

INTRINSEC

Innovative by design

Analyse stratégique

Défense

Cyber Threat Intelligence

6 novembre 2026

@Intrinsec @Intrinsec Blog Website

2026 Intrinsec, Inc. All rights reserved.

Table des matières

Table des matières 2
Synthèse exécutive 3
Points clefs 4
Bonnes pratiques 5
Focus sur les ransomware 6
Répartition par groupe 7
Répartition par pays 8
Cartographie 9
Tableau des ransomware 11
Focus sur les forums 14
Répartition par pays 14
Répartition par secteur 15
Répartition par type 16
Focus sur DDOSIA 17
Analyse tactique 18
MioLab Stealer : Un réseau de diffusion via 448 sites GitHub Pages ciblant les utilisateurs de macOS 18

Synthèse exécutive

Le secteur de la défense fait face à une recrudescence de cybermenaces ciblant ses infrastructures critiques, exploitant des vulnérabilités critiques telles que **PHP2Shell** (CVE-2026-109618[1] et CVE-2026-109619[2]). Ces failles, exploitées en moins de deux heures par des acteurs malveillants, ont permis l'accès à des secrets d'authentification multifactorielle et à des hachages de mots de passe, illustrant une sophistication accrue des attaques. Les **groupes étatiques**, notamment liés à l'écosystème **Lazarus**, utilisent des plateformes d'intelligence artificielle pour **automatiser leurs opérations**, contournant les outils de détection traditionnels et ciblant des entités stratégiques en Amérique du Nord, en Asie et en Europe. Cette campagne, coordonnée via des canaux fermés comme I2P, souligne la nécessité d'une vigilance renforcée face à des opérateurs autonomes capables d'exécuter des attaques en un temps record.

Parallèlement, le secteur de la défense est directement impacté par les activités des groupes de **ransomware**, avec quatorze incidents recensés durant la période analysée. Les États-Unis, le Royaume-Uni et plusieurs pays européens figurent parmi les cibles privilégiées, avec des acteurs comme **Booba Project**, **The Gentlemen** et **Rhysida** menant des attaques contre des entités **militaires** et **gouvernementales**. La démocratisation des kits d'exploitation PHP2Shell sur les forums cybercriminels aggrave cette menace, exposant davantage les organisations à des campagnes de grande envergure. Les infrastructures critiques, y compris celles des acteurs majeurs comme **Airbus**, **Dassault** ou **Thales**, doivent ainsi renforcer leurs mesures de sécurité, notamment autour des systèmes d'authentification et des réseaux opérationnels, pour limiter les risques de compromission.

Les attaques par **déni de service distribué** (DDoS), orchestrées par des groupes comme **NoName057(16)**, ajoutent une couche supplémentaire de complexité, visant des entités telles que **Sagem**, **Eurenco**, le **GICAT**, ou **MESIT holding** pour des **motifs géopolitiques**. Ces dynamiques soulignent l'urgence d'adopter des stratégies de défense adaptées, intégrant une surveillance accrue des forums cybercriminels et une collaboration renforcée entre acteurs publics et privés.

[1] https://nvd.nist.gov/vuln/detail/CVE-2026-109618

[2] https://nvd.nist.gov/vuln/detail/CVE-2026-109619

Points clefs

Les récentes campagnes d'exploitation des vulnérabilités PHP2Shell (CVE-2026-109618[3] et CVE-2026-109619[4]) illustrent une tendance préoccupante pour le secteur de la défense, où des acteurs malveillants, notamment liés à la Corée du Nord, ciblent activement les infrastructures critiques. Selon les rapports de Palo Alto Networks Unit 42 et CYFIRMA, ces vulnérabilités permettent une exécution de code à distance non authentifiée, offrant aux attaquants un accès privilégié aux systèmes compromis. Dans un cas documenté, un acteur a exploité ces failles pour accéder aux hachages de mots de passe et aux secrets d'authentification multifactorielle (MFA) d'une entité gouvernementale européenne en moins de deux heures après l'exploitation initiale. Cette rapidité d'action souligne l'importance d'une détection et d'une réponse immédiates, car les routines traditionnelles de remédiation et de chasse aux menaces, souvent étalées sur plusieurs jours, peuvent échouer à contrer des attaques exécutées par des opérateurs autonomes en un temps record.

Les acteurs associés à l'écosystème Lazarus Group, identifiés avec une confiance modérée grâce à des chevauchements de pseudonymes et des indicateurs linguistiques, ont ciblé un ensemble de 216 hôtes non patchés ou partiellement atténués, répartis aux États-Unis, au Japon, en Corée du Sud, en Thaïlande, en Indonésie, en Australie, à Taïwan, en Inde, à Singapour, aux Émirats arabes unis, en Arabie saoudite et dans l'Union européenne. Cette campagne, coordonnée via un canal I2P fermé, met en lumière une stratégie de reconnaissance ciblée visant des secteurs critiques, notamment les infrastructures gouvernementales et industrielles. Parallèlement, l'émergence d'un outil de reconnaissance PHP2Shell sur un forum imitant le rebranding de XSS démontre que ces activités de scanning s'étendent désormais au-delà des groupes parrainés par des États, infiltrant les canaux du cybercrime généraliste.

