CROWDSTRIKE

2025 EUROPEAN THREAT LANDSCAPE REPORT

Sommaire

Présentation générale

Le European Threat Landscape Report 2025 de CrowdStrike fournit des informations clés sur la cyberactivité observée et les développements géopolitiques connexes dans la région. Il synthétise les cybermenaces (États-nations, cybercriminalité et cyberactivisme) qui pèsent sur l'Europe afin d'informer les acteurs des secteurs public et privé.

L'Europe est une cible de choix pour les cybercriminels, probablement en raison de la rentabilité relative des entités basées en Europe, du cadre juridique de la région et des motivations politiques des acteurs de la cybercriminalité. Alors que la chasse au gros gibier (BGH) représente une cybermenace persistante, les entités basées en Europe sont également confrontées à l'évolution des techniques de cybercriminalité, notamment des campagnes exploitant le phishing vocal (vishing) et les leurres CAPTCHA. Les cyberadversaires, qu'ils soient originaires d'Europe ou la ciblent, bénéficient d'un écosystème souterrain hautement organisé et résilient, accessible via les forums du clearnet et du darknet anglophones et russophones. Cet écosystème facilite la collaboration et accueille des services d'accès au réseau, des logiciels malveillants prêts à l'emploi et le violence en tant que service (VaaS).

L'invasion à grande échelle de l'Ukraine par la Russie en février 2022 a déclenché une vague de cyberintrusions ciblées visant des entités ukrainiennes. Bien que la plupart de ces opérations aient été menées par des cybercriminels alliés de la Russie ou favorables à la Russie, les cybercriminels en lien avec la Corée du Nord ont également mené des opérations visant des entités ukrainiennes. Au-delà des opérations spécifiques aux conflits, la Russie, l'Iran, la République populaire démocratique de Corée (Corée du Nord), la Chine, la Turquie, le Kazakhstan et l'Inde ciblent constamment des entités européennes par le biais de cyberopérations motivées par la collecte de renseignements stratégiques, les opérations d'influence (OI), le vol de propriété intellectuelle et les gains financiers opportunistes.

Les événements géopolitiques, y compris les conflits en cours entre la Russie et l'Ukraine et entre Israël et le Hamas, ont été les principaux moteurs de la cyberactivité mondiale dirigée contre les pays européens. Cette activité consistait principalement en des attaques par déni de service distribué (DDoS), des campagnes de type « hack-and-leak » et des dégradations de sites web.

Ce rapport fournit une vue détaillée du paysage européen des cybermenaces sur la base des données fournies par CrowdStrike Intelligence de janvier 2024 à septembre 2025. Il émane de l'équipe CrowdStrike Counter Adversary Operations, qui intègre deux groupes étroitement alignés : CrowdStrike Intelligence et CrowdStrike OverWatch. L'équipe CrowdStrike Intelligence fournit des rapports exploitables qui identifient les nouveaux cyberadversaires, suivent leurs activités et surveillent les cybermenaces émergentes en temps réel. À l'aide de ces renseignements, l'équipe CrowdStrike OverWatch réalise un Threat Hunting proactif sur l'ensemble des données de télémétrie du client afin de détecter et de traiter les activités malveillantes avant qu'elles ne s'intensifient.

Alors que le paysage européen des cybermenaces continue d'évoluer, les organisations doivent rester vigilantes face à un large éventail de cyberadversaires, allant des groupes cybercriminels aux cyberactivistes, en passant par les cybercriminels à la solde d'États. Grâce à des stratégies de sécurité basées sur le renseignement, les parties prenantes à l'échelle régionale peuvent renforcer leurs défenses, atténuer les risques et garder une longueur d'avance sur les cybermenaces émergentes dans un paysage de plus en plus complexe.

CONVENTIONS DE DÉNOMINATION

CYBERADVERSAIRE	ÉTAT-NATION OU CATÉGORIE
BEAR	RUSSIE
BUFFALO	VIETNAM
CHOLLIMA	RDPC (CORÉE DU NORD)
CRANE	ROK (RÉPUBLIQUE DE CORÉE)
HAWK	SYRIE
JACKAL	CYBERACTIVISME
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GÉORGIE
OCELOT	COLOMBIE
PANDA	RÉPUBLIQUE POPULAIRE DE CHINE
SAIGA	KAZAKHSTAN
SPHINX	ÉGYPTE
SPIDER	CYBERCRIMINALITÉ
TIGER	INDE
WOLF	TURQUIE

Portrait de la cybercriminalité

Big Game Hunting ou Chasse au gros gibier

DEPUIS LE 1ER JANVIER 2024, LES CYBERCRIMINELS ADEPTES DE LA CHASSE AU GROS GIBIER ONT IDENTIFIÉ ENVIRON 2 100 VICTIMES BASÉES EN EUROPE SUR PLUS DE 100 SITES DE FUITE DE DONNÉES DÉDIÉS À L'EXTORSION DE DONNÉES ET AUX RANSOMWARES (DLS).

Les victimes basées en Europe représentent près de 22 % des entités nommées sur les sites de fuite dédiés que CrowdStrike Intelligence surveille, ce qui en fait la deuxième région la plus ciblée après l'Amérique du Nord. Selon l'ensemble de données, les entités européennes sont plus de deux fois plus susceptibles d'être ciblées que les entités de la région Asie-Pacifique et Japon. Les entités européennes sont des cibles attrayantes pour les cyberadversaires spécialisés dans la chasse au gros gibier, probablement en raison des facteurs suivants :

- **Pressions juridiques :** les cybercriminels ont tiré parti des sanctions pour compromission de données prévues par le Règlement général sur la protection des données (RGPD) de l'UE afin de faire pression sur les victimes et d'obtenir le paiement des rançons ; plusieurs cybercriminels ont menacé de dénoncer les entités pour non-conformité réglementaire via leur site de fuite dédié, dans des demandes de rançon ou lors de négociations.
- **Cibles lucratives :** l'Europe compte cinq des 10 entreprises les plus importantes au monde — en France, en Allemagne, aux Pays-Bas, en Suisse et au Royaume-Uni. Comme les cyberadversaires spécialisés dans la chasse au gros gibier basent généralement leurs demandes de rançon sur les revenus de l'organisation ciblée, ils perçoivent probablement que les organisations européennes sont en capacité de payer des rançons conséquentes.
- **Motivations politiques :** bien que les cyberadversaires spécialisés dans la chasse au gros gibier soient principalement motivés par l'aspect financier, certains ont exprimé des positions politiques et menacé d'entreprendre des actions à motivation politique. WIZARD SPIDER, par exemple, a soutenu l'invasion russe de l'Ukraine en 2022, et des organisations de l'UE telles qu'Europol ont également signalé que les cybercriminels traditionnels et hybrides[1] coopéraient dans l'intérêt mutuel[2].

1 Les cybercriminels hybrides agissent selon une combinaison de motivations, notamment la cybercriminalité, les États-nations, le cyberactivisme et les opérations d'influence.

2 https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

Selon les données présentes sur les sites de fuite dédiés, le Royaume-Uni, l'Allemagne, l'Italie, la France et l'Espagne ont été les pays européens les plus ciblés. Ces pays représentent les plus grandes économies d'Europe, à l'exception de la Russie, qui est absente de l'ensemble de données (voir la section *Interdictions associées au ciblage des entités en Russie et dans la région de la CEI* à la page 12). Entre janvier 2024 et septembre 2025, les secteurs les plus ciblés ont été la fabrication, les services professionnels, la technologie, l'industrie et l'ingénierie, ainsi que la vente au détail. Les entrées des sites de fuite dédiés nommant des entités basées en Europe ont augmenté de près de 13 % d'une année sur l'autre, passant d'environ 1 220 à 1 380 entrées (Figure 1).

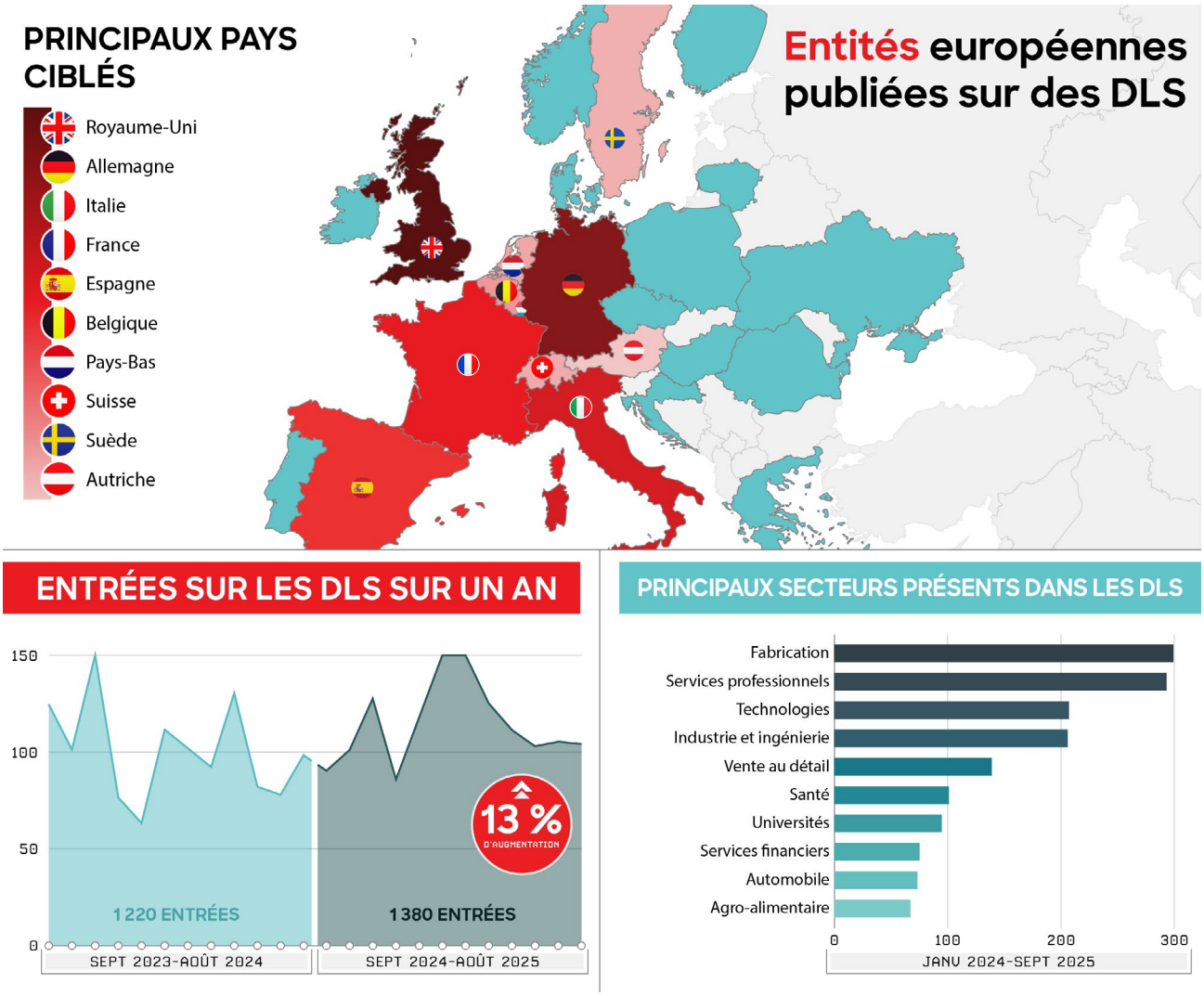


Figure 1. Entrées de sites de fuite dédiés par pays, secteur et période

Parmi ces victimes basées en Europe, 92 % ont été nommées sur des sites de fuite dédiés associés aux ransomwares (par exemple, LockBit de *BITWISE SPIDER*). En règle générale, les cyberadversaires qui exploitent ces sites de fuite dédiés utilisent les ransomwares et le vol de données pour extorquer les victimes. Les 8 % restants ont été nommés sur des sites de fuite dédiés appartenant à des cyberadversaires s'appuyant uniquement sur le vol de données (par exemple, Clop de *GRACEFUL SPIDER*).

Au cours de la période considérée, BITWISE SPIDER, PUNK SPIDER, OCULAR SPIDER, TRAVELING SPIDER et BRAIN SPIDER ont impacté le plus grand nombre de victimes européennes (Figure 2). De plus, dans ce laps de temps, les opérations menées par les forces de l'ordre ont gravement nui à certaines de ces opérations.

Par exemple, les niveaux d'activité des affiliés de BITWISE SPIDER ont considérablement diminué à la suite de l'Opération Cronos, fruit d'une collaboration entre les forces de l'ordre à l'échelle internationale. Une autre initiative de ce type, l'Opération Phobos Aetor, a permis la saisie du site de fuite dédié *8BASE* de BRAIN SPIDER, ainsi que l'arrestation de quatre auteurs présumés d'attaques par ransomware, également membres du groupe *8BASE*. De plus, OCULAR SPIDER a fermé son ransomware en tant que service (RaaS) *RansomHub* suite à des conflits entre les affiliés de *RansomHub* et l'administrateur *RaaS* de DragonForce.

Cependant, des cyberadversaires prolifiques tels que PUNK SPIDER, TRAVELING SPIDER et des cybercriminels anonymes, y compris les affiliés du RaaS *Qilin*, continuent de représenter une cybermenace importante pour les entités européennes.

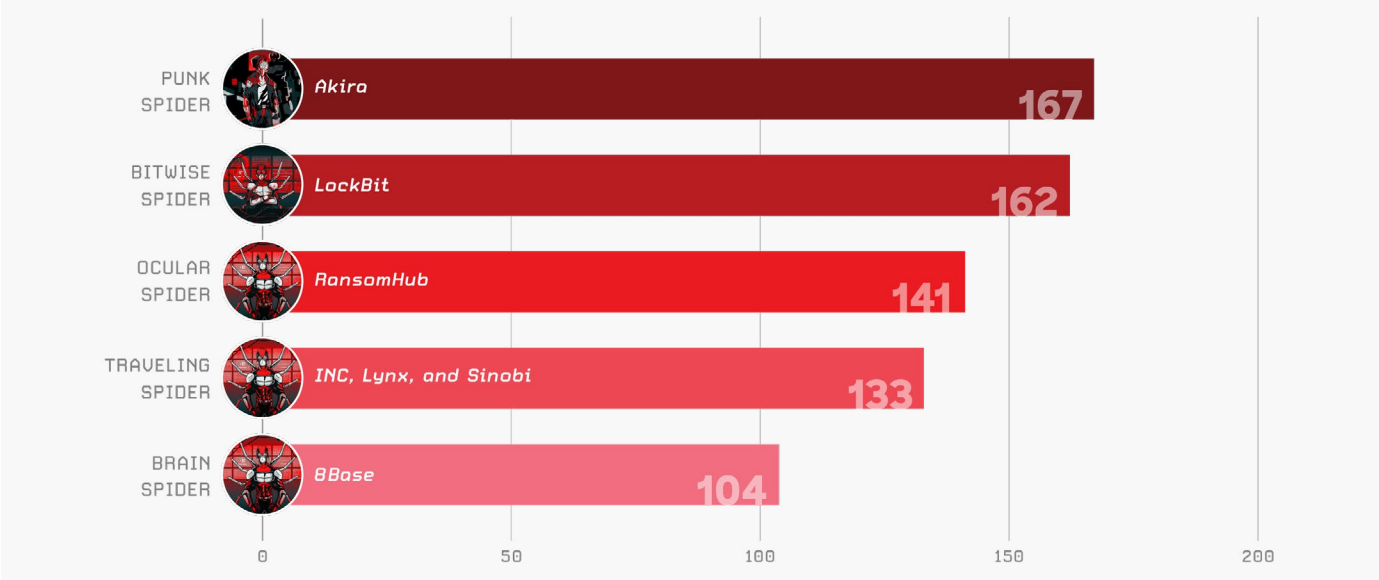


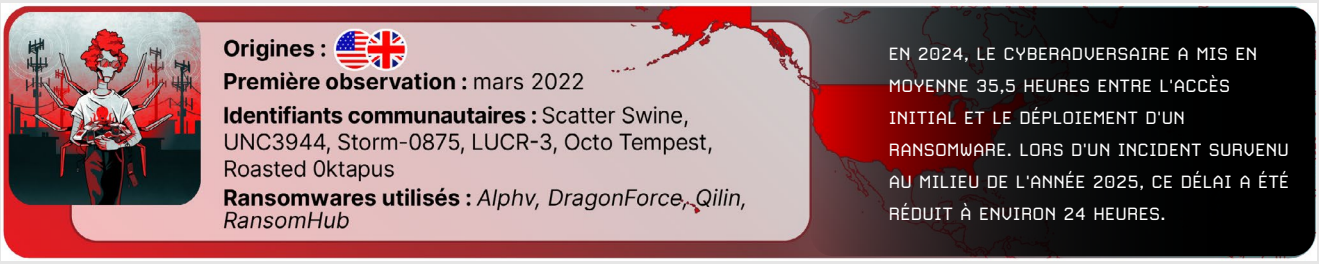
Figure 2. Cyberadversaires prédominants en matière de ransomwares et d'extorsion ciblant les entités européennes, entre janvier 2024 et septembre 2025

Indépendamment de la localisation géographique des victimes, les cyberadversaires spécialisés dans la chasse au gros gibier utilisent généralement les mêmes tactiques, techniques et procédures (TTP). Au cours de la période visée par le rapport, les groupes spécialisés dans la chasse au gros gibier ont fait grand usage des TTP suivants :

- La collecte d'identifiants à partir de bases de données de configuration pour la sauvegarde et la restauration, qui stockent souvent les identifiants utilisés pour accéder à l'infrastructure de l'hyperviseur
- Le chiffrement à distance de fichiers, l'exécution de ransomwares (souvent à partir d'un système non géré)[3] et l'exécution du processus de chiffrement des fichiers en dehors du système ciblé
- L'exploitation de l'accès aux systèmes non gérés pour voler des données et déployer des ransomwares
- Le déploiement d'un ransomware Linux sur l'infrastructure VMware ESXi

3 Un système non géré est un système qui ne comporte aucun logiciel de détection et de réponse aux incidents (EDR).

En 2025, SCATTERED SPIDER cible le secteur de la vente au détail au Royaume-Uni



Actif depuis 2022, SCATTERED SPIDER est devenu l'un des cyberadversaires les plus agressifs et perturbateurs du secteur de la cybercriminalité. SCATTERED SPIDER mène une série d'actions à motif financier, notamment le vol de cryptomonnaies, le détournement de cartes SIM et l'extorsion. Depuis 2023, il cible principalement les entreprises à forte valeur ajoutée dans le cadre de campagnes de ransomware et de vol de données. Les intrusions de SCATTERED SPIDER se caractérisent par des campagnes de vishing sophistiquées ciblant les services d'assistance et utilisées pour obtenir un accès initial, une technique d'attaque innovante ciblant le cloud et, surtout, une rapidité sans égal.

