: Tactics, Techniques, and Procedures in a Shifting Threat Landscape,» 16 03 2026. [En ligne].
Available: https://cloud.google.com/blog/topics/threat-intelligence/ransomware-ttps-shifting-threat-landscape
[129] S. Push, «Silent Push Identifies More Than 10,000 Infected IPs as Part of SystemBC Botnet Malware Family,» 04 02 2026. [En ligne].
Available: https://www.silentpush.com/blog/systembc/
[130] T. R. Media, «Ransomware gangs advancing Moscow's geopolitical aims, Romanian cyber chief warns,» 23 02 2026. [En ligne].
Available: https://therecord.media/ransomware-gangs-advancing-moscow-geopolitical-interests-warns-romania
[131] CheckPoint, «"Handala Hack" – Unveiling Group's Modus Operandi,» 12 03 2026. [En ligne].
Available: https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/
[132] Rapid7, «Muddying the Tracks: The State-Sponsored Shadow Behind Chaos Ransomware,» 06 05 2026. [En ligne].
Available: https://www.rapid7.com/blog/post/tr-muddying-tracks-state-sponsored-shadow-behind-chaos-ransomware/.

[133] Symantec, «North Korean Lazarus Group Now Working With Medusa Ransomware,» 24 02 2026. [En ligne]. Available: https://www.security.com/threat-intelligence/lazarus-medusa-ransomware
[134] BleepingComputer, «North Korean Lazarus group linked to Medusa ransomware attacks,» 24 02 2026. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/north-korean-lazarus-group-linked-to-medusa-ransomware-attacks/
[135] CERT-XMCO, «BILAN DES ACTIVITÉS 2024,» 03 02 2025. [En ligne]. Available: https://19998389.fs1.hubspotusercontent-na1.net/hubfs/19998389/2025-02_YUNO_bilan_2024-1.pdf
[136] Reliaquest, «Is Zendesk Scattered Lapsus$ Hunters' Latest Campaign Target?,» 26 11 2025. [En ligne]. Available: https://reliaquest.com/blog/zendesk-scattered-lapsus-hunters-latest-target/
[137] B. Computer, «Salesforce investigates customer data theft via Gainsight breach,» 20 11 2025. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/salesforce-investigates-customer-data-theft-via-gainsight-breach/
[138] LevelBlue, «Scattered LAPSUS$ Hunters: Anatomy of a Federated Cybercriminal Brand,» 04 11 2025. [En ligne]. Available: https://www.levelblue.com/blogs/spiderlabs-blog/scattered-lapsuss-hunters-anatomy-of-a-federated-cybercriminal-brand
[139] Aqua, «Update: Ongoing Investigation and Continued Remediation,» 01 04 2026. [En ligne]. Available: https://www.aquasec.com/blog/trivy-supply-chain-attack-what-you-need-to-know/
[140] Aikido, «Popular telnyx package compromised on PyPI by TeamPCP,» 27 03 2026. [En ligne]. Available: https://www.aikido.dev/blog/telnyx-pypi-compromised-teampcp-canisterworm
[141] EndorLabs, «TeamPCP Isn't Done: Threat Actor Behind Trivy and KICS Compromises Now Hits LiteLLM's 95 Million Monthly Downloads on PyPI,» 24 03 2026. [En ligne]. Available: https://www.endorlabs.com/learn/teampcp-isnt-done
[142] OpenSourceMalware, «TeamPCP Supply Chain Campaign: A March 2026 Retrospective,» 26 03 2026. [En ligne]. Available: https://opensourcemalware.com/blog/teampcp-supply-chain-campaign
[143] D. Spiegel, «Wie ein mutmaßlicher Erpresserboss aus Russland der Justiz entkam,» 01 03 2025. [En ligne]. Available: https://www.spiegel.de/netzwelt/web/ransomware-gruppe-black-basta-wie-ein-mutmasslicher-erpresser-aus-russland-der-justiz-entkam-a-df47e7f1-69de-4d60-bc34-af22e6e8fc05
[144] ESET, « First known AI-powered ransomware uncovered by ESET Research,» 26 08 2025. [En ligne]. Available: https://www.welivesecurity.com/en/ransomware/first-known-ai-powered-ransomware-uncovered-eset-research/
[145] XMCO, «ActuSécu n°62,» 2025. [En ligne]. Available: https://content.xmco.fr/actusecu-62
[146] T. Guardian, «Sinaloa cartel hacked security cameras to track and kill FBI informants, US says,» 28 06 2025. [En ligne]. Available: https://www.theguardian.com/world/2025/jun/27/sinaloa-cartel-fbi-hackers