Enfin, l'incident impliquant LiteLLM, où une clé maître divulguée a permis à un attaquant de voler des jetons GitHub et de détourner un pipeline de release, met en exergue les risques

[3] https://nvd.nist.gov/vuln/detail/CVE-2026-109618

[4] https://nvd.nist.gov/vuln/detail/CVE-2026-109619

liés à la gestion des identités et des accès dans les environnements DevOps. Pour des entreprises comme Dassault Aviation, dont les chaînes d'approvisionnement logicielles et les processus de développement reposent sur des outils similaires, cet incident souligne l'importance de politiques strictes de rotation des secrets et de segmentation des accès. Les workflows malveillants ciblant les clés d'inférence API, comme observé dans cet incident, montrent que les outils d'orchestration d'agents doivent être traités avec la même rigueur que les matériaux de signature de code, afin de prévenir des compromissions similaires.

Bonnes pratiques

• Appliquer immédiatement les correctifs pour les vulnérabilités PHP2Shell (CVE-2026-109618[5], CVE-2026-109619[6]) sur tous les serveurs PHP exposés à Internet, en priorisant les versions 8.2 à 8.5, et désactiver la fonctionnalité session.upload_progress jusqu'à la mise à jour complète.

• Renforcer les contrôles d'accès et la surveillance des appliances VPN et pare-feu exposées, notamment Ivanti Connect Secure, Fortinet FortiGate et Palo Alto GlobalProtect, en appliquant les correctifs disponibles et en réinitialisant les identifiants stockés ou utilisés via ces dispositifs.

• Déployer des mécanismes d'authentification résistants au phishing, tels que les clés de sécurité matérielles ou les passkeys, pour les comptes d'administration et les services critiques, afin de contrer les attaques par usurpation d'identité et les techniques adversary-in-the-middle (AiTM).

• Isoler les environnements de développement et de production des modèles d'IA, en désactivant l'accès Internet direct pour les modèles en phase d'entraînement et en appliquant des politiques de moindre privilège pour les agents autonomes afin de prévenir les fuites de données et les attaques par exfiltration.

• Auditer et surveiller en continu les configurations des services cloud et des plateformes SaaS, en particulier les autorisations accordées aux applications tierces et les clés API

[5] https://nvd.nist.gov/vuln/detail/CVE-2026-109618

[6] https://nvd.nist.gov/vuln/detail/CVE-2026-109619

exposées, pour détecter et remédier aux accès non autorisés ou aux fuites de données via des comptes compromis ou des vulnérabilités de configuration.

Focus sur les ransomware

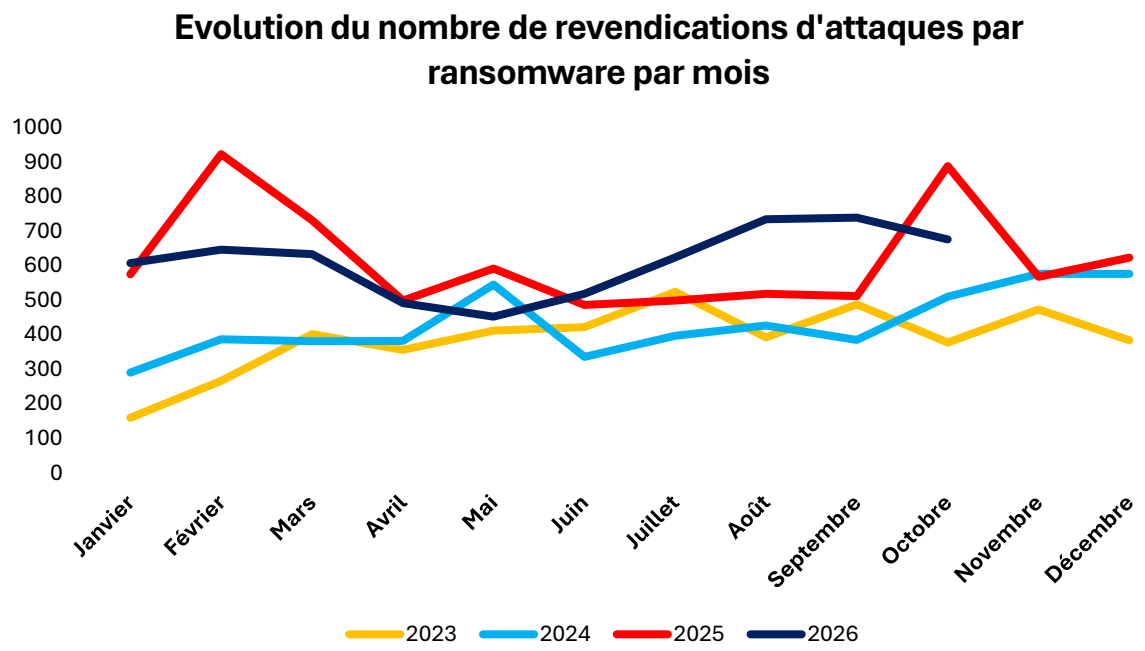
Cette section offre une vue d'ensemble des activités des groupes de ransomware, en soulignant les cibles et l'étendue géographique des attaques. Elle met en lumière les principaux acteurs de la menace et permet d'identifier les dynamiques régionales de propagation des ransomware, essentielles pour ajuster les stratégies de défense.