Bien que SCATTERED SPIDER cible principalement les entreprises du secteur privé basées en Amérique du Nord, il a également ciblé des entités en Finlande, en France, en Allemagne, au Luxembourg, en Suède et au Royaume-Uni. Après une période d'inactivité entre décembre 2024 et mars 2025, le cyberadversaire a ciblé de nombreuses entités de vente au détail basées au Royaume-Uni en avril 2025 dans le but de déployer le ransomware *DragonForce*.

Parmi les actions menées en avril 2025, on retrouve une possible tentative d'opération à accès rapproché dans le cadre de laquelle un cybercriminel connu du monde de la cybercriminalité, souvent nommé « The Com » (un écosystème en ligne principalement anglophone composé de plusieurs sous-groupes interconnectés), a tenté de recruter des personnes pour visiter le siège social d'un détaillant basé au Royaume-Uni qui aurait subi une attaque orchestrée par SCATTERED SPIDER. Selon les instructions du cybercriminel, les personnes sélectionnées pour l'opération devaient se procurer un ordinateur portable Windows à usage unique, se rendre au siège social de l'entité basée au Royaume-Uni pour se connecter au réseau Wi-Fi sur place et fournir un accès à distance à l'ordinateur portable via le protocole RDP. La question est de savoir si cette opération à accès rapproché a réellement eu lieu. Cependant, l'évocation d'une telle technique distingue les cybercriminels occidentaux de leurs homologues russes.

Contrairement à la plupart des cyberadversaires spécialisés dans la chasse au gros gibier, les membres de SCATTERED SPIDER sont basés dans les pays occidentaux. CrowdStrike Intelligence a identifié des membres individuels basés aux États-Unis et au Royaume-Uni. En juillet 2025, la National Crime Agency du Royaume-Uni a annoncé l'arrestation de quatre personnes, âgées de 17 à 20 ans, en lien avec de récents incidents ayant impacté des détaillants basés au Royaume-Uni[4]. En septembre 2025, deux de ces personnes ont de nouveau été arrêtées et accusées d'avoir joué un rôle dans un incident survenu en 2024 et ayant impacté le service Transport for London[5]. Malgré de précédentes arrestations, ces individus étaient actifs depuis au moins 2022, ce qui démontre à quel point la perturbation des activités cybercriminelles est complexe, même lorsque les associés d'un cyberadversaire sont sous la juridiction d'une autorité.

4 https://www.nationalcrimeagency.gov.uk/news/retail-cyber-attacks-nca-arrest-four-for-attacks-on-m-s-co-op-and-harrods

5 https://www.nationalcrimeagency.gov.uk/news/two-charged-for-tfl-cyber-attack

Techniques prépondérantes en matière de cybercriminalité

LE VISHING EN PASSE DE DEVENIR UNE CYBERMENACE NOTABLE

Depuis 2024, les cybercriminels ont de plus en plus recours au vishing pour obtenir un accès initial. Le vishing est un type de technique d'ingénierie sociale selon lequel un cyberadversaire appelle une victime pour l'encourager à fournir des identifiants ou à effectuer une action depuis leur endpoint. En plus de faciliter la fraude, des cybercriminels comme CURLY SPIDER et MUTANT SPIDER ont utilisé le vishing pour obtenir un accès initial aux groupes de ransomwares (voir la section *Access brokers initiaux* à la page 14). De même, des acteurs ou affiliés des cyberadversaires spécialisés dans la chasse au gros gibier ROYAL SPIDER, TUNNEL SPIDER et WANDERING SPIDER ont utilisé le vishing dans leurs opérations.

Fin 2024, un utilisateur très probablement associé à MUTANT SPIDER a posté un message sur le forum russophone Exploit, affirmant préférer les cibles basées en Amérique du Nord à celles basées en Europe, car elles étaient plus susceptibles de payer des rançons plus élevées.

Cependant, le vishing deviendra probablement une cybermenace plus importante pour les entités basées en Europe. Cette évaluation est réalisée avec un degré de confiance modéré sur la base des récents incidents de vishing à fort impact ayant touché des entités en Europe (voir la section *SCATTERED SPIDER cible le secteur de la vente au détail au Royaume-Uni en 2025* à la page 8). On constate également que les cybercriminels font de plus en plus appel à des locuteurs natifs de leurs régions cibles pour les campagnes de vishing. Par exemple, PLUMP SPIDER a fait appel à des lusophones pour cibler des entités basées au Brésil, et une campagne de vishing datant de février 2025 a très certainement impliqué des germanophones pour la diffusion de TeamViewer et *SH RAT* auprès d'entités en Allemagne.

AU COURS DE LA PÉRIODE VISÉE PAR LE RAPPORT, CROWDSTRIKE OVERWATCH ET L'ÉQUIPE CROWDSTRIKE FALCON® COMPLETE NEXT-GEN MDR ONT OBSERVÉ PRÈS DE 1 000 INCIDENTS LIÉS AU VISHING DANS LE MONDE. LA PLUPART DE CES INCIDENTS ONT EU UN IMPACT SUR DES ENTITÉS BASÉES EN AMÉRIQUE DU NORD, PROBABLEMENT EN RAISON DE L'OMNIPRÉSENCE DE LA LANGUE ANGLAISE AINSI QUE DU CHIFFRE D'AFFAIRES ÉLEVÉ DES ENTITÉS CIBLÉES.

LES FAUX CAPTCHA RESTENT UN VECTEUR D'ATTAQUE COURANT

Depuis le milieu de l'année 2024, les cybercriminels ont commencé à largement adopter les leurres CAPTCHA (alias *ClickFix*) pour diffuser des logiciels malveillants. Cette technique d'ingénierie sociale consiste à utiliser des pages qui imitent les tests d'authentification CAPTCHA pour convaincre les victimes de copier, coller et exécuter du code malveillant dans la boîte de dialogue Exécuter ou le terminal Windows.

Les campagnes identifiées ont utilisé des e-mails de phishing, de la publicité malveillante et l'empoisonnement de l'optimisation pour les moteurs de recherche (SEO) pour diriger les cibles vers de fausses pages CAPTCHA. Alors que les campagnes exploitant des leurres CAPTCHA sont souvent opportunistes, certains cybercriminels adaptent les faux CAPTCHA à leurs cibles spécifiques, telles que les entités du secteur de l'hôtellerie et du voyage.

EN 2024 ET 2025, CROWDSTRIKE A IDENTIFIÉ PLUS DE 1 000 INCIDENTS IMPLIQUANT DES LEURRES CAPTCHA AYANT IMPACTÉ DES CLIENTS BASÉS EN EUROPE (FIGURE 3).

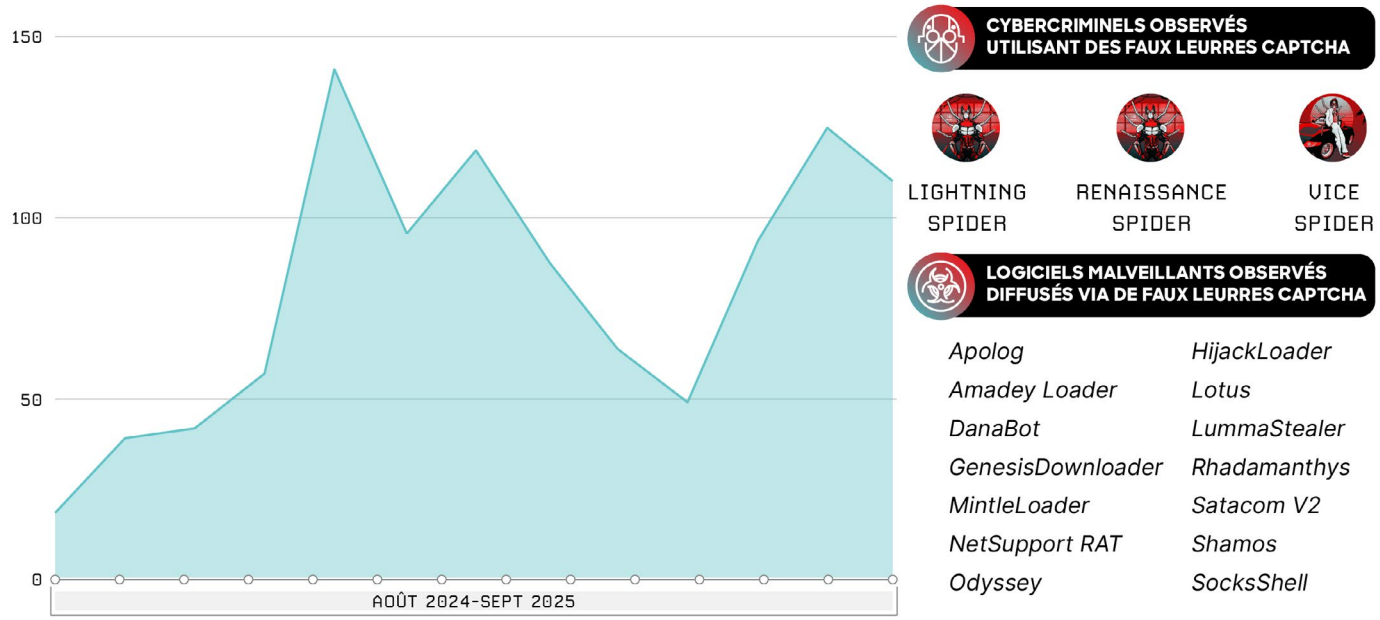


Figure 3. Incidents liés aux leurres CAPTCHA auprès de clients basés en Europe

Sur les forums de cybercriminalité russophones Exploit et XSS, plusieurs outils qui peuvent être utilisés pour créer de fausses pages CAPTCHA personnalisables ou prêtes à l'emploi pour Windows, macOS et Linux (voir la section *Écosystème clandestin* à la page 11) ont été proposés. Parmi les fonctionnalités, on pouvait retrouver la dissimulation de code créée dynamiquement, des capacités de contournement de la sécurité et des fonctions de leurre (par exemple, l'imitation des plateformes de gestion des cryptomonnaies). Ces services rendent les leurres CAPTCHA facilement accessibles à un large éventail de cybercriminels.

LIGHTNING SPIDER, RENAISSANCE SPIDER et VICE SPIDER ont tous historiquement ciblé des entités basées en Europe et utilisé des leurres CAPTCHA dans leurs campagnes. De plus, des cybercriminels non identifiés ont utilisé des leurres CAPTCHA pour diffuser *l'Odyssey* de BRASH SPIDER, *le Shamos* de COOKIE SPIDER, *le chargeur Amadey* de HAZARD SPIDER, *le Lotus* de LUNAR SPIDER, *le DanaBot* de SCULLY SPIDER et le *MintleLoader* (alias MintsLoader, MintLoader) dans des campagnes ciblant l'Europe et d'autres zones géographiques.

Écosystème clandestin

Bien que les opérations menées par les forces de l'ordre permettent parfois de saisir des infrastructures et d'arrêter des administrateurs qui exploitent des plateformes basées en Europe, l'écosystème clandestin européen, et plus particulièrement russophone, reste robuste. De nombreux forums, places de marché et canaux Telegram persistants et émergents soutiennent les cybercriminels montrant différents niveaux de sophistication, en servant de plaques tournantes pour la collaboration, le partage de connaissances et d'outils, et la fourniture de divers services de facilitation de la cybercriminalité.

FORUMS DE CYBERCRIMINALITÉ RUSSOPHONES

Depuis près de trois décennies, les cybercriminels se sont regroupés sur les forums russophones clandestins. Bien que ces forums aient initialement fourni une plateforme pour le carding (c'est-à-dire le vol et la vente de détails de cartes de crédit), l'écosystème a rapidement évolué pour proposer des forums spécialisés dans divers services de cybercriminalité ou méthodes de monétisation[6].

La multiplication des forums de cybercriminalité a permis aux cybercriminels de partager leurs connaissances sur les techniques d'attaque et les outils, ainsi que de vendre et développer leurs services. Certains forums, notamment Exploit et XS, qui ont été fragilisés par les récentes arrestations et la saisie de domaines clearnet, accueillent des discussions générales sur la cybercriminalité. Cependant, de nombreux forums se spécialisent dans des services spécifiques de cybercriminalité ou des méthodes de monétisation, notamment :

- **Le carding :** connu comme l'une des premières grandes activités de cybercriminalité dans l'écosystème clandestin russophone, le carding continue de faire l'objet de discussions sur des forums généralistes et spécialisés (par exemple, WWH-Club ou le fameux CarderPlanet). Les « carders » (кардеры) échangent des données de carte de paiement obtenues par compromission de données ou via le piratage de distributeurs de billets, les logiciels malveillants installés sur les points de vente (POS) ou encore le piratage de formulaires[7].
- **Services financiers :** sur ces forums, on retrouve des services relatifs à la fraude financière, au blanchiment d'argent et à l'encaissement. Le forum DarkMoney, administré par un acteur de RENAISSANCE SPIDER, était historiquement l'un des principaux forums de services financiers, générant un revenu publicitaire de 200 000 € par mois.
- **Probiv :** le terme « probiv » (пробив) décrit un service important dans l'écosystème clandestin russophone selon lequel les utilisateurs échangent des informations personnelles obtenues à partir de données divulguées ou recrutent des utilisateurs internes disposant d'un accès spécifique aux données. Les autorités russes se sont récemment attaquées aux fuites de données et aux services probiv, en partie en raison de leur rôle dans la facilitation du journalisme d'investigation[8].
- **Ransomware :** à la suite de l'attaque DarkSide très médiatisée et orchestrée par *CARBON SPIDER* en mai 2021, les forums de cybercriminalité russophones ont interdit les discussions liées aux ransomwares. En conséquence, un cybercriminel probablement lié au groupe *Babuk Locker* (aujourd'hui disparu) a créé le forum RAMP, qui fournit une section dédiée aux programmes d'affiliation RaaS.

Cet écosystème de cybercriminalité accueille une large base de cybercriminels et de services de facilitation, y compris des access brokers initiaux et des data brokers, des fournisseurs d'hébergement hypersécurisé, des services d'encaissement et des mixeurs de cryptomonnaies, des opérateurs de malwares en tant que service (MaaS) et de RaaS, ainsi que des spammeurs. Afin de réguler les interactions et d'instaurer la confiance entre les acheteurs, les vendeurs et les autres utilisateurs, les forums de cybercriminalité russophones ont développé un modèle d'auto-régulation qui comprend l'arbitrage des litiges, des garants de transactions et un système de dépôt fiduciaire automatisé, un système de réputation et de niveaux d'utilisateurs, une fonctionnalité de dépôt[9] et des règles de forum appliquées par les administrateurs et les modérateurs.

---

6 https://www.justice.gov/archives/opa/pr/ukrainian-national-who-co-founded-cybercrime-marketplace-sentenced-18-years-prison
https://www.own.security/ressources/blog/russian-language-cybercriminal-forums---chapter-i-an-excursion-into-the-core-of-the-underground-ecosystem

7 Dans le cadre d'opérations de piratage de formulaires (attaques Magecart, piratage de paiement en ligne, écoute du trafic réseau), les cybercriminels injectent du code JavaScript malveillant dans les sites web pour collecter des informations sur les cartes de paiement des clients et/ou des informations personnellement identifiables (IPI) à partir des couches frontales des sites web.

8 https://meduza.io/en/feature/2025/07/29/too-much-is-slipping-through

9 Souvent, les administrateurs des forums exigeront des vendeurs qu'ils versent un dépôt d'une valeur proportionnelle à ce qu'ils vendent. Par exemple, un utilisateur qui tente de vendre un produit pour 10 000 USD peut être invité à déposer ce montant dans un portefeuille dédié du forum.

Interdictions associées au ciblage des entités en Russie et dans la région de la CEI

L'interdiction de cibler les organisations et les citoyens russes, ainsi que les pays de la Communauté des États indépendants (CEI), est depuis longtemps une règle tacite et souvent codifiée dans l'écosystème clandestin russophone. Bien que cette interdiction soit probablement motivée par la volonté d'éviter les forces de l'ordre locales, le patriotisme joue aussi vraisemblablement un rôle, les cybercriminels basés dans la CEI préférant cibler des entités externes.