[147] Europol, «The changing DNA of serious and organised crime,» 27 05 2025. [En ligne]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
[148] Europol, «Steal, deal and repeat: How cybercriminals trade and exploit your data,» 12 06 2025. [En ligne]. Available: https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data
[149] T. Record, «Ransomware gangs advancing Moscow's geopolitical aims, Romanian cyber chief warns,» 23 02 2026. [En ligne]. Available: https://therecord.media/ransomware-gangs-advancing-moscow-geopolitical-interests-warns-romania
[150] DomainTools, «The APT35 Dump Episode 4: Leaking The Backstage Pass To An Iranian Intelligence Operation,» 16 12 2025. [En ligne]. Available: https://dti.domaintools.com/the-apt35-dump-episode-4-leaking-the-backstage-pass-to-an-iranian-intelligence-operation/
[151] Sophos, «Abraham's Ax Likely Linked to Moses Staff,» 26 01 2023. [En ligne]. Available: https://www.sophos.com/fr-fr/blog/abrahams-ax-likely-linked-to-moses-staff
[152] CheckPoint, «Sicarii Ransomware: Truth vs Myth,» 14 01 2026. [En ligne]. Available: https://research.checkpoint.com/2026/sicarii-ransomware-truth-vs-myth/
[153] Halcyon, «Alert: Sicarii Ransomware Encryption Key Handling Defect,» 23 01 2026. [En ligne]. Available: https://www.halcyon.ai/ransomware-alerts/alert-sicarii-ransomware-encryption-key-handling-defect
[154] Symantec, «North Korean Lazarus Group Now Working With Medusa Ransomware,» 24 02 2026. [En ligne]. Available: https://www.security.com/threat-intelligence/lazarus-medusa-ransomware
[155] LeMonde, «French researcher freed from Russian jail arrives home after prisoner swap,» 08 01 2026. [En ligne]. Available: https://www.lemonde.fr/en/international/article/2026/01/08/french-researcher-freed-from-russian-jail-arrives-home-after-prisoner-swap_6749213_4.html
[156] BleepingComputer, «Black Basta boss makes it onto Interpol's 'Red Notice' list,» 16 01 2026. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/black-basta-boss-makes-it-onto-interpols-red-notice-list/
[157] ESET, « DynoWiper update: Technical analysis and attribution,» 30 01 2026. [En ligne]. Available: https://www.welivesecurity.com/en/eset-research/dynowiper-update-technical-analysis-attribution/
[158] ESET, « ESET Research: Sandworm behind cyberattack on Poland's power grid in late 2025,» 23 01 2026. [En ligne]. Available: https://www.welivesecurity.com/en/eset-research/eset-research-sandworm-cyberattack-poland-power-grid-late-2025/
[159] Twitter/X, «The operators of RaaS BQTlock are offering it for free for those hacktivists willing to use it to target Israel networks,» 27 01 2026. [En ligne]. Available: https://x.com/Cyberknow20/status/2016104925239865699
[160] L. M. Informatique, «Transfert de fichiers Cleo: le groupe de ransomware Clop à la manoeuvre,» 17 12 2024. [En ligne]. Available: https://www.lemondeinformatique.fr/actualites/lire-transfert-de-fichiers-cleo-le-groupe-de-ransomware-clop-a-la-manoeuvre-95560.html
[161] 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/
[162] FranceInfo, « Lycées paralysés, mairies visées... On vous présente Qilin Ransomware, à l'origine de nombreuses cyberattaques en France et dans le monde,» 22 10 2025. Available: https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/lycees-paralyses-mairies-visees-on-vous-presente-qilin-ransomware-a-l-origine-de-nombreuses-cyberattaques-en-france-et-dans-le-monde_7564588.html
[163] Trellix, «Analysis of Black Basta Ransomware Chat Leaks,» 18 03 2025. [En ligne]. Available: https://www.trellix.com/blogs/research/analysis-of-black-basta-ransomware-chat-leaks/
[164] LevelBlue, «A Deep Dive into the Leaked Black Basta Chat Logs,» 14 04 2025. [En ligne]. Available: https://www.levelblue.com/resources/research-reports/a-deep-dive-into-the-leaked-black-basta-chat-logs/