Note : Les noms des acteurs suivent la nomenclature de Flashpoint. Les suffixes de version (par ex. v2, v3, 2.0) peuvent être utilisés pour distinguer des sites de fuite successifs ou différentes itérations d'une même opération et ne désignent pas nécessairement un acteur ou un ransomware distinct.

Durant la période étudiée dans cette analyse, 677 victimes ont pu être mises en évidence. Le secteur de la Défense a été visé 14 fois. Les trois secteurs les plus impactés sont INDUSTRIEL (158), MANUFACTURIER (158) et SANTE (141).

Les pays les plus impactés sont: États-Unis (311), Allemagne (31) et Canada (27).

En ce qui concerne les modes opératoires les plus actifs dans le domaine de l'écosystème ransomware dans le secteur de la Défense, on peut citer les trois suivants : Booba Project (3), The Gentlemen (2) et Rhysida (2).



Répartition par groupe

Cette sous-section présente une ventilation des activités par mode opératoire d'attaque, en identifiant les collectifs les plus actifs et les plus impactant.

Le graphique ci-dessous montre la répartition des secteurs touchés par les attaques de ransomware au cours de la période couverte par cette analyse.

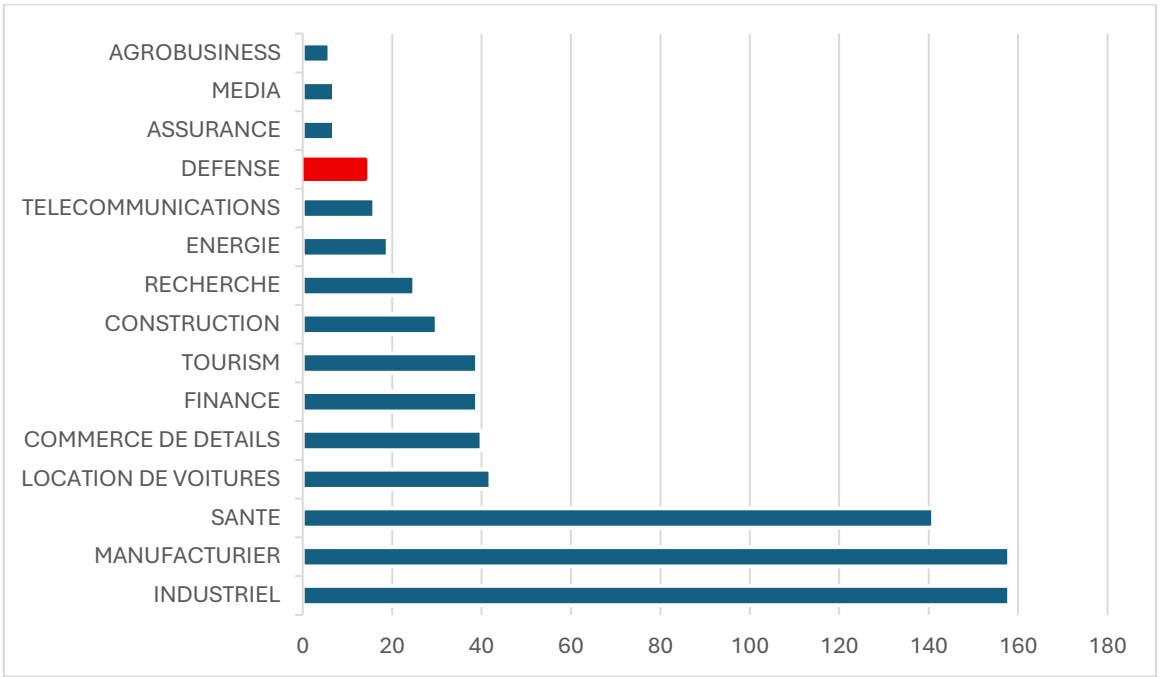


Figure 1 - Répartition des secteurs impactés par les attaques de ransomware (du 01/10/2026 au 31/10/2026).

Le graphique ci-dessous montre les 5 principaux groupes d'intrusion responsables du plus grand nombre de compromissions dans tous les secteurs au cours de la période analysée.