De nombreux et opérateurs de MaaS et de RaaS russophones interdisent à leurs clients et affiliés de cibler la Russie et la région de la CEI. Par exemple, la vente du *chargeur Amadey* de HAZARD SPIDER sur le forum XSS indiquait que le chargeur n'était « pas opérationnel dans la Fédération de Russie et dans les pays frères ». *Le chargeur Amadey* met en application cette interdiction en n'exécutant pas les commandes C2 (commande et contrôle) si les ID de disposition de clavier des pays de la CEI sont identifiés sur le système. Des garde-fous similaires pour la langue d'interface utilisateur par défaut des systèmes se trouvent dans *Lumma Stealer et Matanbuchus et Rhadamanthys de* DEMON SPIDER.

Bien que le ciblage d'entités dans ces régions ne soit pas toujours explicitement interdit sur les forums de cybercriminalité, les cybercriminels russophones ont ostracisé leurs paires qui ne respectent pas cette interdiction. En mars 2024, un utilisateur du forum XSS associé à BRASH SPIDER, développeur des voleurs d'informations *Doshell Stealer* et *Odyssey* sur macOS, a accusé COOKIE SPIDER de cibler la région de la CEI et a appelé à son expulsion du forum.

FORUMS DE cYBERCRIMINALITÉ ANGLOPHONES

Les forums de cybercriminalité anglophones sont devenus des plaques tournantes essentielles au sein de l'écosystème européen plus large de la cybercriminalité, servant de places de marché et d'espaces communautaires où les cybercriminels échangent des outils, des données et une expertise. Contrairement aux forums russophones qui ont historiquement dominé le développement de logiciels malveillants sophistiqués et le recrutement d'affiliés pour des programmes de ransomwares, les forums anglophones ont créé des passerelles accessibles pour des cybercriminels européens aux niveaux de compétence variés. Ils offrent un accès simplifié aux données de compromission, aux outils banalisés et aux services de blanchiment d'argent, le tout soutenu par des fonctionnalités de renforcement de la confiance telles que le dépôt fiduciaire automatisé et les scores de réputation.

Sur les forums tels que BreachForums, on trouve généralement des bases de données contenant des données personnelles et d'entreprise compromises, des identifiants d'accès pour les VPN d'entreprise et les environnements cloud, ainsi que des outils tels que des voleurs d'informations, des chargeurs et des kits de phishing. Les fournisseurs proposent également des tutoriels, des listes d'access brokers initiaux et des services de blanchiment qui permettent aux cybercriminels pour monétiser leurs opérations. Les transactions sont généralement réalisées à l'aide de cryptomonnaies, et de nombreux forums utilisent des services de dépôt fiduciaire pour modérer les transactions, réduisant ainsi le risque de fraude dans les communautés intrinsèquement indignes de confiance.

Direction de BreachForums : intervention des forces de l'ordre

BreachForums est devenu une plateforme essentielle dans l'écosystème de la cybercriminalité anglophone après que les autorités ont saisi son prédécesseur, RaidForums, en avril 2022. Après que les forces de l'ordre ont arrêté l'administrateur de RaidForums, Diogo Santos Coelho (connu sous le nom d'Omnipotent) au Portugal et saisi le domaine, la place laissée vacante a rapidement été occupée par Pompompurin, un membre très respecté de la communauté de RaidForums, qui a lancé BreachForums en mars 2022.

Pompompurin a été arrêté en 2023, et la propriété du forum a été transférée à ShinyHunters, qui avait mené de nombreuses opérations de vol de données très médiatisées. ShinyHunters est probablement basé en France, comme le corrobore un acte d'accusation du ministère américain de la Justice (DOJ) datant de juin 2021 et visant plusieurs individus basés en France et associés au groupe. La direction du forum a connu plusieurs transitions jusqu'à ce que le cyberadversaire britannique BUTLER SPIDER (alias *IntelBroker*) en devienne le principal propriétaire et administrateur en août 2024.

BUTLER SPIDER, qui était un membre éminent du forum, a revendiqué la responsabilité de la vente et de l'exposition de données sensibles appartenant aux gouvernements américain et européen. En janvier 2025, BUTLER SPIDER a démissionné de son poste d'administrateur de BreachForums, affirmant qu'il n'avait pas le temps nécessaire pour assurer la gestion du forum. En février 2025, certaines sources indiquent que les autorités françaises auraient procédé à l'arrestation de BUTLER SPIDER. Son inactivité depuis mars 2025 a conduit d'autres membres du forum à se demander si le cyberadversaire avait été arrêté.

En avril 2025, le forum a été mis hors ligne, bien que les administrateurs de l'époque aient affirmé avoir intentionnellement fermé le forum car il avait été ciblé par un exploit zero day. En juin 2025, la brigade française de lutte contre la cybercriminalité aurait arrêté quatre personnes répondant aux surnoms de ShinyHunters, Hollow, Noct et Depressed pour leur rôle dans le développement et l'administration de BreachForums.

Le parcours tumultueux de BreachForums démontre comment certains cybercriminels peuvent à eux seuls influencer de manière significative l'activité d'un forum, tout en attirant l'attention des forces de l'ordre internationales.

ACCESS BROKERS INITIAUX

Les access brokers initiaux (IAB) sont des cybercriminels qui obtiennent et vendent des accès aux réseaux d'entreprise sur des forums et des places de marché. Les IAB utilisent diverses TTP pour obtenir un accès initial, notamment l'utilisation abusive d'identifiants compromis, l'exploitation des vulnérabilités et l'utilisation de l'ingénierie sociale. Les entités basées en Europe sont une cible de choix parmi les IAB et leurs acheteurs. Les acheteurs potentiels préfèrent le plus souvent accéder à des entités américaines, suivies par les entités européennes, canadiennes et australiennes.

DEPUIS JANVIER 2024, CROWDSTRIKE INTELLIGENCE A IDENTIFIÉ 260 ACCESS BROKERS INITIAUX VENDANT DES ACCÈS RÉSEAU À PLUS DE 1 400 ENTITÉS BASÉES EN EUROPE.

La plupart des entités vendues se trouvent au Royaume-Uni, en Espagne, en Allemagne, en Italie et en France, ainsi que dans les secteurs universitaire, de la vente au détail, des services professionnels, de la fabrication, de l'industrie et de l'ingénierie. À l'instar d'autres services du même type, les IAB russophones se sont souvent imposé des restrictions sur la vente d'accès aux entités en Russie et dans la région de la CEI (Figure 4).

	ROYAUME-UNI	ESPAGNE	ALLEMAGNE	ITALIE	FRANCE	PAYS-BAS	BELGIQUE	SUÈDE	SUISSE	PORTUGAL	AUTRICHE	POLOGNE	DANEMARK	NORVÈGE	RÉPUBLIQUE	AUTRES	GRAND TOTAL
Universités	40	10	23	19	16	14	5	1	1	9	1	7	0	0	1	15	162
Vente au détail	28	25	10	20	12	2	4	5	6	2	2	5	7	2	0	14	135
Services professionnels	34	10	24	6	13	9	2	6	5	3	5	2	4	3	2	6	133
Fabrication	20	9	16	14	3	6	3	3	5	0	4	1	0	2	0	6	92
Industrie et ingénierie	19	5	18	16	4	5	7	3	3	0	3	1	0	0	0	5	85
Technologies	14	14	7	10	9	5	2	4	1	6	0	1	3	4	0	3	83
Administrations	4	7	3	10	9	1	1	5	0	1	1	0	1	1	0	6	50
Services financiers	13	3	1	7	6	5	0	0	2	1	0	1	1	0	3	7	49
Télécommunications	5	5	4	4	5	2	0	1	0	1	1	1	0	0	1	10	40
Santé	4	2	4	1	5	8	5	0	1	0	0	1	1	0	1	6	38
Automobile	1	3	7	5	1	4	0	2	1	0	0	0	0	1	0	3	27
Énergie	2	1	3	3	3	0	0	0	1	0	0	3	1	1	0	2	20
Médias	4	1	1	0	10	0	0	0	1	0	0	0	0	0	1	2	20
Transports	1	0	1	2	2	6	0	2	0	0	0	0	0	0	1	3	18
Logistique	6	5	1	1	2	0	0	0	0	0	1	0	1	0	0	0	17
Autre	100	65	38	40	55	14	18	10	15	5	9	4	7	5	5	72	462
Grand total	292	161	160	156	153	80	46	42	41	28	27	27	24	19	15	160	1 431

Figure 4. Répartition des entités vendues par les access brokers initiaux, par principaux pays et secteurs européens, entre janvier 2024 et septembre 2025

Sur la base de cet ensemble de données, les pays et les secteurs les plus proposés par les IAB coïncident généralement avec ceux nommés sur les sites de fuite dédiés de chasse au gros gibier (voir la section *Chasse au gros gibier* à la page 5). Cela est probablement dû à divers facteurs, dont la collaboration étroite entre les IAB et les cyberadversaires spécialisés dans la chasse au gros gibier. Par exemple, HOOK SPIDER, qui a opéré sous plusieurs pseudonymes sur les forums de cybercriminalité russophones Exploit, RAMP et XSS, a très probablement vendu des accès à plusieurs cyberadversaires spécialisés dans la chasse au gros gibier (y compris BITWISE SPIDER et BRAIN SPIDER) et est historiquement associé à SCATTERED SPIDER.

MALWARES EN TANT QUE SERVICE (MAAS)

Le MaaS est un service facilitateur qui propose des logiciels malveillants (par exemple, des logiciels malveillants bancaires, des voleurs d'informations, des crypteurs et des chargeurs), selon un modèle similaire au SaaS légitime. Grâce au modèle MaaS, les cybercriminels peuvent accéder beaucoup plus facilement à des outils qu'ils n'auraient pas le temps ou les ressources de développer autrement.

Les opérateurs MaaS proposent leurs outils par le biais de divers modèles commerciaux, notamment des accords d'achat, de location ou de paiement à l'installation, ainsi que des programmes d'affiliation prévoyant un partage des bénéfices entre les opérateurs MaaS et leurs affiliés (Figure 5). Les opérateurs MaaS russophones proposent généralement leurs services sur des forums de cybercriminalité (notamment Exploit), des canaux Telegram publics ou privés et, dans le cas de LUNAR SPIDER, via un système de recommandation.

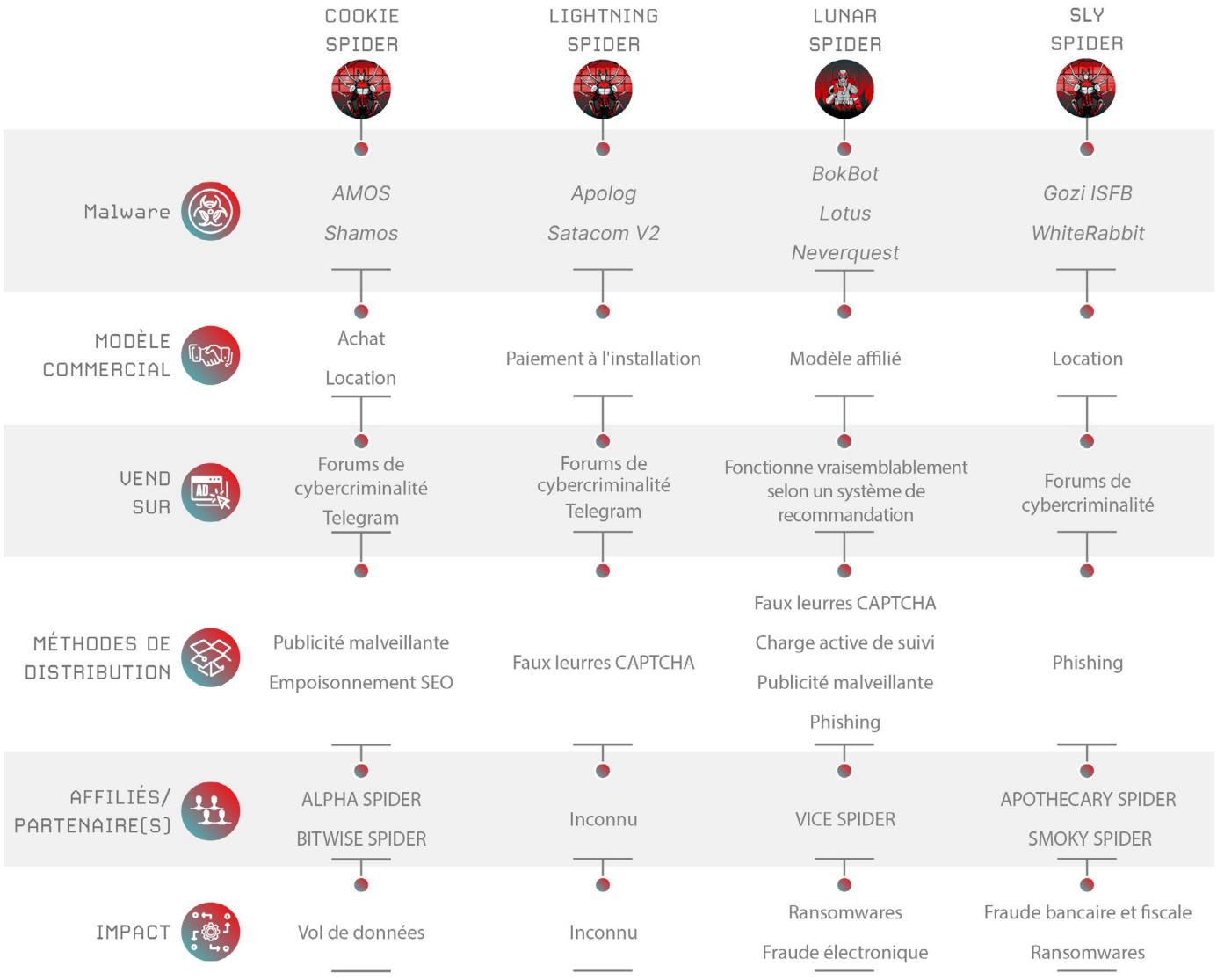


Figure 5. Des opérateurs MaaS de premier plan ciblant des pays européens

Alors que les opérations policières telles que l'opération Endgame ou la saisie de XSS en juillet 2025 perturbent régulièrement l'écosystème, les opérateurs MaaS restent résilients, en partie grâce à la persistance de membres de longue date qui agissent en quasi-impunité dans leurs juridictions. Cependant, Vyacheslav Igorevich Penchukov (alias Tank), un membre de LUNAR SPIDER actif depuis 2009 et initialement membre du gang *JabberZeus*, a été arrêté à Genève, en Suisse, en 2022 et extradé vers les États-Unis au début de l'année 2024.

Outre le fait de faciliter les activités d'autres cybercriminels, la persistance et la prolifération des opérateurs MaaS compliquent également l'attribution, car ils fournissent les mêmes outils à un grand nombre de cybercriminels, souvent distribués selon des TTP similaires. Les cyberadversaires à la solde d'États exploitent ce modèle, comme le cyberadversaire associé à la Russie EMBER BEAR, qui a tiré parti de *Matanbuchus* (fourni par DEMON SPIDER), de *SmokeLoader* (fourni par SMOKY SPIDER) et de *Raccoon Stealer*. En mai 2025, le ministère américain de la Justice a inculpé 16 membres du MaaS *DanaBot* de SCULLY SPIDER, révélant que des cybercriminels liés à la Russie avaient utilisé ce service criminel pour soutenir des opérations militaires et des activités d'espionnage[10].

Outils de communication (Telegram, Tox et Jabber)

Bien que les services de cybercriminalité soient souvent proposés sur des forums dédiés, la communication avec les clients potentiels se fait généralement sur Telegram. Alors que les suppressions de canaux ont augmenté après l'arrestation du PDG de Telegram, Pavel Durov, en août 2024 et que les conditions générales d'utilisation de Telegram ont été mises à jour, les cybercriminels continuent largement d'utiliser Telegram comme principale plateforme de communication. Telegram permet aux services de cybercriminalité de communiquer les mises à jour ou les pannes de service, ainsi que d'offrir une assistance directe aux clients.

Tox et Jabber représentent d'autres méthodes de communication courantes. Les messages Tox sont inaltérables, ce qui empêche les clients de modifier les accords après une vente. De plus, par rapport aux forums de cybercriminalité et à Telegram, Jabber est moins sujet aux perturbations en raison de sa nature décentralisée et de la possibilité pour les cybercriminels d'exploiter leurs propres serveurs Jabber.

VIOLENCE EN TANT QUE SERVICE ET VOL PHYSIQUE DE CRYPTOMONNAIES

Depuis 2024, les vols de cryptomonnaies impliquant des attaques physiques et des enlèvements ont considérablement augmenté, notamment en Europe. En janvier 2025, des cybercriminels ont kidnappé et tenté d'extorquer le cofondateur de Ledger, une entreprise française spécialisée dans les portefeuilles de cryptomonnaies. Bien que les cybercriminels impliqués dans cette affaire (et de nombreux autres) aient été arrêtés, la cybermenace persiste[11]. Entre janvier et septembre 2025, 17 incidents similaires se sont produits en Europe, dont 13 en France[12].

Les individus impliqués dans le vol physique de cryptomonnaies opèrent souvent au sein de communautés de cybercriminels affiliées à « The Com ». Plusieurs de ces personnes ont déjà vendu des outils tels que des bots d'interception de mots de passe à usage unique. Il s'agit d'outils basés sur Telegram qui permettent aux cybercriminels d'automatiser les appels de vishing à destination des victimes, souvent utilisés pour cibler des comptes sur des plateformes d'échange de cryptomonnaies.