[165] LeMagIt, «Ransomware : de REvil à Black Basta, que sait-on de Tramp ?,» 01 03 2025. [En ligne].
Available: https://www.lemagit.fr/actualites/366619807/Ransomware-de-REvil-a-Black-Basta-que-sait-on-de-Tramp
[166] Symantec, «Reynolds: Defense Evasion Capability Embedded in Ransomware Payload,» 05 02 2026. [En ligne].
Available: https://www.security.com/threat-intelligence/black-basta-ransomware-byovd
[167] Spiegel, «Wie ein mutmaßlicher Erpresserboss aus Russland der Justiz entkam,» 01 03 2025. [En ligne].
Available: https://www.spiegel.de/netzwelt/web/ransomware-gruppe-black-basta-wie-ein-mutmasslicher-erpresser-aus-russland-der-justiz-entkam-a-df47e7f1-69de-4d60-bc34-af22e6e8fc05.
[168] BleepingComputer, «Black Basta boss makes it onto Interpol's 'Red Notice' list,» 16 01 2026. [En ligne].
Available: https://www.bleepingcomputer.com/news/security/black-basta-boss-makes-it-onto-interpols-red-notice-list/
[169] ArcticWolf, «Russian RomCom Utilizing SocGholish to Deliver Mythic Agent to U.S. Companies Supporting Ukraine,» 25 11 2025. [En ligne].
Available: https://arcticwolf.com/resources/blog/romcom-utilizing-socgholish-to-deliver-mythic-agent-to-usa-companies-supporting-ukraine/
[170] Prodaft, «Inside the Latest Espionage Campaign of Nebulous Mantis,» 25 04 2025. [En ligne].
Available: https://catalyst.prodaft.com/public/report/inside-the-latest-espionage-campaign-of-nebulous-mantis/overview#heading-1000|0
[171] AttackIQ, «The Evolution of RomCom: From Backdoor to Cyberwar,» 23 09 2025. [En ligne].
Available: https://www.attackiq.com/2025/09/23/evolution-of-romcom/
[172] ESET, « Update WinRAR tools now: RomCom and others exploiting zero-day vulnerability,» 11 08 2025. [En ligne].
Available: https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/
[173] SecurityAffairs, «Qilin Ransomware gang claims the hack of the Ministry of Foreign Affairs of Ukraine,» 07 03 2025. [En ligne].
Available: https://securityaffairs.com/175025/cyber-crime/qilin-ransomware-ministry-of-foreign-affairs-of-ukraine.html
[174] M. T. Intelligence, «Since late February 2025, Microsoft has observed Moonstone Sleet, a North Korean state actor, deploying Qilin ransomware at a limited number of orgs,» 06 03 2025. [En ligne].
Available: https://x.com/MsftSecIntel/status/1897738961348374621
[175] T. Micro, «Warlock: From SharePoint Vulnerability Exploit to Enterprise Ransomware,» 20 08 2025. [En ligne].
Available: https://www.trendmicro.com/ru_ru/research/25/h/warlock-ransomware.html
[176] Sophos, «GOLD SALEM tradecraft for deploying Warlock ransomware,» 11 12 2025. [En ligne].
Available: https://www.sophos.com/fr-fr/blog/gold-salem-tradecraft-for-deploying-warlock-ransomware
[177] Reliaquest, «Storm-2603 Exploits CVE-2026-23760 to Stage Warlock Ransomware,» 09 02 2026. [En ligne].
Available: https://reliaquest.com/blog/threat-spotlight-storm-2603-exploits-CVE-2026-23760-to-stage-warlock-ransomware/
[178] B. Computer, «Hackers breach SmarterTools network using flaw in its own software,» 09 02 2026. [En ligne].
Available: https://www.bleepingcomputer.com/news/security/hackers-breach-smartertools-network-using-flaw-in-its-own-software/
[179] Morphisec, « Pay2Key's Resurgence: Iranian Cyber Warfare Targets the West,» 08 07 2025. [En ligne].
Available: https://www.morphisec.com/blog/pay2key-resurgence-iranian-cyber-warfare/
[180] Microsoft, «Since late February 2025, Microsoft has observed Moonstone Sleet, a North Korean state actor, deploying Qilin ransomware at a limited number of orgs.,» 06 03 2025. [En ligne].
Available: https://x.com/MsftSecIntel/status/1897738961348374621
[181] Bitdefender, « The Korean Leaks – Analyzing the Hybrid Geopolitical Campaign Targeting South Korean Financial Services With Qilin RaaS,» 24 11 2025. [En ligne].
Available: https://www.bitdefender.com/en-us/blog/businessinsights/korean-leaks-campaign-targets-south-korean-financial-services-qilin-ransomware
[182] T. H. News, «Qilin Ransomware Turns South Korean MSP Breach Into 28-Victim 'Korean Leaks' Data Heist,» 26 11 2025. [En ligne].
Available: https://thehackernews.com/2025/11/qilin-ransomware-turns-south-korean-msp.html
[183] Microsoft, « Moonstone Sleet emerges as new North Korean threat actor with new bag of tricks,» 28 05 2024. [En ligne].
Available: https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/
[184] S2W, « ScarCruft's New Language: Whispering in PubNub, Crafting Backdoor in Rust, Striking with Ransomware,» 07 08 2025. [En ligne].
Available: https://s2w.inc/en/resource/detail/899
[185] SentinelOne, «Comrades in Arms? | North Korea Compromises Sanctioned Russian Missile Engineering Company,» 07 08 2023. [En ligne].
Available: https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/
[186] D. C. Blog, «To Russia With Love: Assessing a KONNI-Backdoored Suspected Russian Consular Software Installer,» 21 02 2024. [En ligne].
Available: https://medium.com/@DCSO_CyTec/to-russia-with-love-assessing-a-konni-backdoored-suspected-russian-consular-software-installer-ce618ea4b8f3
[187] 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
[188] 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
[189] 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/
[190] Symantec, «Fog Ransomware: Unusual Toolset Used in Recent Attack,» 12 06 2025. [En ligne].
Available: https://www.security.com/threat-intelligence/fog-ransomware-attack
[191] 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
[192] Ransomwarelive, «Ransomwarelive,» 10 04 2025. [En ligne].
Available: https://www.ransomware.live/id/SGFydmVzdEBSdW5Tb21IV2FyZXM=
[193] Group-IB, «Ransomware debris: an analysis of the RansomHub operation,» 30 04 2025. [En ligne].
Available: https://www.group-ib.com/blog/ransomware-debris/
[194] 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
[195] 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/
[196] 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.