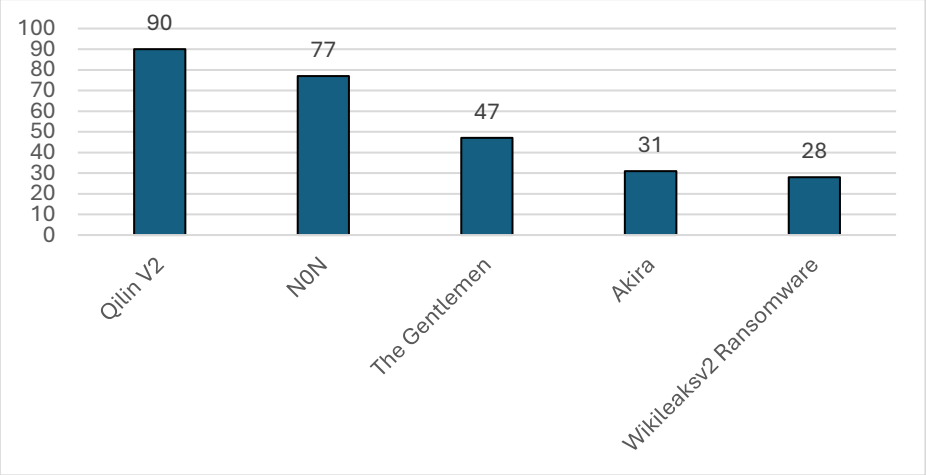


Figure 2 – Top 5 des groups d'intrusion par nombre de victimes (tous secteurs) (du 01/10/2026 au 31/10/2026).

Le graphique ci-dessous présente les 5 principaux groupes d'intrusion ayant fait le plus de victimes dans le secteur analysé au cours de la période étudiée.

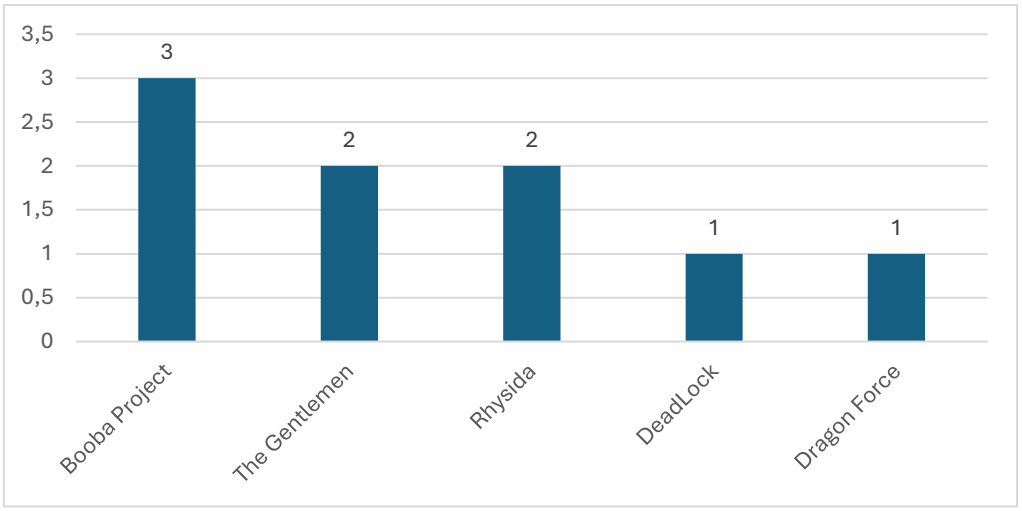


Figure 3 - Top 5 des groupes d'intrusion par nombre de victimes (du 01/10/2026 au 31/10/2026).

Répartition par pays

La répartition par pays met en évidence les zones géographiques les plus touchées par les attaques de ransomware. Elle reflète l'exposition accrue des États-Unis, du Royaume-Uni et

de certains pays européens, soulignant l'internationalisation croissante de ces cybermenaces.

Le graphique ci-dessous montre les 10 pays les plus touchés par les attaques de ransomware au cours de la période analysée, en fonction du nombre d'organisations compromises.