---

10 https://www.crowdstrike.com/en-us/blog/crowdstrike-partners-with-doj-disrupt-danabot-malware-operators/

11 https://www.france24.com/en/france/20250621-france-arrests-five-kidnapping-cryptocurrency-entrepreneur-father

12 https://github.com/jlopp/physical-bitcoin-attacks

RENAISSANCE SPIDER représente une cybermenace importante pour l'Europe

RENAISSANCE SPIDER est un cyberadversaire basé en Russie et actif dans un éventail d'activités allant de la cybercriminalité au cyberespionnage et aux opérations d'influence, et ayant également contribué à des actes de sabotage physique.

- RENAISSANCE SPIDER mène des campagnes de phishing de grande ampleur, ciblant principalement les secteurs public et privé de l'Ukraine. Il a ciblé de façon sporadique des entités à travers l'Europe, notamment en Allemagne, en Italie, en Lituanie, en Moldavie, en Pologne, en Suisse et au Royaume-Uni. Ce cyberadversaire est probablement motivé à la fois par le gain financier et la collecte de renseignements.
- RENAISSANCE SPIDER a ciblé des entités à travers l'Europe au moyen d'opérations d'influence menées par e-mail et sur les réseaux sociaux par le biais de diverses identités fictives, notamment le faux cyberactiviste *DaVinci Group*, ou en se faisant passer pour de vrais journalistes moldaves en utilisant leurs comptes de messagerie compromis. Plus récemment, le cyberadversaire a envoyé de fausses menaces à la bombe par e-mail à diverses entités européennes, dans l'objectif vraisemblable de saper le soutien apporté à l'Ukraine.
- En août 2024, RENAISSANCE SPIDER a créé le prétendu VaaS *Fire Cells Group*, en recrutant des personnes pour mener des actions de subversion et de sabotage en Ukraine. Sous le prétexte d'agir au nom du *Fire Cells Group*, le cyberadversaire a mené des opérations d'influence, a offert de l'argent pour l'assassinat de responsables ukrainiens et a très probablement payé des individus pour organiser des incendies criminels contre des véhicules militaires ukrainiens et des infrastructures civiles.

CrowdStrike Intelligence estime que les opérateurs de RENAISSANCE SPIDER agissent probablement sous la direction ou en coordination avec les services spéciaux russes. Cette évaluation est réalisée avec un degré de confiance modéré sur la base des activités du cyberadversaire (par exemple, opérations d'influence et sabotage), du ciblage aligné sur les intérêts de l'État russe, de l'arrestation probable de membres du groupe en 2021 et d'autres accusations pesant sur les cybercriminels.

Portrait des menaces étatiques

Les conflits cinétiques, notamment la guerre en Ukraine et les conflits au Moyen-Orient, sont les principaux moteurs de la cyberactivité en Europe. Dans ces contextes, les cybercriminels à la solde d'États emploient principalement leurs cybercapacités à des fins de soutien, par exemple pour obtenir une visibilité sur des entités gouvernementales et militaires cibles afin de soutenir l'effort de guerre ou pour renforcer les opérations d'information (et de désinformation). Certains cyberadversaires ont également utilisé leurs accès aux réseaux comme arme pour dégrader, perturber ou détruire l'accès aux infrastructures critiques et aux fonctions gouvernementales essentielles.

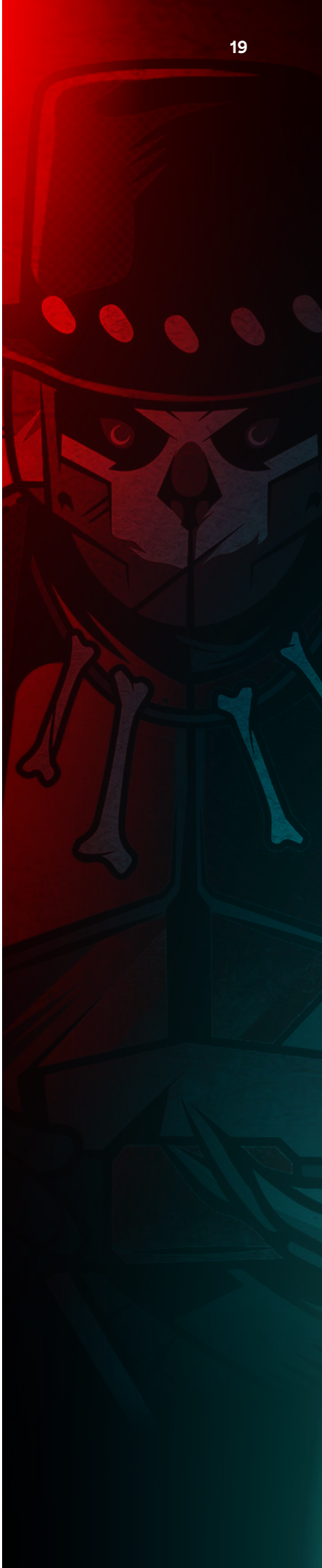
Parallèlement, un large éventail de cyberactivités commanditées par les États persiste. Ces campagnes vont des intrusions ciblées à des fins d'espionnage traditionnel, visant à obtenir des informations géopolitiques et opérationnelles ou à faciliter le vol de propriété intellectuelle, à des intrusions opportunistes à des fins lucratives.

Cyberactivité axée sur les conflits

CONFLITS EN LIEN AVEC LA RUSSIE

L'invasion à grande échelle de l'Ukraine par la Russie en février 2022 a déclenché une vague de cyberintrusions ciblées, orchestrées à la fois par des cybercriminels bien établis et émergents. Les mandats de renseignement propres à chaque cyberadversaire forment, collectivement, une vaste campagne de collecte d'informations au service de divers objectifs stratégiques. Bien que la plupart des activités de collecte de renseignements liées au conflit soient menées par les services de renseignement russes (RIS), principalement le GRU (alias GU, Direction principale de l'état-major général des forces armées de la Fédération de Russie) et le Service fédéral de sécurité de la Fédération de Russie (FSB), les agences de renseignement de la Corée du Nord ont également été impliquées dans des opérations cinétiques et cyber visant l'Ukraine.

Figure 6. Les cyberadversaires liés au conflit en Ukraine



Les cyberadversaires liés au GRU mènent des opérations de collecte de renseignements et de perturbation

Le cyberadversaire associé au GRU FANCY BEAR a mené de nombreuses campagnes simultanées visant des entités militaires et gouvernementales ukrainiennes. Bien qu'il ait utilisé son kit d'outils de phishing d'identifiants personnalisé pour ses opérations de phishing ciblant les utilisateurs du service de messagerie web ukrainien gratuit **ukr.net** depuis 2023, il a également exploité *ClickFix*, des fichiers RDP malveillants et des grands modèles de langage open source dans ses campagnes.

La collecte de renseignements de FANCY BEAR se concentre sur le soutien aux objectifs militaires de la Russie en Ukraine sur les plans stratégique, opérationnel et tactique. Le cyberadversaire cible d'importantes entités nationales et locales dans divers secteurs, telles que des organismes gouvernementaux, ainsi que des individus, y compris des membres des forces armées ukrainiennes.

Parallèlement, le cyberadversaire associé au GRU VOODOO BEAR s'est concentré sur les infrastructures critiques ukrainiennes, en menant des opérations destructrices contre des entités des secteurs de l'énergie, des télécommunications et des services publics. Dans les cas où il n'a pas déployé immédiatement de logiciel malveillant de type wiper, VOODOO BEAR a probablement conservé son accès pour se déplacer latéralement et compromettre d'autres réseaux, afin de soutenir ses besoins en matière de collecte de renseignements et d'opérations destructrices.

Début 2025, CrowdStrike OverWatch a détecté que VOODOO BEAR utilisait la porte dérobée *POEMGATE* exploitant le protocole SSH ainsi qu'un enregistreur d'identifiants, dans les environnements d'entités ukrainiennes du secteur des télécommunications. En juin 2025, le cyberadversaire a poursuivi les opérations d'accès initial en diffusant de faux programmes d'installation d'antivirus contenant la porte dérobée *Sumbur*, qui télécharge et exécute des charges actives supplémentaires pour faciliter la persistance à long terme.

Les cyberadversaires liés au FSB mènent des opérations d'information et de collecte de renseignements

Les priorités de ciblage des cybercriminels liés au FSB russe sont restées les mêmes depuis 2022. PRIMITIVE BEAR continue de mener des campagnes de harponnage (spear phishing) de grande ampleur contre les organisations gouvernementales et militaires ukrainiennes, certainement pour recueillir des renseignements qui soutiennent les objectifs de guerre de la Russie, tels que le renforcement de son influence politique et militaire.

GOSSAMER BEAR mène des opérations de phishing d'identifiants ciblant les entités gouvernementales et militaires ukrainiennes, ainsi que des organisations non gouvernementales (ONG) du Royaume-Uni et de l'UE. CrowdStrike Intelligence estime, avec un degré de confiance modéré, que les opérations de phishing d'identifiants menées par GOSSAMER BEAR soutiennent probablement des opérations d'influence visant à saper le moral des citoyens ukrainiens ou à dénigrer et affaiblir la crédibilité de la gouvernance britannique et des institutions occidentales.

Autres clusters d'activités associés à la Russie

Depuis au moins 2017, le cluster d'activités associé à la Russie RepeatingUmbra cible les entités gouvernementales et de défense ukrainiennes. En 2024 et 2025, le cluster a mené des campagnes de phishing d'identifiants et a utilisé plusieurs variantes de son téléchargeur personnalisé *Pryatki* pour diffuser *Cobalt Strike* auprès de cibles ukrainiennes.

Depuis 2022, le besoin accru de renseignements pour soutenir l'effort de guerre russe a conduit à l'émergence de nouveaux cybercriminels qui mènent souvent des opérations de grande ampleur, mais peu sophistiquées, contre des cibles gouvernementales et militaires ukrainiennes. Par exemple, CrudeScientist, un cluster d'activités probablement associé à la Russie et actif depuis au moins novembre 2023, a maintenu un rythme opérationnel élevé jusqu'au début de l'année 2025 avec des TTP très cohérentes et peu sophistiquées.

De même, FamishedLibrarian, un autre cluster d'activités probablement associé à la Russie et actif depuis au moins novembre 2022, s'appuie sur des TTP de diffusion relativement inchangées et continue de commettre des erreurs de sécurité opérationnelle (OPSEC) qui exposent l'infrastructure de sa campagne.

UN CLUSTER D'ACTIVITÉS EST UN REGROUPEMENT DE COMPORTEMENTS MALVEILLANTS CONNEXES QUI PARTAGENT DES OUTILS, DES TECHNIQUES OU UNE INFRASTRUCTURE COMMUNS, ET QUI SONT SUIVIS PAR CROWDSTRIKE LORSQU'IL N'Y A PAS ENCORE ASSEZ DE PREUVES POUR ATTRIBUER L'ACTIVITÉ À UN CYBERADVERSAIRE SPÉCIFIQUE.

Agents éphémères recrutés par Telegram

Depuis l'invasion à grande échelle de l'Ukraine par la Russie en février 2022, Moscou a de plus en plus recours à des tactiques de guerre hybride, incluant notamment le sabotage, contre l'Ukraine et ses alliés européens. En 2024 et 2025, de nombreux cas de sabotage liés à la Russie ont été signalés dans toute l'Europe. En réponse, l'UE a sanctionné les membres de l'unité 29155 du GRU russe pour leurs tentatives de déstabilisation, y compris les cyberattaques[13].

Les services spéciaux russes s'appuient de plus en plus sur des agents éphémères pour mener des opérations de subversion et de sabotage. Les « agents éphémères » sont des opérateurs recrutés par un service de renseignement, souvent pour une tâche spécifique de faible importance, dans l'idée qu'ils sont remplaçables. L'utilisation d'agents éphémères renforce la dénégation plausible, tout en étant peu coûteuse et relativement peu risquée. Elle s'est d'ailleurs probablement révélée utile à la lumière de l'expulsion massive de diplomates et d'agents du renseignement russes par les pays européens.

Les agents éphémères sont souvent recrutés et coordonnés sur Telegram par le biais d'intermédiaires criminels ou extrémistes, ce qui brouille toute tentative d'attribuer clairement les opérations à un commanditaire[14]. Depuis octobre 2024, RENAISSANCE SPIDER agit en tant qu'intermédiaire sous le prétexte de mener des opérations au nom du fournisseur VaaS *Fire Cells Group*.

Cibler les alliés ukrainiens

Les cybercriminels alliés de la Russie ont également ciblé des entités européennes pour leur soutien public à l'Ukraine. Par exemple, en mars 2022, RepeatingUmbra a manifesté un regain d'intérêt pour le ciblage d'entités allemandes et baltes, possiblement en raison du soutien que ces pays ont apporté à l'égard du conflit. Parallèlement, entre fin mars et mai 2022, PRIMITIVE BEAR a temporairement élargi ses cibles, passant de l'Ukraine à des entités gouvernementales en Lettonie, en Moldavie et en Lituanie, probablement en réponse au soutien public qu'ils ont exprimé à Kiev immédiatement après l'invasion[15].

Bien que d'autres gouvernements européens pro-ukrainiens aient également été ciblés, vraisemblablement en réaction partielle à leur soutien à l'Ukraine, CrowdStrike Intelligence estime que ces campagnes plus larges sont principalement motivées par des besoins permanents en matière de collecte de renseignement (voir la section *Activité associée à la Russie* à la page 26).

---

13 https://www.economist.com/graphic-detail/2025/07/22/russian-sabotage-attacks-surged-across-europe-in-2024

14 https://www.tv4.se/artikel/5vLIzItKYKnriPm0uJvd1N/saepo-larmar-vaervar-missbrukare-foer-att-utfoera-sabotage-i-sverige
https://www.abw.gov.pl/pl/informacje/2662,Dzialal-na-rzecz-obcego-wywiadu-przeciwko-RP-21-lipca-br-Kolumbijczyk-uslyszal-z.html
https://dossier.center/gru-guide/

15 https://eng.lsm.lv/article/politics/diplomacy/latvian-officials-immediately-condemn-putins-ukraine-invasion.a445051/
https://web.archive.org/web/20220507122804/https://www.bbc.com/ukrainian/features-61155192
https://www.eurointegration.com.ua/rus/news/2022/04/18/7137985/
https://www.delfi.lt/a/89541661

Cyberactivité associée à la Corée du Nord visant l'Ukraine

Tout au long de 2024 et 2025, la Corée du Nord a renforcé ses liens avec la Russie, en offrant un soutien diplomatique, économique et militaire lors de l'invasion de l'Ukraine par la Russie. L'alliance a atteint son apogée en octobre 2024, lorsque la Corée du Nord a déployé des troupes en Russie pour l'aider dans ses opérations militaires en Ukraine. En échange de son soutien militaire, la Russie aurait fourni à la Corée du Nord des équipements de défense aérienne avancés, des missiles antiaériens et des systèmes de guerre électronique[16].

Le soutien militaire croissant apporté par la Corée du Nord à la Russie coïncide avec le ciblage des entités de défense européennes par LABYRINTH CHOLLIMA en août 2024 et mai 2025, ainsi qu'avec le ciblage des entités diplomatiques européennes par VELVET CHOLLIMA entre mars et août 2025. Ces campagnes ont probablement été motivées par les besoins de la Corée du Nord en matière de renseignement militaire liés à la guerre en Ukraine[17].

Depuis le renforcement de leur alliance, la Corée du Nord et la Russie ont promis de collaborer plus étroitement sur les questions militaires, y compris dans le domaine cyber. Les dirigeants des agences de renseignement de chaque pays se sont également rencontrés à plusieurs reprises. Un rapport de juin 2025 affirmait que les deux parties cherchaient à conclure un accord de partage de renseignements[18].

Les cyberadversaires associés à la Russie se concentrent sur l'Ukraine

Au cours de la période visée par le rapport, les opérations liées à la Russie visant l'Europe ont porté presque exclusivement sur le soutien aux objectifs de la Russie, à savoir assurer le contrôle de la Russie sur les territoires annexés de l'est de l'Ukraine, assurer la neutralité politique et militaire de l'Ukraine vis-à-vis de l'OTAN et établir un gouvernement favorable à la Russie en Ukraine.

Depuis 2022, au moins deux opérations destructrices liées à la Russie et visant principalement des entités ou des capacités ukrainiennes ont atteint des entités en dehors de l'Ukraine, démontrant ainsi le risque d'effets sur d'autres entités européennes[19]. L'une d'entre elles a entraîné des dommages collatéraux, tandis que l'autre a intentionnellement visé la Pologne, dont le gouvernement soutient l'Ukraine.

À moins que le soutien occidental à l'Ukraine ne change de manière significative, notamment si les forces militaires occidentales s'impliquent directement dans des opérations contre les forces russes, il est peu probable que les cybercriminels russes mènent des attaques destructrices contre des entités non ukrainiennes en Europe. Cependant, CrowdStrike Intelligence estime que le gouvernement russe acceptera probablement le risque de dommages collatéraux mineurs subis par des entités en dehors de l'Ukraine, résultant de cyberopérations visant les capacités militaires ukrainiennes.