[197] 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/
[198] 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/
[199] H. T. A. A. E. o. S. VPNs, «Huntress,» 13 08 2025. [En ligne]. Available: https://www.huntress.com/blog/exploitation-of-sonicwall-vpn
[200] 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/
[201] 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/
[202] 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/
[203] 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
[204] 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
[205] Resecurity, «ShinyHunters Launches Data Leak Site: Trinity of Chaos Announces New Ransomware Victims,» 03 10 2025. [En ligne]. Available: https://www.resecurity.com/es/blog/article/shinyhunters-launches-data-leak-site-trinity-of-chaos-announces-new-ransomware-victims
[206] FalconFeeds.io, «The Emergence of "Scattered LAPSUS$ Hunters": An Investigative Timeline of Leaks and Chaos,» 12 08 2025. [En ligne]. Available: https://falconfeeds.io/blogs/scattered-lapsus-hunters-investigative-timeline
[207] B. Computer, «Meet ShinySp1d3r: New Ransomware-as-a-Service created by ShinyHunters,» 19 11 2025. [En ligne]. Available: https://www.bleepingcomputer.com/news/security/meet-shinysp1d3r-new-ransomware-as-a-service-created-by-shinyhunters/
[208] 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
[209] 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/
[210] 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/
[211] 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
[212] 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/
[213] 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/
[214] 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
[215] 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/
[216] 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
[217] 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/
[218] 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/
[219] Halcyon, «INC Ransom,» 01 07 2023. [En ligne]. Available: https://www.halcyon.ai/threat-group/inc-ransom
[220] Fortinet, «Inc Ransomware,» 01 04 2026. [En ligne]. Available: https://www.fortiguard.com/threat-actor/6333/inc-ransomware
[221] RansomwareLive, «cryopur.com,» 25 11 2025. [En ligne]. Available: https://www.ransomware.live/id/Y3J5b3B1ci5jb21AaW5jcmFuc29t.
[222] RansomwareLive, «Afpa,» 06 08 2025. [En ligne]. Available: https://www.ransomware.live/id/QWZwYUBpbmNyYW5zb20=
[223] RansomwareLive, «Mission Locale Montpellier,» 29 01 2025. [En ligne]. Available: https://www.ransomware.live/id/TWIzc2IvbiBMb2NhbGUgTW9udHBlbGxpZXJAaW5jcmFuc29t
[224] RansomwareLive, «abeyor.fr,» 15 03 2025. [En ligne]. Available: https://www.ransomware.live/id/YWJleW9yLmZyQGluY3JhbnNvbQ==
[225] RansomwareLive, «alleray-labrouste,» 12 06 2025. [En ligne]. Available: https://www.ransomware.live/id/YWxsZXJheS1sYWJyb3VzdGVAaW5jcmFuc29t
[226] 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/
[227] 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/
[228] CERT-XMCO, «Une vision globale de la veille cyber.,» 24 04 2026. [En ligne]. Available: https://www.xmco.fr/cybersecurite/veille-en-vulnerabilites-yuno
[229] CERT-XMCO, «Je dois surveiller mon exposition numérique sur internet (Clear, Deep et Dark web),» 24 04 2026. [En ligne]. Available: https://www.xmco.fr/xperience/surveiller