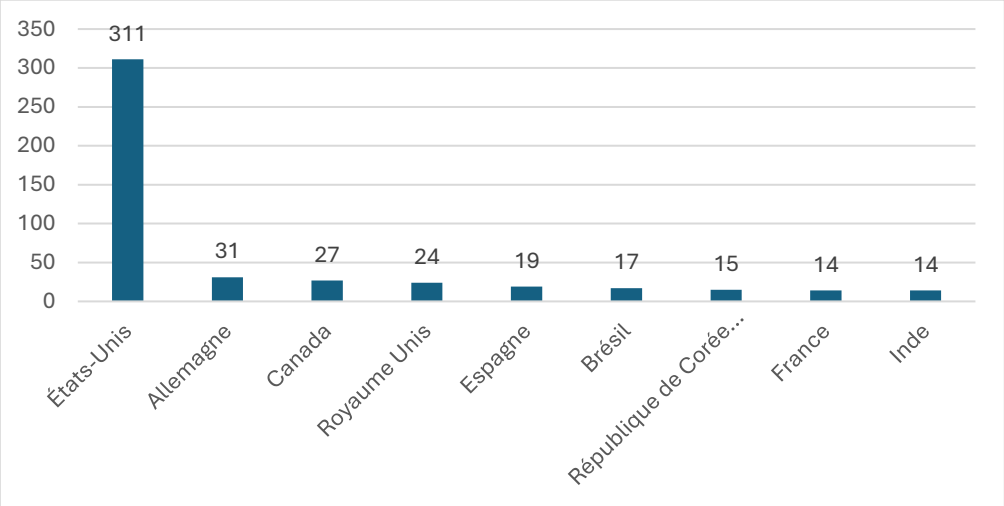


Figure 4 - Top10 des pays les plus touchés par les attaques ransomware (du 01/10/2026 au 31/10/2026).

Cartographie

La cartographie suivante illustre la répartition géographique des attaques par ransomware tous secteurs confondus. Elle met en évidence les pays les plus ciblés par ces cyberattaques à l'échelle internationale.

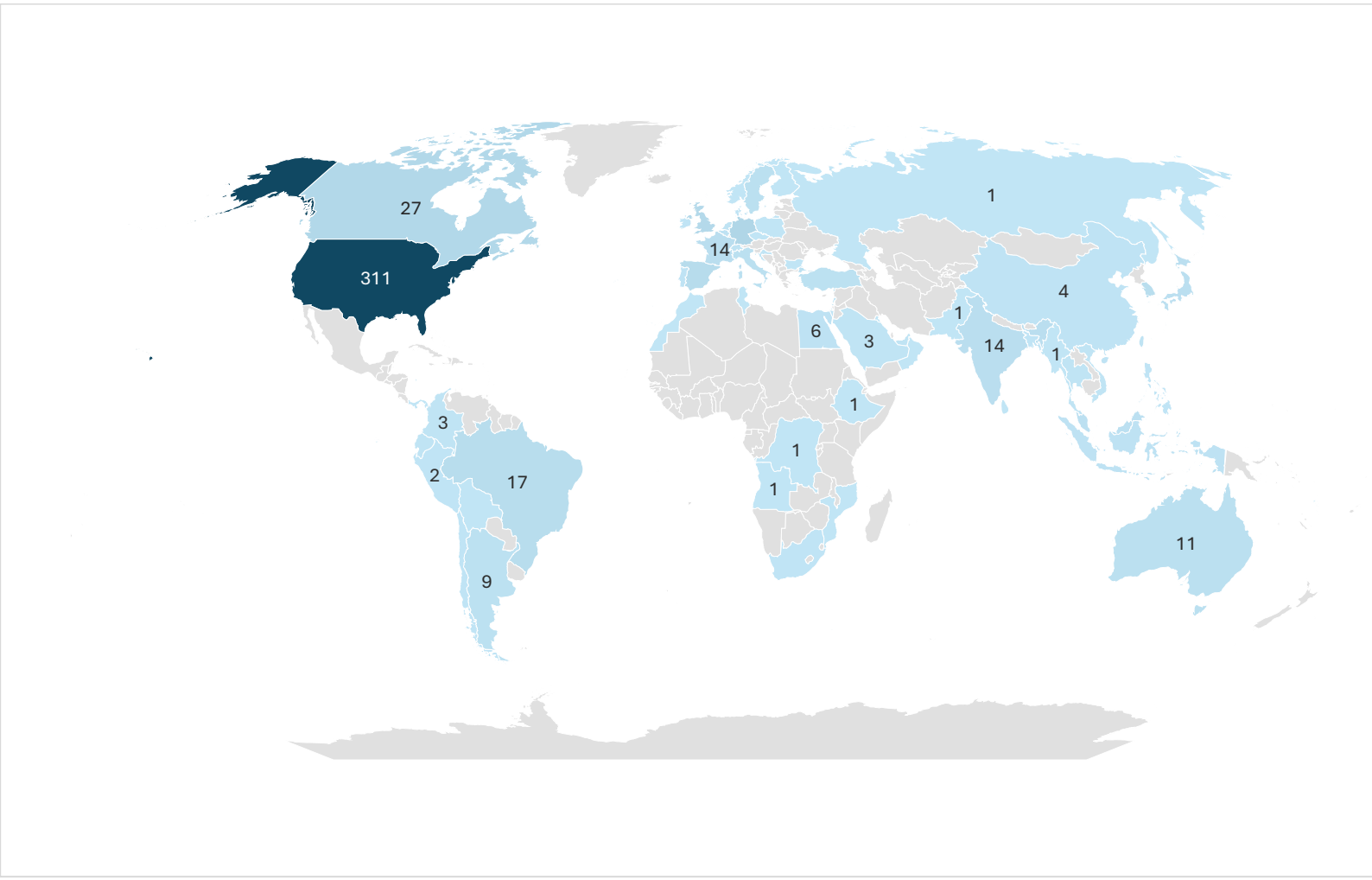


Figure 5 – Zones géographiques touchées par des attaques de ransomware (du 01/10/2026 au 31/10/2026).