16 https://assets.korearisk.com/uploads/2025/05/Unlawful-Military-Cooperation-including-Arms-Transfers-between-North-Korea-and-Russia-MSMT_2025_1-1.pdf

17 https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/

18 https://www.dailynk.com/english/n-korea-uses-moscow-security-meeting-to-advance-intelligence-cooperation-with-russia/

19 https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-inukraine-and-poland/

RETOMBÉES DES CONFLITS AU MOYEN-ORIENT

Les conflits cinétiques au Moyen-Orient, en particulier entre Israël et le Hamas, ont été les principaux moteurs des cyberopérations soutenues par l'Iran et du cyberactivisme pro-iranien envers les entités européennes. Bien que la cyberactivité iranienne se soit principalement concentrée sur les entités basées en Israël, les relations diplomatiques tendues entre l'Iran et les pays européens ont conduit un nombre restreint de cybercriminels liés à l'Iran à cibler des entités européennes. Les cyberadversaires liés à l'Iran ont mené diverses opérations dans la région, notamment des opérations d'espionnage, de « hack and leak » et des campagnes destructrices. Alors que les tensions entre Israël et l'Iran restent palpables, les cyberadversaires liés à l'Iran continueront probablement à cibler Israël et ses alliés occidentaux impliqués dans le conflit par le biais d'efforts d'usurpation d'identité et de campagnes de harponnage (spear phishing).

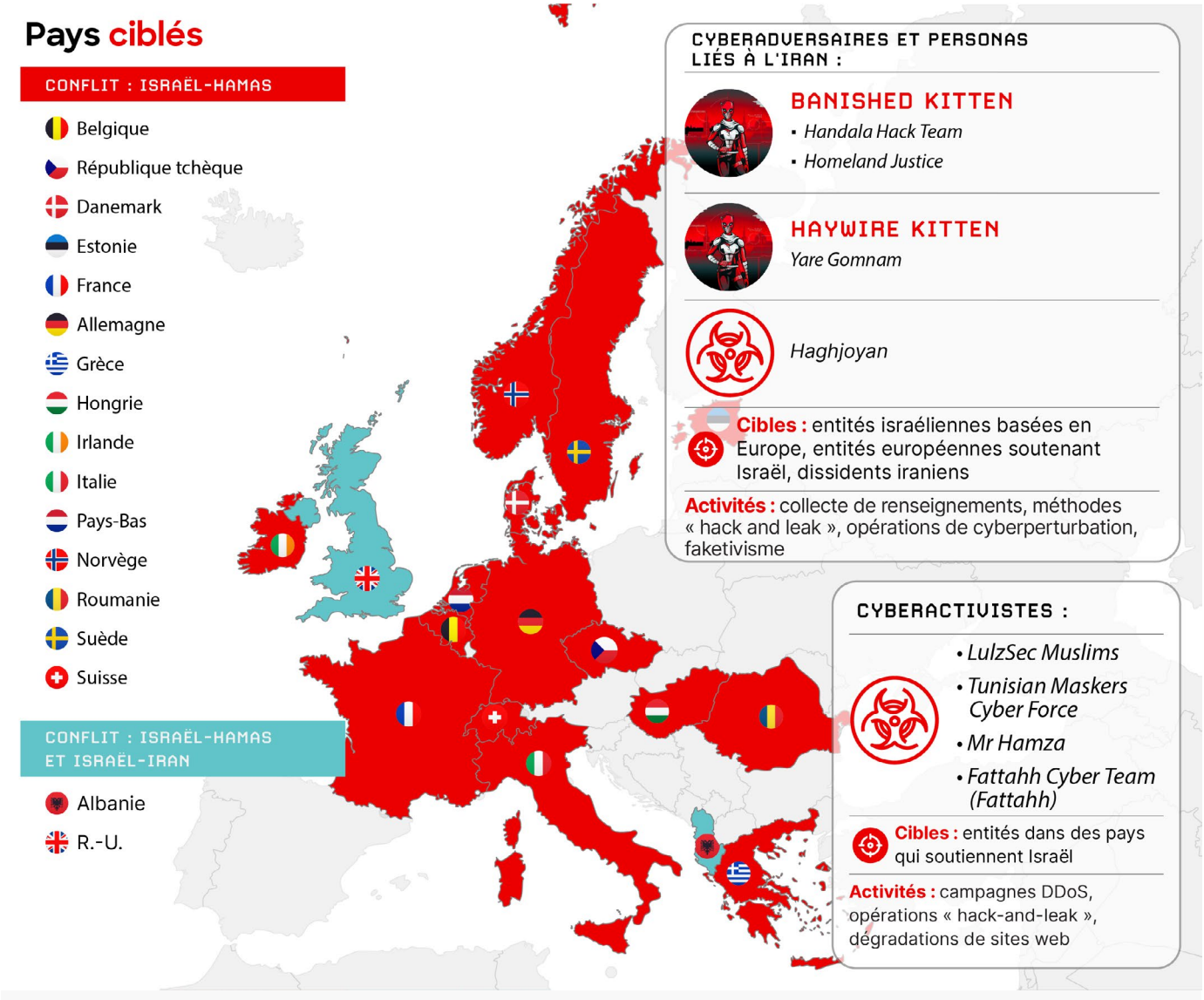


Figure 7. Activité associée à l'Iran et retombées cyberactivistes des conflits au Moyen-Orient

Opérations de collecte de renseignements

Entre la fin du mois de juillet et la mi-août 2025, des campagnes de harponnage (spear phishing), presque certainement menées par un cybercriminel lié à l'Iran et affilié au Corps des gardiens de la révolution islamique (CGRI), ont ciblé un établissement universitaire basé au Royaume-Uni, probablement dans le but de collecter des renseignements. Le cyberadversaire aurait utilisé des messages à thème professionnel pour inciter les victimes à télécharger et à exécuter le logiciel malveillant *AIDente*. Cette opération a coïncidé avec la montée des tensions entre le Royaume-Uni et l'Iran au sujet des négociations nucléaires, ainsi qu'avec la décision de l'Allemagne, de la France et du Royaume-Uni (connus collectivement sous le nom d'E3) d'activer le mécanisme de « snapback » rétablissant les sanctions contre l'Iran à la fin du mois d'août 2025. Bien qu'il soit peu probable que l'Iran mène des opérations ouvertement perturbatrices ou destructrices pendant les négociations, le pays reste vraisemblablement concentré sur la collecte de renseignements alors que le processus de rétablissement des sanctions se poursuit[20].

Opérations de type « hack-and-leak »

Depuis 2024, les cybergroupes liés à l'Iran ont intensifié leurs opérations de « hack-and-leak » sous le prétexte d'agir au nom de faux profils de cyberactivistes (alias « faketivistes »), en ciblant des entités israéliennes ou des entités dans des pays qui soutiennent publiquement Israël. Cette tactique s'inscrit dans une logique de guerre asymétrique peu coûteuse, permettant à l'Iran de riposter, de déstabiliser ses cyberadversaires et de façonner la perception du public tout en maintenant la dénégation plausible et en évitant les conflits militaires conventionnels.

En juillet 2025, deux cybergroupes liés à l'Iran, le groupe de cyberactivistes pro-IRGC *Gomnaman Team* et le persona Handala Hack Team associé à *BANISHED KITTEN*, ont revendiqué la responsabilité d'opérations de type « hack-and-leak » visant un média d'opposition iranien basé au Royaume-Uni. Les groupes ont affirmé avoir divulgué les informations personnelles des employés ainsi que des e-mails et des fichiers sensibles. Cette action aurait été menée en réponse à la coopération du média avec les agences de renseignement israéliennes. Les revendications de la *Handala Hack Team* et de la *Gomnaman Team* en juillet 2025 s'inscrivent dans le cadre d'une campagne plus vaste d'opérations d'influence, probablement destinée à contrôler l'information et à réprimer les dissidents à l'extérieur de l'Iran, tout en sapant la confiance dans les médias d'opposition à un moment politiquement sensible pour le régime.

Opérations de cyberperturbation

En janvier 2024, le persona YareGomnam (alias Yare Gomnam Cyber Team), *probablement associé à* HAYWIRE *KITTEN*, a revendiqué la responsabilité d'une attaque DDoS contre un organe de presse du gouvernement néerlandais et le site web anglophone d'une organisation liée à la défense. *YareGomnam* a déclaré que les attaques DDoS étaient menées en réponse à la participation des Pays-Bas à la coalition dirigée par les États-Unis, responsable de frappes militaires contre des sites houthis au Yémen en janvier 2024. Cependant, l'information diffusée à la mi-janvier 2024 et selon laquelle un ingénieur néerlandais avait participé à un sabotage du programme nucléaire iranien en 2007 a peut-être également influencé les priorités de ciblage du groupe.

ACTIONS DES CYBERACTIVISTES AXÉES SUR LES CONFLITS

Entre janvier 2024 et septembre 2025, les conflits mondiaux (y compris ceux entre la Russie et l'Ukraine, Israël et le Hamas et Israël et l'Iran) ont engendré des actions cyberactivistes généralisées, notamment des attaques DDoS, des opérations de « hack-and-leak », des dégradations de sites web et des campagnes destructrices. Bien que ces attaques aient principalement visé des entités au sein des pays ou des régions activement engagés dans les conflits, certaines actions ont eu un impact sur les nations européennes. Les attaques cyberactivistes ont ciblé des pays perçus comme soutenant l'Ukraine ou Israël, ainsi que des entités européennes dans les secteurs de la finance, des télécommunications, du gouvernement, de l'énergie, de la logistique, des forces de l'ordre et des infrastructures critiques.

20 https://www.iranintl.com/en/202507268188

Entité cyberactiviste	Activité régionale
BOUNTY JACKAL	Entre janvier 2024 et septembre 2025, le cyberadversaire et cyberactiviste pro-russe BOUNTY JACKAL a mené des campagnes DDoS étendues et quasi quotidiennes contre des entités européennes en réponse à un soutien militaire ou financier à l'Ukraine ou à des opinions russophobes perçues. Le ciblage du cyberadversaire était fort probablement opportuniste et le kit d'outils *DDoSia*, dédié aux attaques DDoS, a été utilisé pour coordonner ses campagnes avec son réseau mondial de bénévoles. En plus du soutien DDoS fourni par les bénévoles, BOUNTY JACKAL a collaboré avec des cyberactivistes partageant les mêmes idées, notamment *UserSec*, *People's Liberation Front*, *Cyber Army of Russia (CARR), HackNeT* et *Z-Alliance* à plusieurs reprises,pour cibler des entités européennes dans les domaines de la finance, des télécommunications, des pouvoirs publics, de l'énergie, de la logistique, des forces de l'ordre et des infrastructures critiques, ainsi qu'une alliance militaire occidentale. De nombreuses campagnes BOUNTY JACKAL ont presque certainement été programmées pour coïncider avec les élections ou les manifestations en cours en Europe. Cela met en évidence les motivations anti-UE plus vastes du cyberadversaire (tout en continuant de cibler les pays perçus comme pro-Ukraine) et son désir d'attirer l'attention sur les campagnes en synchronisant les attaques avec des événements majeurs se déroulant dans la géographie cible.
Cyber Army of Russia (alias *CARR*)	Tout au long de l'année 2024, le cyberactiviste pro-russe *CARR* a affirmé avoir mené de nombreuses campagnes DDoS contre des entités européennes en représailles au soutien militaire et financier occidental à l'Ukraine. La *CARR* a également assuré avoir mené plusieurs campagnes aux côtés de BOUNTY JACKAL et de *Z-Alliance*, y compris les attaques DDoS d'avril 2024 contre les sites web d'entités gouvernementales, énergétiques et logistiques espagnoles. En septembre et octobre 2024, la *CARR* a revendiqué la responsabilité de la compromission de systèmes de contrôle industriels (ICS) en Pologne, en France, aux États-Unis et à Taïwan. En décembre 2024, la *CARR* a supprimé son canal Telegram public et a annoncé que les membres du groupe continueraient à mener des attaques DDoS sous le nom de *Z-Alliance*.
Fattahh Cyber Team (alias *Fattahh*)	En janvier 2024, le groupe de cyberactivistes pro-IRGC *Fattahh Cyber Team* a dégradé un site web de fabrication néerlandais avec des messages pro-Houthis. Bien que le groupe soit encore actif en octobre 2025, cet incident est le seul cas connu ayant ciblé l'Europe.
LulzSec Muslims	Jusqu'en août 2024 au minimum, le groupe cyberactiviste pro-palestinien et pro-islam *LulzSec Muslims* a affirmé avoir ciblé de nombreuses entités dans le monde, y compris des pays d'Europe occidentale, du Nord et du Sud, mais aucun en Europe de l'Est à part l'Ukraine. L'activité a consisté en des opérations de type « hack-and-leak », des attaques DDoS et la dégradation de sites web menées contre des entités dans des pays que le groupe perçoit comme soutenant directement ou indirectement Israël dans le conflit avec le Hamas.
Mr Hamza	En janvier 2025, le cyberactiviste pro-islam *Mr Hamza* a affirmé avoir mené des attaques DDoS contre la police fédérale et nationale, des entités chargées de la sécurité et du renseignement, un ministère de la Défense et des services militaires en Belgique, en République tchèque, au Danemark, en Estonie, en Allemagne, en Hongrie, en Irlande, en Italie, aux Pays-Bas, en Norvège, en Roumanie, en Suède et aux États-Unis. Cette activité a été motivée par le soutien perçu de ces pays à Israël.
Tunisian Maskers Cyber Force	De mai à juin 2025, le groupe cyberactiviste pro-palestinien *Tunisian Maskers Cyber Force* a mené sa campagne #Dark_Pulse_V2, ciblant des entités basées au Royaume-Uni, en réponse au soutien du pays à Israël dans le conflit entre Israël et le Hamas. Le groupe a affirmé avoir mené des attaques DDoS contre des entités financières, de services professionnels, d'hôtellerie et de vente au détail basées au Royaume-Uni et partagé des liens vers des outils de surveillance de sites web pour prouver le succès de la campagne. Dans le cadre de cette campagne, la *Tunisian Maskers Cyber Force* a menacé de divulguer des e-mails provenant d'une entité gouvernementale non spécifiée (possiblement basée en Europe) et des données prétendument obtenues d'une entité de services professionnels précédemment ciblée. Cependant, comme le groupe cyberactiviste n'a pas fait mention de ces cybermenaces par la suite ou publié les données sur ses canaux de réseaux sociaux connus, on ne sait pas si elles ont été mises à exécution.
Z-Alliance (alias *Z-Pentest*)	Fin 2024 et début 2025, *Z-Alliance* a affirmé avoir compromis les systèmes de contrôle et d'acquisition des données (SCADA) d'au moins six entités aux États-Unis, en France, en Allemagne, en Ukraine et à Taïwan et a revendiqué la responsabilité de la compromission de plusieurs ICS en France, en Grèce, en Lituanie, en Italie, en Pologne, en Espagne et en Suède. Ces intrusions étaient motivées par les sentiments pro-russes, anti-ukrainiens et anti-occidentaux du groupe et étaient probablement destinées à gagner en notoriété.

Tableau 1. Activité des groupes cyberactivistes contre des cibles européennes

Les conflits en cours et émergents continueront très probablement à motiver les actions cyberactivistes, à la fois dans les zones de conflit et à l'échelle mondiale, car les cyberactivistes cherchent à mener des actions de représailles motivées par le soutien perçu à l'Ukraine, à répandre leurs idéologies ou à tirer parti de la couverture médiatique pour attirer l'attention. Cette évaluation est réalisée avec un degré de confiance élevé sur la base des actions de cyberactivistes observées en réponse aux conflits mondiaux depuis au moins 2022.

Cyberactivité des États-nations non axée sur les conflits

Bien que des conflits majeurs aient modifié les priorités de ciblage et le rythme opérationnel de certains cyberadversaires à la solde d'États, les facteurs sous-jacents du cyberespionnage restent constants. La demande persistante des États-nations en matière de renseignement, dans le but d'orienter les politiques nationales, de soutenir les entreprises publiques ou de financer les régimes autoritaires, garantit la poursuite d'une série de cyberopérations.