[230] LeMagIt, «Ransomware : Colonial Pipeline, la cyberattaque de trop ?,» 17 05 2021. [En ligne].
Available: https://www.lemagit.fr/actualites/252500851/Ransomware-Colonial-Pipeline-la-cyberattaque-de-trop
[231] T. W. S. Journal, «Russia Arrests Hackers Tied to Major U.S. Ransomware Attacks, Including Colonial Pipeline Disruption,» 14 01 2022. [En ligne].
Available: https://www.wsj.com/tech/cybersecurity/russia-says-it-raided-prolific-ransomware-group-revil-with-arrests-seizures-11642179589
[232] BBC, «REvil ransomware gang arrested in Russia,» 14 01 2022. [En ligne].
Available: https://www.bbc.com/news/technology-59998925

Déployez votre veille en une heure avec yuno

By xmco

- **TYPE DE VEILLE**
  Couverture complète : bulletins de sécurité, menaces et incidents, actualités, ransomware, IOC, catalogue KEV et veille sectorielle
- **PERSONNALISATION DE LA VEILLE**
  Personnalisation granulaire selon vos technologies, vos niveaux de criticité et vos destinataires
- **INDÉPENDANCE DES SOURCES**
  Production Yuno alimentée directement par les bulletins éditeurs, collectés via des scrapers propriétaires.
  Enrichissement complémentaire à partir de sources institutionnelles.
- **QUALITÉ DE L'ANALYSE**
  Chaque vulnérabilité est consolidée, replacée dans son contexte et synthétisée pour une lecture immédiate
- **GESTION DU BRUIT**
  Synthèse quotidienne permettant une prise de connaissance complète en moins de 5 minutes
- **RÉACTIVITÉ ET ACTIONNABILITÉ**
  Informations disponibles dès J+1, priorisées et immédiatement exploitables
- **PILOTAGE & SUIVI**
  Tableaux de bord intégrés pour le pilotage et le suivi de la remédiation
- **INTÉGRATION / CONNECTEURS**
  API disponible pour une intégration flexible dans votre système d'information existant
- **DÉPLOIEMENT**
  Opérationnel en 1 heure, pas d'installation requise, simple paramétrage de la plateforme SaaS

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.

UGAP C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière cert by xmco ANSSI qsa

Renseignement :

info@xmco.fr

01 79 35 29 30

www.xmco.fr