Tableau des ransomware

Aucune entité française de votre secteur n'a été compromise par des groupes de ransomware durant la période analysée.

Le tableau suivant dresse la liste des entités compromises à l'international par des groupes de ransomware, à l'exception des victimes françaises, mettant en lumière les tendances sectorielles et géographiques.

Date	Victime	Secteur	Pays	Groupe
2026-10-29	**Circleville Police Department**	Defense Ministries (Including The Military)	États-Unis	Booba Project
2026-10-29	**South Weber City**	Defense Ministries (Including The Military)	États-Unis	Booba Project
2026-10-27	**Bristol City Council**	Défense, Defense Ministries (Including The Military)	Royaume Unis	Wallstreet
2026-10-27	**Gemeente Machelen-Diegem**	Défense, Defense Ministries (Including The Military)	Belgique	Rhysida
2026-10-20	**City Hall - Everett, MA**	Défense, Defense Ministries (Including The Military)	États-Unis	Booba Project
2026-10-17	**Oak Grove Technologies**	Défense, Industrie de la	États-Unis	Dragon Force

		défense, R Défense		
2026-10-13	**Policía Nacional del Ecuador**	Defense Ministries (Including The Military)	Ecuador	Hyflock
2026-10-10	**Royal Thai Air Force**	Défense, Industrie de la défense, R Défense	Thaïlande	The Gentlemen
2026-10-10	**Secretaría de Modernización e Innovación del Municipio de Río Grande**	Défense, Defense Ministries (Including The Military)	Argentine	Qilin V2
2026-10-09	**Anne Arundel County**	Défense, Defense Ministries (Including The Military)	États-Unis	Rhysida
2026-10-07	**Flydubai**	Défense, Industrie de la défense	Émirats arabes unis	everest
2026-10-06	**Skyplan Services**	Défense, Industrie de la défense	Canada	The Gentlemen
2026-10-04	**TGD: Digital Government Platform**	Défense, Defense Ministries (Including The Military)	Argentine	Kazu
2026-10-02	**Far West Contractors**	Défense, R Défense,	États-Unis	DeadLock

Industrie de la défense

Focus sur les forums

Dans cette section, nous présentons une vue d'ensemble des activités de surveillance menées sur les forums cybercriminels durant la période analysée. 52 pays ont été ciblés à travers la vente de bases de données, de documents, de logs, d'offres d'accès initial, etc.

L'analyse repose sur des renseignements collectés à partir de plusieurs plateformes clandestines majeures, notamment DarkForums et Exploit, offrant une vision de l'ampleur et de la répartition géographique des activités malveillantes observées au cours de la période de reporting.

Répartition par pays

La répartition par pays met en évidence les zones géographiques les plus ciblées par les ventes illicites sur les forums cybercriminels.

Le graphique ci-dessous présente les 10 pays les plus touchés durant la période analysée, sur la base du nombre d'annonces liées à la vente de bases de données, de documents, de logs et d'accès initiaux.