ACTIVITÉ ASSOCIÉE À LA RUSSIE

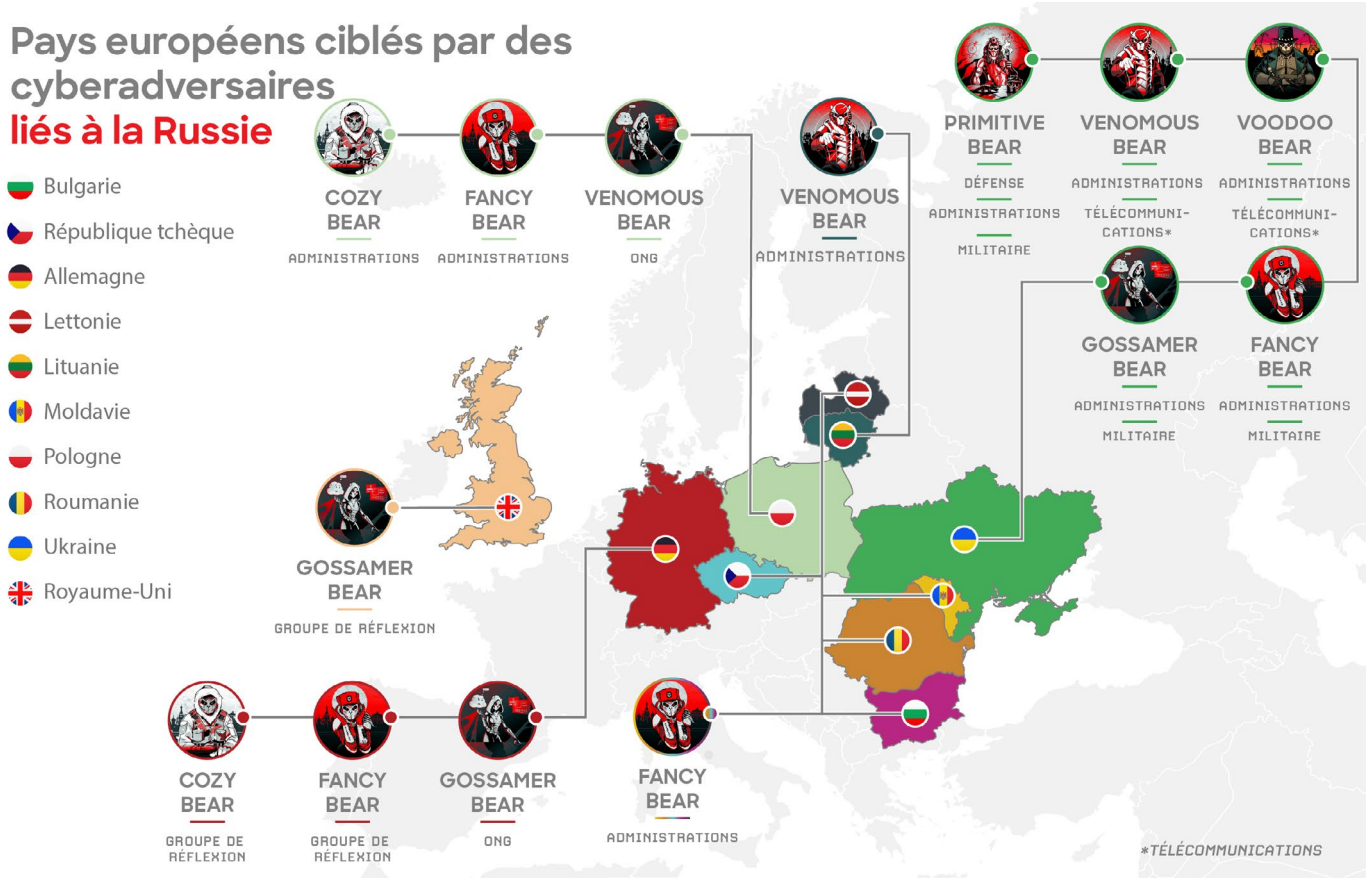


Figure 8. Ciblage des pays européens par des acteurs associés à la Russie

Bien que la plupart des cyberadversaires et cybercriminels à la solde d'États et associés à la Russie se concentrent sur l'Ukraine, le ciblage stratégique d'autres États européens, en particulier les pays membres de l'OTAN, reste une priorité.

Les modèles de ciblage des cyberadversaires associés à la Russie en matière de collecte de renseignements, observés dans différents secteurs, s'alignent sur les objectifs politiques et militaires de la Russie en Europe. Pour soutenir davantage l'effort de guerre de la Russie en Ukraine, ces cyberadversaires collectent des renseignements stratégiques, opérationnels et tactiques, permettant à la Russie de suivre l'aide militaire apportée à l'Ukraine. Le ciblage d'entités est également fortement susceptible d'inciter la Russie à collecter des renseignements politiques pour exploiter les divisions internes qui sapent le soutien européen à l'Ukraine et font voler en éclats la cohésion de l'OTAN et l'UE.

Les cyberopérations en lien avec la Russie menées contre des entités dans des pays européens non membres de l'OTAN servent probablement des objectifs stratégiques distincts. Pour les entités des pays alliés de l'Occident, ces intrusions visent sûrement principalement à collecter des renseignements et à surveiller les relations avec l'UE et l'OTAN. Pour les pays qui cherchent activement à rejoindre ces institutions, ces cybercriminels ont probablement l'intention de surveiller et potentiellement de perturber leur adhésion et de réaffirmer la sphère d'influence régionale de la Russie.

Ces opérations illustrent l'intégration par la Russie de ses campagnes de collecte de renseignements et d'influence, centrées sur les activités de l'OTAN, les relations énergétiques et l'élaboration des politiques. La persistance des cybercriminels et le volume élevé de leurs campagnes indiquent que la Russie alloue des ressources de haut niveau à ces campagnes et donne la priorité aux opérations européennes de collecte de renseignements et d'influence.

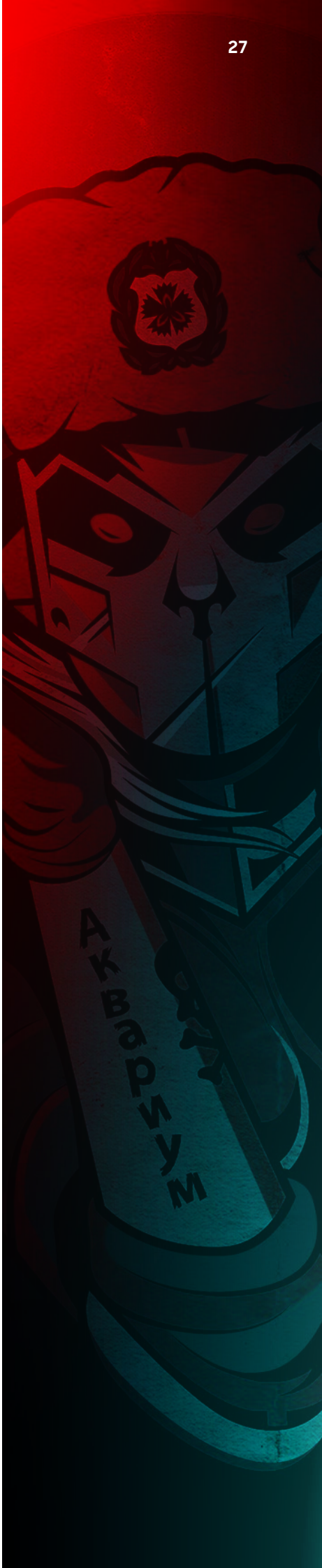
Ciblage du secteur gouvernemental européen

FANCY BEAR, un cyberadversaire associé au GRU, a maintenu un rythme opérationnel élevé contre les entités gouvernementales européennes. Tout au long de l'année 2024, le cyberadversaire a exploité les vulnérabilités et mené des campagnes de diffusion de logiciels malveillants ciblant probablement des entités gouvernementales dans des pays européens, notamment la Pologne, la Moldavie, la République tchèque, la Bulgarie et la Lettonie. Tout au long de l'année 2025, FANCY BEAR a continué à exploiter les vulnérabilités des clients de messagerie web tels que Zimbra, Roundcube et MDaemon pour récupérer les données d'authentification ainsi que pour rediriger et exfiltrer les e-mails.

FANCY BEAR a très certainement ciblé des entités gouvernementales tchèques à l'aide d'appâts liés à la coopération avec l'OTAN et a exploité les vulnérabilités NTLM contre des entités gouvernementales roumaines, mettant en évidence les objectifs persistants du cyberadversaire en matière de collecte de renseignements. Les États membres de l'OTAN et les pays qui ont conclu des partenariats formels et des accords de coopération avec l'OTAN resteront une cible principale à long terme pour les opérations futures de FANCY BEAR.

Depuis octobre 2020, le cyberadversaire COZY BEAR, associé au Service de renseignements extérieurs de la Fédération de Russie (SVR), poursuit sa campagne DiplomaticOrbiter ciblant les ministères européens des Affaires étrangères (MFA) afin de collecter des renseignements conformes aux objectifs de renseignement diplomatique et stratégique du SVR. Le cyberadversaire a repris ses activités en janvier 2025, au cours desquelles il a très probablement utilisé des e-mails de harponnage (spear phishing) pour diffuser son nouveau téléchargeur personnalisé, *BoomTwins*. En octobre 2024, COZY BEAR a sans doute ciblé des entités gouvernementales européennes lors d'une campagne de phishing distincte à grande échelle. Le cyberadversaire a distribué des fichiers RDP malveillants et enregistré plus de 180 domaines imitant des ministères de la Défense, des forces armées et des groupes de réflexion.

Entre 2023 et 2025, VENOMOUS BEAR a déployé son implant *CoreTech* et son *RAT Kazuar* dans des campagnes menées contre plusieurs entités gouvernementales d'Europe de l'Est, y compris celles en Ukraine. Depuis l'invasion à grande échelle de la Russie, CrowdStrike Intelligence a observé une activité restreinte de la part de VENOMOUS BEAR à l'encontre des pays d'Europe de l'Est, y compris l'Ukraine. Cependant, CrowdStrike Intelligence estime avec un degré de confiance modéré que VENOMOUS BEAR a ciblé et continuera de cibler des entités gouvernementales d'Europe de l'Est, probablement en raison des exigences habituelles du cyberadversaire en matière de collecte de renseignements, qui ont été établies en même temps que ses capacités de collecte de renseignements, avant février 2022.



Tout au long de 2024 et 2025, le cluster d'activités RepeatingUmbra, en lien avec la Russie, a ciblé des individus et des entités en Europe de l'Est par le biais de campagnes intensives de phishing d'identifiants et de diffusion de logiciels malveillants. Le cluster d'activités a mené de vastes opérations de phishing d'identifiants à l'encontre de personnes et d'entités publiques polonaises, lituaniennes, lettones et ukrainiennes, ainsi que de personnes russophones.

De plus, RepeatingUmbra a continué d'utiliser des documents malveillants pour diffuser divers chargeurs tels que *Pryatki*, aboutissant finalement au déploiement d'un beacon *Cobalt Strike* contre des entités d'Europe de l'Est. Il est fort probable que RepeatingUmbra continue à collecter des renseignements tout en menant des opérations d'influence, telles que la compromission des comptes de réseaux sociaux de politiciens et le blanchiment de données volées par des groupes cyberactivistes, pour déstabiliser les pays d'Europe de l'Est.

En août et septembre 2025, un cybercriminel probablement lié à la Russie a mené des campagnes de phishing sur WhatsApp ciblant des entités et des individus en Moldavie, y compris un membre probable des forces armées moldaves. Le cybercriminel a détourné les fonctionnalités d'association d'appareils pour accéder aux comptes WhatsApp des victimes. En septembre 2025, le cybercriminel aurait utilisé l'application de messagerie Signal pour diffuser un lien vers un site web malveillant usurpant une véritable pétition liée au programme économique moldave. Le site web a incité les cibles à se connecter à WhatsApp pour « empêcher la fraude électorale ».

Toujours en septembre 2025, un autre cybercriminel probablement lié à la Russie a exploité la compromission opportuniste des serveurs Zimbra Collaboration pour collecter des e-mails. Le cybercriminel a indiqué que sa cible comprenait des entités gouvernementales, à but non lucratif, politiques et logistiques situées en Europe, en particulier en Moldavie. CrowdStrike Intelligence estime que ce cybercriminel non identifié recueille certainement des renseignements pour le compte du FSB.

Ciblage du secteur européen de la défense

En octobre 2024, COZY BEAR a tiré parti de l'usurpation de domaine, en utilisant des domaines enregistrés depuis au moins août 2024, dans le but probable de cibler une organisation internationale de défense ainsi que des entités gouvernementales et privées européennes et nord-américaines. De plus, en juillet 2025, les sanctions imposées par le gouvernement britannique à des membres de l'unité 26165 du GRU accusent ce groupe d'avoir accédé à des caméras de surveillance privées situées à proximité d'installations militaires, de ports, de postes frontaliers et d'autres infrastructures de transport dans plusieurs pays européens, dont la Moldavie. Cela met en évidence l'étendue des besoins de la Russie en matière de collecte de renseignements sur les cibles militaires et d'infrastructures critiques.

Le secteur européen de l'énergie utilisé dans le contenu d'appât

Lors d'une campagne menée en avril 2024, FANCY BEAR a utilisé des appâts sur le thème des énergies renouvelables, ce qui indique probablement que le secteur de l'énergie constitue une priorité importante pour la collecte de renseignements du RIS, en raison des lourdes sanctions imposées au secteur pétrolier et gazier russe. FANCY BEAR a eu recours à un sous-domaine pour diffuser un document-appât usurpant le « profil énergétique » de l'Autriche, attribué de manière frauduleuse à une organisation intergouvernementale du secteur de l'énergie.

En décembre 2023, l'Autriche importait 98 % de son gaz depuis la Russie[21]. La ministre autrichienne de l'Énergie a annoncé en février 2024 que le pays cherchait à mettre fin à son contrat d'importation avec Gazprom. Bien que la cible exacte de la campagne reste inconnue, l'appât indique que FANCY BEAR ciblait potentiellement des entités énergétiques européennes. L'opération démontre les objectifs de renseignement à long terme poursuivis par la Russie, portant sur les relations énergétiques européennes et sur l'élaboration des politiques dans ce domaine.

Ciblage du secteur européen des groupes de réflexion

Entre la fin de l'année 2023 et le 2e trimestre 2024, le groupe associé au FSB GOSSAMER BEAR a mené des campagnes de phishing d'identifiants contre des groupes de réflexion britanniques spécialisés dans les affaires internationales, la défense et la sécurité. Le cyberadversaire a probablement utilisé les données obtenues comme arme lors d'opérations d'influence de type « hack-and-leak » ultérieures. FANCY BEAR a également exploité les vulnérabilités NTLM contre une entité gouvernementale roumaine et probablement contre un groupe de réflexion allemand dans le cadre de ses opérations de collecte de renseignements. Parallèlement, la campagne DiplomaticOrbiter de COZY BEAR ciblait les groupes de réflexion occidentaux dans le cadre de sa collecte habituelle de renseignements.

AU COURS DE SA CAMPAGNE DE PHISHING D'OCTOBRE 2024, COZY BEAR A ENREGISTRÉ PLUS DE 180 DOMAINES USURPANT L'IDENTITÉ DE GROUPES DE RÉFLEXION ET D'ENTITÉS DE DÉFENSE, DÉMONTRANT LA PRIORITÉ PROBABLEMENT ACCORDÉE À LA SURVEILLANCE DES ENTITÉS OCCIDENTALES GOUVERNEMENTALES, TECHNOLOGIQUES, DE DÉFENSE ET À BUT NON LUCRATIF MAJEURES POUR LA COLLECTE DE RENSEIGNEMENTS STRATÉGIQUES.

Ciblage du secteur européen des médias et des ONG

GOSSAMER BEAR a ciblé des médias et des ONG européens par le biais de campagnes de « hack-and-leak », utilisant des documents volés comme arme pour ses opérations d'influence. De janvier à août 2025, GOSSAMER BEAR a continué ses opérations de phishing d'identifiants ciblant probablement des groupes de réflexion, des dissidents et des ONG en Europe et en Afrique. Conformément à l'attention historique du cyberadversaire portée aux « les organisations indésirables »,[22] en 2025, GOSSAMER BEAR a ciblé au moins une ONG œuvrant au renforcement des liens entre la société civile allemande et les pays d'Europe de l'Est.

Après le début du conflit entre Israël et le Hamas en octobre 2023, GOSSAMER BEAR a enregistré plusieurs domaines usurpant l'identité d'une entité européenne chargée de l'application de la loi afin de récupérer les identifiants Microsoft Outlook de personnes associées. Début février 2024, GOSSAMER BEAR a enregistré des domaines usurpant l'identité d'une entité européenne d'entraînement militaire axée sur l'Afrique, ce qui correspond à l'intérêt stratégique croissant de Moscou pour ce continent. La Russie s'est positionnée comme une alternative aux partenaires occidentaux pour l'Afrique, alors que les forces de l'UE et des États-Unis réduisent leur présence continentale. La collecte de renseignements et les opérations d'influence de GOSSAMER BEAR impliquent souvent des campagnes de « hack-and-leak » utilisant des documents volés comme arme contre des gouvernements, des médias, des groupes de réflexion et des ONG.

En janvier 2024, VENOMOUS BEAR a pris pour cible une ONG polonaise avec une nouvelle porte dérobée nommée *dcmd*. Cette action s'inscrivait dans les objectifs de renseignement à long terme du cyberadversaire et dans le cadre d'un ciblage accru des entités polonaises, probablement motivé par le rôle de la Pologne dans l'accueil de réfugiés ukrainiens et l'aide apportée à l'Ukraine.

21 https://www.reuters.com/markets/europe/austria-seeking-end-russian-gas-import-contract-energy-minister-says-2024-02-12/

22 La Russie désigne comme « indésirables » les organisations qu'elle perçoit comme une cybermenace étrangère pour les intérêts de l'État russe, interdisant à ces organisations de faire des affaires en Russie.

ACTIVITÉ ASSOCIÉE À L'IRAN

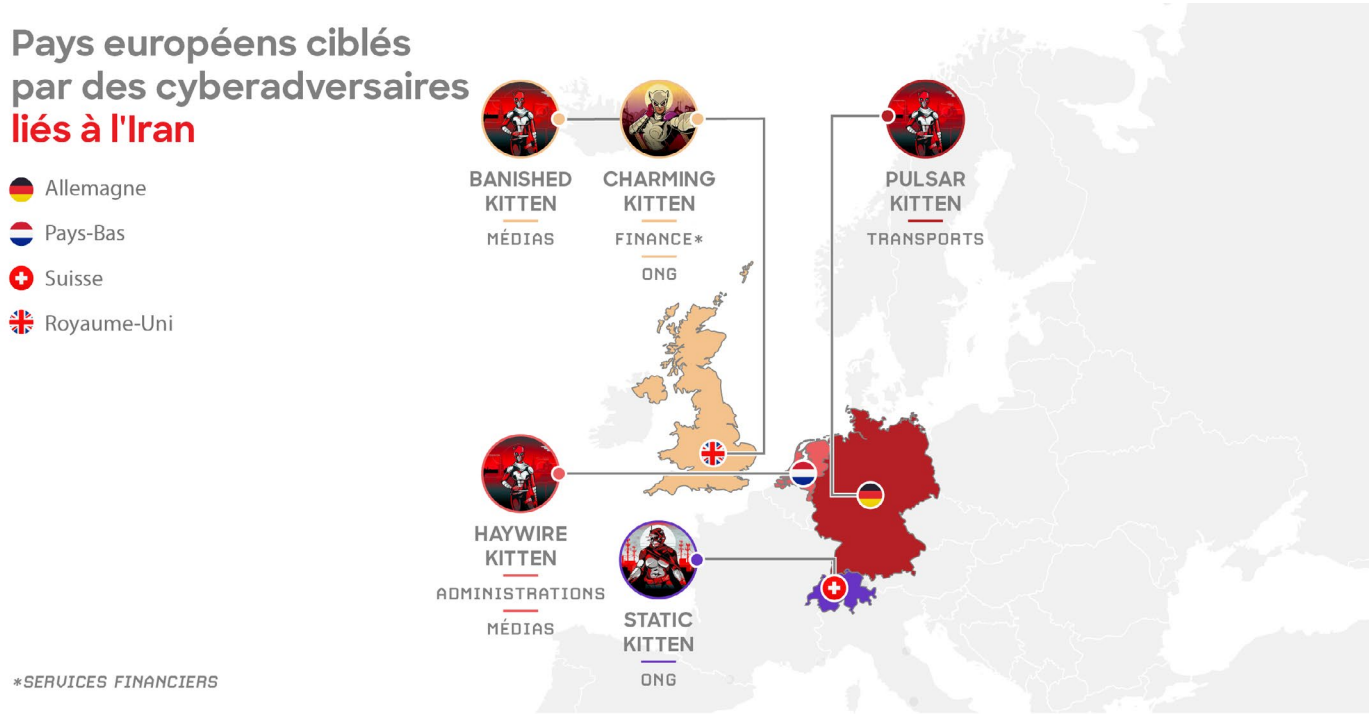


Figure 9. Ciblage des pays européens par des acteurs associés à l'Iran

Les cyberadversaires en lien avec l'Iran ont principalement ciblé Israël, ses alliés et d'autres cibles au Moyen-Orient en raison des tensions régionales actuelles. Cependant, ils ont également continué à collecter des renseignements auprès de cibles européennes, en particulier celles qui s'opposent aux intérêts de l'État iranien. Bien que l'Iran s'abstienne probablement de toute cyberactivité offensive perturbatrice ou destructrice pendant ses tentatives continues de reprendre les négociations nucléaires, les cybercriminels en lien avec l'Iran représentent toujours une cybermenace accrue pour les pays européens.

Fin août 2025, l'E3 a activé le mécanisme de « snapback » rétablissant les sanctions contre l'Iran[23]. L'Iran ne perçoit probablement pas les opérations de collecte de renseignements comme une cyberactivité ouvertement offensive, de sorte que l'activation du mécanisme de « snapback » conduira probablement les cyberadversaires en lien avec l'Iran à cibler spécifiquement les pays de l'E3 pour collecter des renseignements.

Ciblage du secteur gouvernemental européen

Les cyberadversaires en lien avec l'Iran ont systématiquement ciblé des entités gouvernementales européennes, en particulier celles qui s'opposent aux intérêts de l'État iranien. Entre janvier et mars 2025, un cybercriminel en lien avec l'Iran (non attribué de manière formelle) a vraisemblablement mené une campagne de harponnage (spear phishing) ciblant un représentant éminent du Parlement européen, originaire d'Allemagne, qui joue un rôle de premier plan dans le soutien aux groupes d'opposition iraniens.

La campagne s'est appuyée sur des appels vocaux et une ingénierie sociale élaborée. Le personnel du responsable politique allemand aurait reçu des messages et des appels téléphoniques de la part de cybercriminels inconnus se faisant passer pour un contact légitime associé à un groupe de réflexion basé aux États-Unis. Les cybercriminels auraient fini par compromettre un ordinateur portable du bureau du responsable politique, sur lequel ils auraient installé un logiciel malveillant. Bien que les cybercriminels aient réussi à compromettre les systèmes de la cible, les mesures de sécurité du Parlement européen auraient empêché tout vol de données sensibles.

Le responsable politique allemand a probablement été choisi comme cible en raison de sa position politique et de sa proximité professionnelle avec les dissidents iraniens.

23 https://www.iranintl.com/en/202507268188

Ciblage du secteur européen des services financiers

En mai 2024, CHARMING KITTEN a ciblé des entités financières basées au Royaume-Uni avec des campagnes de phishing destinées à collecter des renseignements. Le cyberadversaire a adapté ses opérations en utilisant une infrastructure usurpée, une ingénierie sociale spécifique à sa cible et des sites web usurpant l'identité d'entités légitimes. Il a également systématiquement abusé de services légitimes tels que Microsoft OneDrive pour diffuser son logiciel malveillant personnalisé.

Ciblage du secteur européen des transports

À la mi-juillet 2025, PULSAR KITTEN a probablement mené une opération de harponnage (spear phishing) visant la branche allemande d'une société de transport basée aux États-Unis. Le cyberadversaire a eu recours à des offres d'emploi factices liées à l'aviation pour diffuser son logiciel malveillant sophistiqué *SilkySand* via le service légitime de partage de fichiers ONLYOFFICE. Il a mené cette opération dans un contexte de tensions croissantes entre l'Iran et l'Allemagne, en particulier à la suite de déclarations controversées sur le conflit israélo-iranien et de menaces européennes de réimposer des sanctions. L'opération a servi à la fois des objectifs politiques et de collecte de renseignements, faisant avancer les intérêts de contre-espionnage de l'Iran en Europe occidentale. PULSAR KITTEN a déjà usurpé des sites web de constructeurs automobiles allemands, mais n'avait encore jamais été observé à cibler des entités du secteur des transports.

Du début au milieu de l'année 2025, des cyberadversaires en lien avec l'Iran et affiliés à l'IRGC (y compris PULSAR KITTEN, IMPERIAL KITTEN, un cybercriminel en lien avec l'Iran [non attribué de manière formelle] et HAYWIRE KITTEN) ont probablement usurpé ou ciblé des entités basées en Allemagne.

Ciblage du secteur européen des ONG

En août 2025, STATIC KITTEN a mené une campagne de collecte de renseignements ciblant la branche d'Asie du Sud-Est d'une ONG basée en Suisse. Le cyberadversaire a probablement obtenu un accès initial à l'entité par le biais d'une compromission du serveur web ; cependant, cela n'a pas été confirmé par l'ONG.

Après s'être introduit, STATIC KITTEN a utilisé un compte de service compromis pour se déplacer latéralement dans le réseau. À l'aide de son accès étendu, le cyberadversaire a invoqué PowerShell pour télécharger une charge active malveillante à partir d'une adresse IP contrôlée par le cyberadversaire. Enfin, il a tenté d'écrire des ruches du registre sur disque et de collecter des identifiants, presque certainement en préparation d'une exfiltration.

HAYWIRE KITTEN : une probable campagne de phishing vise l'Europe occidentale

De décembre 2024 à juillet 2025 au moins, HAYWIRE KITTEN a probablement mené une vaste campagne de phishing exploitant l'image de Microsoft et ciblant des organisations occidentales de divers secteurs. L'opération se concentrait sur des entités issues des secteurs de la technologie, des énergies renouvelables, de la fabrication et de l'hôtellerie. Certaines preuves suggèrent que le cyberadversaire a ciblé des entités en France, en Allemagne, en Espagne, en Suisse et aux États-Unis. Le groupe a déployé des pages de collecte d'identifiants exploitant l'image de Microsoft et a probablement utilisé des e-mails de harponnage (spear phishing) avec une pièce jointe PDF contenant une demande de devis (RFQ) pour un espace événementiel situé en Allemagne, qui accueille divers salons professionnels et conférences.

Le ciblage par HAYWIRE KITTEN des entités issues des secteurs de la technologie, des énergies renouvelables et de l'hôtellerie reflète les intérêts stratégiques de l'Iran et suit les modèles de ciblage historiques contre l'Occident. Le cyberadversaire a probablement mené cette opération pour collecter des renseignements.

Cette activité s'inscrit également dans le mode opératoire de HAYWIRE KITTEN, axé sur le ciblage d'entités occidentales, et met en évidence sa capacité à développer une infrastructure de domaines. CrowdStrike Intelligence estime que HAYWIRE KITTEN contrôle probablement l'infrastructure associée à cette campagne de phishing exploitant l'image de Microsoft. Toutefois, il reste incertain que cette infrastructure ait été effectivement mise en œuvre et opérationnalisée avec succès.

ACTIVITÉ ASSOCIÉE À LA CHINE

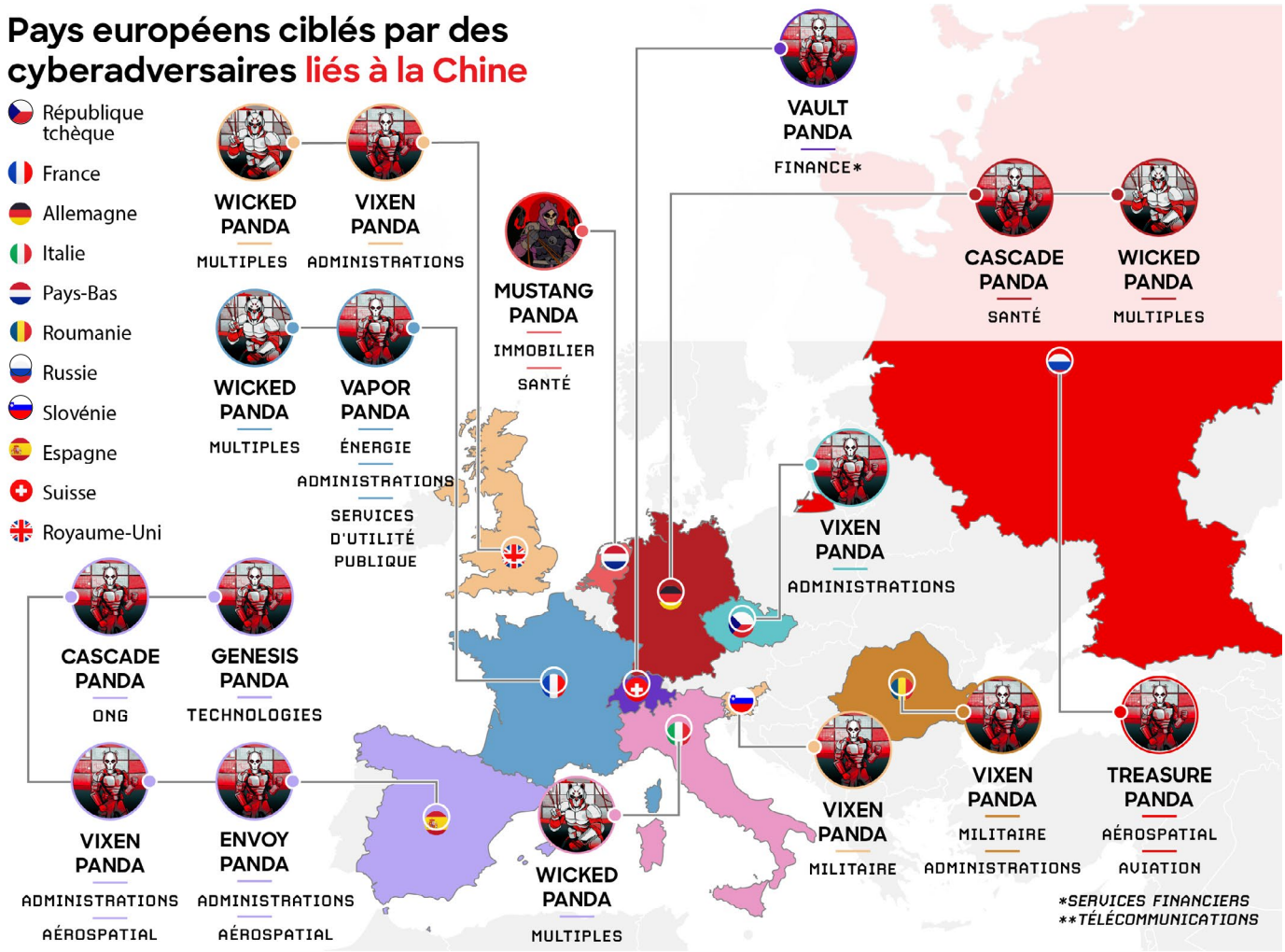


Figure 10. Pays européens ciblés par les cyberadversaires présentant des liens avec la Chine

L'UE, l'un des plus grands partenaires commerciaux et l'une des principales destinations d'investissement de la Chine, joue un rôle clé dans les ambitions chinoises visant à renforcer l'intégration régionale par le biais du commerce en Asie centrale et en Europe de l'Est. La cyberactivité de la Chine visant l'Europe est restée systématiquement axée sur la collecte probable de renseignements pour éclairer l'engagement politique et économique de Pékin dans la région. Pékin cherche également à soutenir les priorités stratégiques du gouvernement dans un contexte de turbulences dans les relations entre l'UE et les États-Unis en matière de commerce et de défense. Les cybercriminels en lien avec la Chine continuent de cibler des entités gouvernementales, de défense, industrielles et aérospatiales européennes.

Les opérations menées par ces cybercriminels visant l'Europe ont probablement pour but de soutenir les priorités stratégiques de la Chine, telles que la relance de l'économie et la prévention de l'ingérence étrangère. La Chine vise également à devenir autonome dans des domaines scientifiques et technologiques clés, d'autant plus que l'accès du pays aux technologies de pointe conçues en dehors de la Chine est de plus en plus restreint.

Ciblage du secteur européen de la santé et des biotechnologies

De multiples cyberadversaires en lien avec la Chine continuent de cibler avec insistance le secteur de la santé et des biotechnologies, qui est l'un des secteurs les plus visés en Europe. En avril 2024, CASCADE PANDA a tenté de déployer le logiciel malveillant *WinDealer* au sein d'une entité de biotechnologie allemande ayant des activités en Chine, démontrant ainsi l'intérêt persistant du cyberadversaire pour les entités ayant une présence transfrontalière.

Les opérations de MUSTANG PANDA ont eu un impact sur plusieurs établissements de soins de santé européens en 2023 et 2024. Ces opérations permettent de déployer des logiciels malveillants modulaires diffusés par USB, notamment l'infecteur de clé USB *LubanBall*, les chargeurs *Tangram* et *Foregram*, ainsi que l'outil d'accès à distance (RAT) *LingerRAT*. Les capacités du cyberadversaire n'ont cessé d'évoluer, et il a récemment déployé l'infecteur *LubanBall* dans un établissement de soins de santé basée aux Pays-Bas en août 2024.

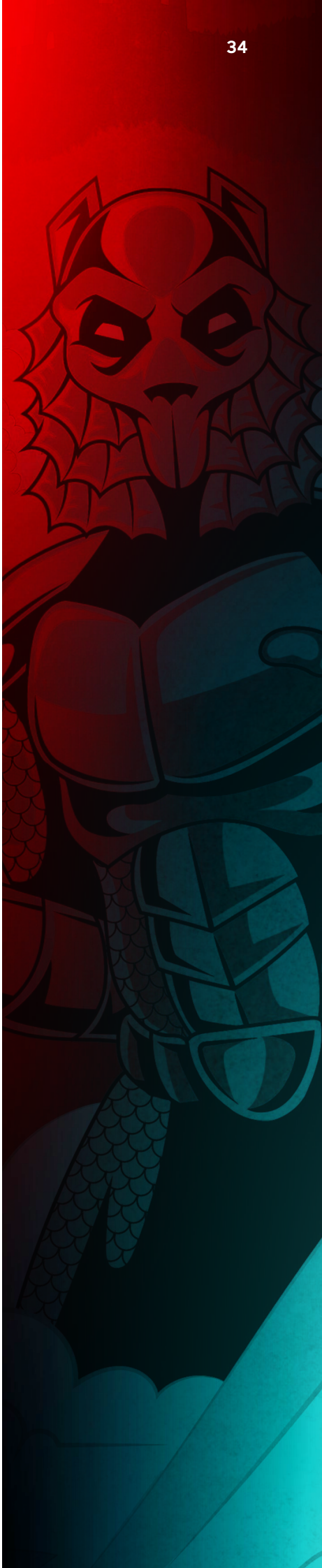
Les cybercriminels en lien avec la Chine ciblent probablement ce secteur pour collecter des renseignements, obtenir des informations personnelles et s'emparer de la propriété intellectuelle associée à la recherche et au développement de vaccins et de technologies biomédicales. Ce modèle de ciblage s'aligne sur l'intérêt stratégique de la Chine à faire progresser ses capacités biotechnologiques et à comprendre les innovations médicales occidentales qui sont essentielles à la sécurité sanitaire nationale.

Ciblage du secteur gouvernemental et de la défense en Europe

Au cours de la période considérée, VIXEN PANDA a été la cybermenace la plus prolifique pour les entités gouvernementales et de défense en Europe. De début 2024 à début 2025, VIXEN PANDA a conduit des opérations de reconnaissance systématique à l'aide d'un réseau de boîtiers relais opérationnels (ORB) identifié sous le nom d'ORB02, démontrant la persistance opérationnelle de l'adversaire et l'étendue de ses capacités.