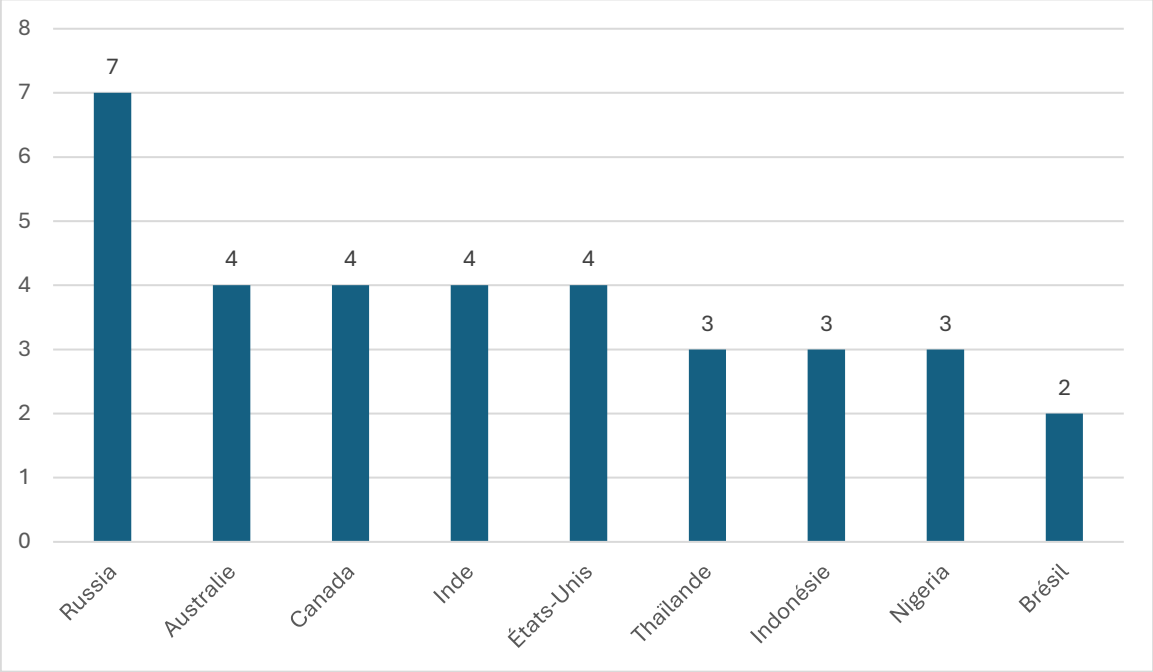


Figure 6 - Top 10 des pays les plus ciblés par les ventes illicites sur les forums cybercriminels (du 01/10/2026 au 31/10/2026).

Répartition par secteur

Le graphique ci-dessous présente la répartition des secteurs touchés par les ventes illicites sur les forums cybercriminels durant la période couverte par cette analyse.

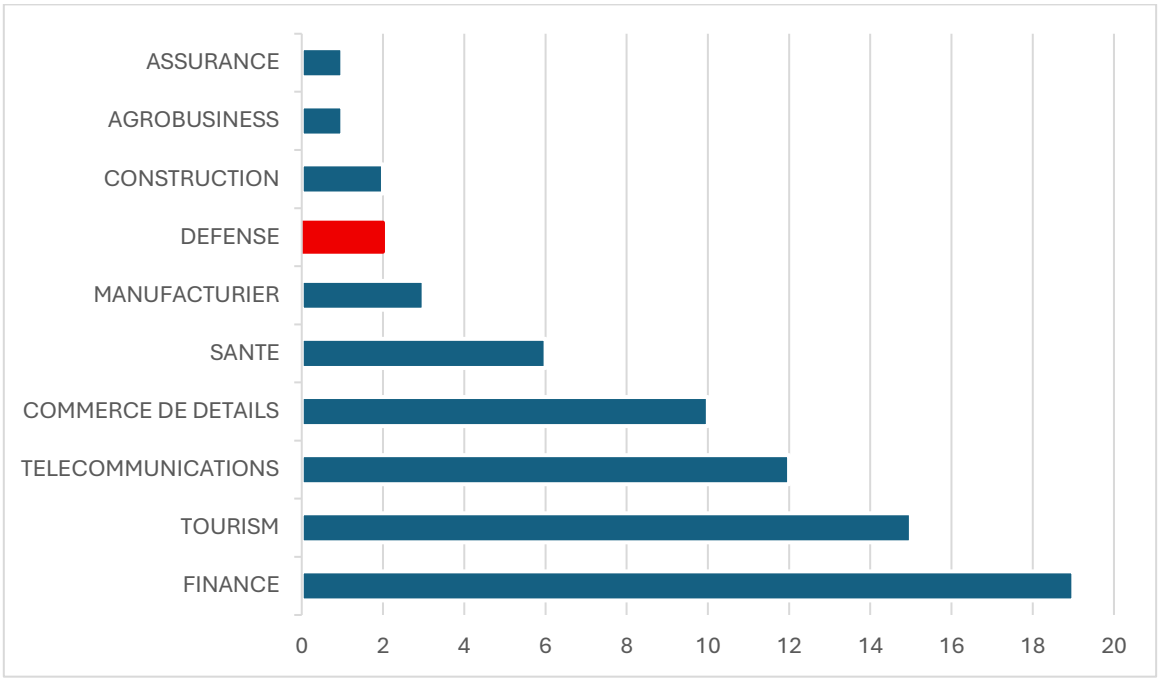


Figure 7 – Répartition des secteurs touchés par les ventes illicites sur les forums cybercriminels (du 01/10/2026 au 31/10/2026).

Répartition par type

Le graphique ci-dessous présente la répartition des types de données vendus sur les forums cybercriminels durant la période couverte par cette analyse.

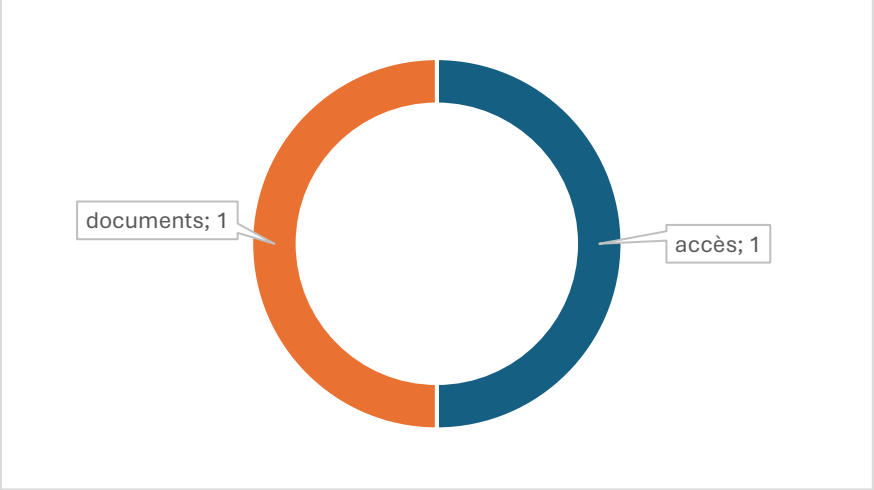


Figure 8 - Répartition des types de données vendus sur les forums cybercriminels (du 01/10/2026 au 31/10/2026).

Focus sur DDOSIA

NoName057(16) est un mode opératoire d'origine russe principalement axé sur l'exploitation des événements géopolitiques pour mener des campagnes de déni de service distribué (DDoS). S'appuyant sur son outil éponyme, DDOSIA, ce collectif coordonne et automatise des attaques visant des organisations, entreprises et institutions perçues comme opposées à ses intérêts ou à ceux de la Russie, dans le cadre d'opérations de perturbation et d'influence dans le cyberespace.

Durant la période analysée, 173 victimes ont été recensées dont 4 pour le secteur concerné. Le tableau ci-dessous recense les entités ciblées par NoName 057 (16) durant la période analysée.

Date	Victime	Secteur	Pays	Groupe
2026-10-21	**Sagem**	Défense	France	NoName 057 (16)
2026-10-13	**GICAT**	Défense	France	NoName 057 (16)
2026-10-13	**Eurenco**	Défense	France	NoName 057 (16)
2026-10-01	**MESIT holding, a.s.**	Défense	Tchéquie	NoName 057 (16)

Analyse tactique

Menées par les experts d'Intrinsec, les analyses tactiques offrent un aperçu unique et actualisé des cybermenaces les plus récentes. Cette section, régulièrement mise à jour, vise à fournir des renseignements opérationnels pertinents pour mieux comprendre les méthodes, infrastructures et campagnes d'attaque actuelles. Chaque analyse s'appuie sur des observations de terrain et des investigations techniques approfondies, contribuant ainsi à améliorer l'anticipation des menaces.

MioLab Stealer : Un réseau de diffusion via 448 sites GitHub Pages ciblant les utilisateurs de macOS

- MioLab est rapidement devenu l'une des plateformes de Malware-as-a-Service les plus avancées ciblant macOS. Depuis son lancement en novembre 2025, MioLab est passé d'un simple voleur d'informations à un écosystème modulaire combinant le vol d'identifiants, le drainage de portefeuilles de cryptomonnaies, la trojanisation de la chaîne d'approvisionnement, la restauration de sessions Google et un composant d'accès à distance persistant.

- L'opérateur est un développeur unique, hautement qualifié, doté d'une forte discipline opérationnelle. Il maintient des cycles de reconstruction stricts tous les 2 à 4 semaines, applique un géoblocage du trafic en provenance de la CEI, offre un support multicanal 24/7 (Telegram, XMPP, Tox, Matrix) et fait preuve d'une expertise approfondie en rétro-ingénierie. Il revendique plus de 16 000 victimes depuis son lancement.

- Les affiliés amplifient considérablement la portée de MioLab, incluant au moins un acteur aligné sur l'espionnage. Bien que la plupart des affiliés soient probablement des cybercriminels motivés financièrement, Google attribue un cluster (UNC7005 / Storm-2945)

à un espionnage aligné sur l'État russe ciblant des diplomates, des universitaires et du personnel d'ONG à travers l'Europe et les États-Unis.

- MioLab exploite une infrastructure C2 résiliente et multicouche conçue pour résister aux tentatives de démantèlement. Le backend est hébergé sur une infrastructure *bulletproof* aux Seychelles et protégé par des pools Cloudflare, des domaines jetables enregistrés avec de fausses identités et un canal de secours d'accès direct. Cette architecture offre une redondance face à plusieurs modes de défaillance.

- Un réseau de diffusion jusqu'alors non documenté utilisant GitHub Pages, composé de 448 dépôts, distribue des charges utiles malveillantes au format DMG à grande échelle. Chaque dépôt usurpe l'identité d'un logiciel macOS légitime et contient une charge utile DMG, une page d'accueil HTML standardisée et un déploiement automatisé via GitHub Pages. Les horodatages des commits révèlent des vagues de mises à jour orchestrées de manière centrale, alignées sur les cycles de reconstruction de MioLab.

INTRINSEC

Innovative by design

Cyber Threat Intelligence

@Intrinsec @Intrinsec Blog Website

Si vous avez des questions concernant ce rapport, veuillez contacter: cti-ir@intrinsec.com

2026 Intrinsec, Inc. All rights reserved.