Les activités de VIXEN PANDA au cours du second semestre 2024 sont passées d'efforts de reconnaissance à large échelle ciblant des centaines d'appareils de sécurité réseau dans plusieurs pays européens à des tentatives ciblées d'exploitation d'appliances périmétriques au sein d'entités gouvernementales et de défense en Slovénie, en Roumanie, en République tchèque et dans des institutions de l'UE. En février 2025, le ciblage par VIXEN PANDA des opérations européennes d'une agence gouvernementale américaine indique que le cyberadversaire maintient son rythme opérationnel et se concentre sur des cibles gouvernementales et de défense de premier plan.

Entre septembre 2024 et mars 2025, les observations issues de données de télémétrie réseau tierces indiquent que TREASURE PANDA a probablement ciblé des entités aérospatiales et de défense russes développant des systèmes de radars militaires. Le périmètre de ciblage étendu du cyberadversaire s'est étendu à l'Europe de l'Est, certainement en raison de l'invasion de l'Ukraine par la Russie en 2022.



En janvier 2024, un cybercriminel associé à la Chine (non attribué de manière formelle) a ciblé une entité gouvernementale italienne et s'est livré à une activité de type « hands-on-keyboard » impliquant la reconnaissance, le vidage de mémoire LSASS et le déploiement de l'implant *PlugX*. Cette opération s'est déroulée peu de temps après que l'Italie s'est officiellement retirée de l'initiative chinoise des Nouvelles Routes de la Soie en décembre 2023, ce qui suggère que le cybercriminel était potentiellement motivé par des intentions de représailles ou de collecte de renseignements.

Le ciblage de plusieurs institutions de l'UE et de pays alliés de l'OTAN par les cybercriminels associés à la Chine reflète probablement la priorité que Pékin accorde à la surveillance de la coordination des politiques de défense européennes et de leur développement. La Chine considère les entités gouvernementales et de défense européennes comme des sources essentielles pour comprendre la dynamique, les capacités de défense et les processus d'élaboration de politiques de l'alliance occidentale. Les cyberadversaires en lien avec la Chine continuent également de cibler les pays européens qui ne sont pas alignés sur la politique occidentale. Ces cyberadversaires ont ciblé des entités russes, en cohérence avec la mission territoriale des unités du Commandement du théâtre d'opérations Nord de l'Armée populaire de libération (APL), vraisemblablement dans le but de collecter des renseignements sur la sécurité nationale et la défense.

Ciblage du secteur européen de la fabrication

VERTIGO PANDA a ciblé le secteur européen de la fabrication avec des techniques d'exploitation basées sur l'usage de clés USB. En février 2024, VERTIGO PANDA a ciblé les opérations d'une entité manufacturière d'Europe occidentale basée au Vietnam à l'aide d'une clé USB infectée contenant plusieurs composants malveillants, dont l'implant signature du cyberadversaire, *InstituteX*. Étant donné la nature persistante de la diffusion de logiciels malveillants via des supports amovibles, CrowdStrike Intelligence ne peut pas déterminer si ces exemples représentent de nouvelles tentatives de déploiement *d'InstituteX* ou des réinfections continues de la part de VERTIGO PANDA.

Ciblage du secteur européen des services financiers

Les entités de services financiers sont confrontées à des efforts ciblés de collecte de renseignements de la part de cyberadversaires associés à la Chine, VAULT PANDA ayant conduit des activités de reconnaissance visant des institutions financières suisses en janvier 2024. Le cyberadversaire a utilisé *Acunetix* pour effectuer une reconnaissance initiale dans le but d'identifier les vulnérabilités exploitables.

En août 2024, WICKED PANDA a mené une campagne de phishing à grande échelle ciblant des entités d'assurance dans plusieurs pays européens, dont le Royaume-Uni, la France, l'Italie et l'Allemagne. Le cyberadversaire a utilisé des e-mails de l'administration fiscale compromis pour diffuser le logiciel malveillant *Voldemort*.

Les cyberadversaires en lien avec la Chine semblent cibler les institutions financières pour collecter des renseignements et voler des informations personnelles. Les données recueillies servent probablement à évaluer les actifs monétaires et à faciliter les activités de renseignement subséquentes. Cela suggère l'intérêt de la Chine à comprendre les capacités financières européennes et à identifier potentiellement des cibles pour de futures opérations d'espionnage économique.

Ciblage du secteur européen universitaire

Les établissements universitaires et les organismes de recherche sont systématiquement ciblés dans le cadre de campagnes multisectorielles étendues, VIXEN PANDA ayant conduit des activités de reconnaissance visant des entités universitaires et des instituts de recherche de l'UE en avril 2024. WICKED PANDA a également ciblé des institutions universitaires européennes dans le cadre d'une campagne de phishing d'août 2024 qui a touché plus de 70 cibles à l'échelle mondiale. Le fait de cibler les institutions de recherche de l'UE aux côtés d'entités gouvernementales et militaires suggère que la Chine reconnaît le rôle essentiel du monde universitaire dans les avancées technologiques et les capacités de défense européennes.

Ciblage du secteur européen de la technologie

En juin et juillet 2025, CrowdStrike OverWatch et les Services CrowdStrike ont répondu à l'activité d'intrusion de GENESIS PANDA dans une entreprise technologique basée en Espagne. Le cyberadversaire a probablement obtenu l'accès initial par compromission d'une instance Microsoft SQL Server. Au cours de l'intrusion, GENESIS PANDA s'est livré à une activité de reconnaissance de base, a tenté de se déplacer latéralement via Windows Remote Shell et a téléchargé plusieurs implants et outils, y compris *Sliver* et *Cobalt Strike*, à partir d'une infrastructure connue contrôlée par ce dernier.

Au cours de la période considérée, l'activité liée à la Chine ciblant les organisations technologiques basées en Europe a été faible. Cependant, les cyberadversaires en lien avec la Chine ont systématiquement ciblé des entités technologiques plus que tout autre secteur dans le monde. Les organisations technologiques sont régulièrement ciblées pour répondre aux exigences traditionnelles de collecte de renseignements et d'espionnage industriel des cyberadversaires, indiquant que le cyberespionnage fait partie intégrante des efforts nationaux de la Chine en matière de collecte d'informations. Étant donné que les cyberadversaires en lien avec la Chine ont historiquement ciblé de manière significative des entités technologiques du monde entier, le secteur technologique européen est probablement une cible prioritaire pour eux.

Ciblage du secteur européen des organisations à but non lucratif et des ONG

En juin 2024, CASCADE PANDA a déployé avec succès le logiciel malveillant *WinDealer* dans les bureaux d'une organisation à but non lucratif d'Europe occidentale basée en Chine. Ce ciblage a démontré l'intérêt de la Chine pour la surveillance des ONG internationales opérant sur le territoire chinois et suggère des préoccupations potentielles concernant les opérations d'influence étrangère ou les activités de collecte de renseignements menées par des organisations à but non lucratif.

ACTIVITÉ ASSOCIÉE À LA CORÉE DU NORD

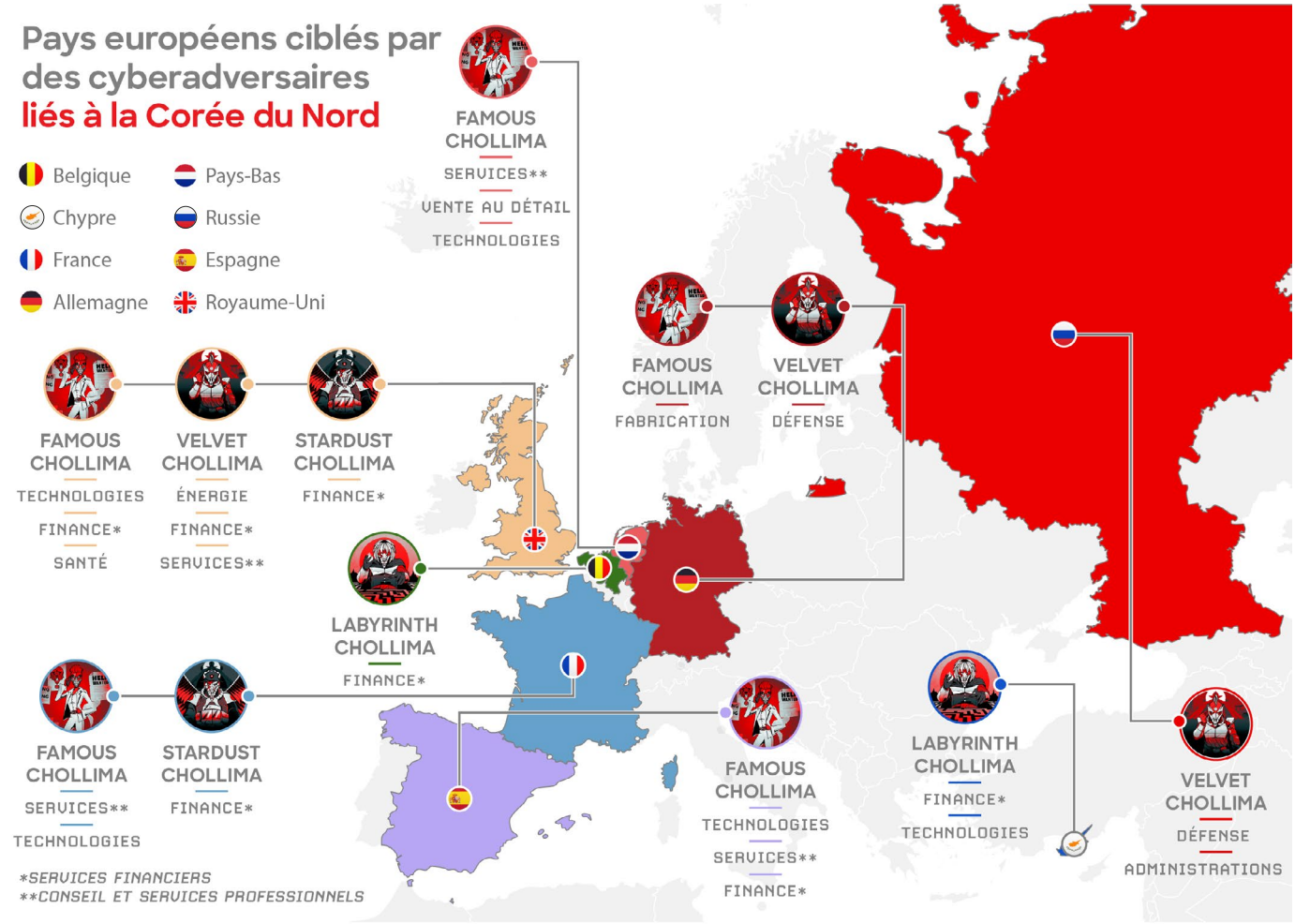


Figure 11. Ciblage des pays européens par des acteurs associés à la Corée du Nord

La Corée du Nord a toujours ciblé des entités européennes, en raison du rôle central de l'Europe sur les plans économique, diplomatique et militaire, ainsi que de son influence majeure sur les questions relatives à la péninsule coréenne. Les cyberadversaires présentant des liens avec la Corée du Nord sont motivés par la collecte de renseignements sur les affaires politiques, les questions militaires et la production de devises, et ont ciblé diverses entités gouvernementales, de défense, de services financiers et de conseil européennes. Ce ciblage s'aligne sur les priorités de la Corée du Nord visant à obtenir des armes nucléaires et une technologie militaire de pointe et à acquérir une influence régionale en Asie du Nord-Est.

Ciblage du secteur européen de la défense

Depuis au moins avril 2024, les cyberadversaires associés à la Corée du Nord VELVET CHOLLIMA et LABYRINTH CHOLLIMA ont ciblé des entités de défense européennes dans le but éventuel de s'emparer de leur propriété intellectuelle et/ou de répondre à des exigences en matière de renseignement militaire. Cette activité soutient probablement la technologie militaire de la Corée du Nord et permet au pays d'obtenir des renseignements tactiques sur les systèmes d'armement européens, que les forces ukrainiennes pourraient utiliser contre les soldats de la Corée du Nord combattant en alliance avec la Russie.

En outre, plusieurs pays européens mettent des forces et du matériel à disposition du commandement de l'ONU stationné en République de Corée. Le commandement de l'ONU est un organisme multilatéral formé en 1950 pour contrer l'agression de la Corée du Nord contre la République de Corée, pendant la guerre de Corée. La guerre de Corée s'est achevée par un armistice, maintenant les belligérants dans un état de guerre sur le plan juridique et faisant des organisations européennes de défense et militaires une cible attrayante pour les opérations de cyberespionnage de la Corée du Nord.

Entre mai et septembre 2024 au moins, VELVET CHOLLIMA a probablement ciblé les employés d'un fabricant allemand de matériel de défense via une campagne de phishing d'identifiants, en déployant son logiciel malveillant *HTTPSpy*. Le fait de cibler des entités du secteur de la fabrication de matériel de défense pour collecter de la propriété intellectuelle ou des renseignements militaires est cohérent avec le périmètre de ciblage et les motivations connues de VELVET CHOLLIMA.

En août 2024, LABYRINTH CHOLLIMA s'est fait passer pour un recruteur afin d'inciter un employé d'une entité de défense européenne à télécharger un fichier ZIP malveillant lié à une offre d'emploi, hébergé sur un service de partage de fichiers basé sur le cloud. Cette entité de défense, qui travaille dans des domaines d'intérêt élevé pour le régime nord-coréen (p. ex. satellites et reconnaissance aérienne), s'aligne sur les besoins de la Corée du Nord en matière de renseignement[24]. Par la suite, en mai 2025, le cyberadversaire a ciblé une entité de défense européenne avec un fichier ZIP lié à une offre d'emploi diffusé via WhatsApp.

Ciblage des services financiers européens

Les institutions financières et les entreprises de technologie financière (fintech) européennes sont des cibles de premier plan pour les opérations à motivation financière de la Corée du Nord, car l'Europe compte de nombreuses entités financières et fintech bien établies. De nombreuses juridictions européennes ont également assoupli la réglementation financière, ce qui pourrait contribuer à une perception de niveaux de sécurité inférieurs ou à une réticence à signaler les incidents de cybersécurité. Les deux scénarios sont susceptibles d'accroître l'intérêt des cyberadversaires en lien avec la Corée du Nord à cibler ces entités.

Entre janvier et juin 2025, STARDUST CHOLLIMA, qui dispose d'un mandat exclusif de production de devises, a ciblé des entités européennes des secteurs de la cryptomonnaie et de la finance. Plusieurs incidents ont impliqué l'utilisation d'appâts de phishing liés à la vidéoconférence, se présentant comme des opportunités d'investissement en capital-risque. Ces appâts incitaient les cibles à télécharger et à exécuter des charges actives AppleScript qui étaient censées corriger les problèmes d'accès aux réunions ou de son. Les campagnes menées par STARDUST CHOLLIMA sont très probablement motivées par les besoins de la Corée du Nord en matière d'assets numériques, ainsi que par sa stratégie de contournement des sanctions internationales.

Au 3e trimestre 2024, LABYRINTH CHOLLIMA s'est fait passer pour un recruteur sur LinkedIn afin d'inciter un employé d'une fintech basée en Europe de l'Ouest à rejoindre un espace de travail Slack lié à la fausse entreprise. La victime a téléchargé un projet Python infecté par un cheval de Troie contenant *SnakeBaker* qui se présentait comme une évaluation de compétences. Après l'exécution du projet par la victime, LABYRINTH CHOLLIMA a accédé à sa clé d'accès à l'environnement cloud, a effectué une reconnaissance, s'est déplacé latéralement et a finalement détourné des fonds en cryptomonnaie.

24 https://kcnawatch.org/newstream/1610155111-665078257/on-report-made-by-supreme-leader-kim-jong-un-at-8th-congress-of-wpk/

Ciblage du secteur européen de l'énergie

Entre avril et octobre 2024, VELVET CHOLLIMA a usurpé l'identité d'entités énergétiques britanniques et de nombreuses organisations aux États-Unis et au Japon. Il n'y a aucune certitude quant au fait que VELVET CHOLLIMA ait spécifiquement ciblé le secteur de l'énergie, ou bien qu'il ait tenté de compromettre l'accès d'une personne accédant à des sites web publics du secteur de l'énergie. Dans le premier cas, les données recueillies pourraient alimenter les besoins persistants en renseignement de la Corée du Nord dans le domaine des technologies de l'énergie. De plus, la technologie de l'énergie nucléaire est intrinsèquement à double usage, et la Corée du Nord pourrait vraisemblablement utiliser toute information volée pour soutenir son programme nucléaire militaire.

Cependant, cette activité est anormale pour VELVET CHOLLIMA. À l'heure actuelle, les cyberadversaires de la Corée du Nord ne représentent pas une cybermenace significative pour les entreprises énergétiques européennes.

Ciblage du secteur européen des services professionnels

De plus, au cours de la campagne qui a eu lieu d'avril à octobre 2024, VELVET CHOLLIMA a ciblé des entités du secteur des services professionnels du Royaume-Uni à l'aide de domaines usurpés. Cette activité soutient probablement les objectifs plus globaux du cyberadversaire en matière de collecte de renseignements, visant à surveiller les positions politiques des pays occidentaux et à accéder à des entités qui influencent les processus décisionnels diplomatiques et économiques.

FAMOUS CHOLLIMA

Au cours de la période visée par le rapport, FAMOUS CHOLLIMA a eu recours à des logiciels malveillants et des menaces internes pour cibler des entités basées en Europe dans le cadre d'opérations opportunistes et ne ciblant aucun secteur spécifique. Les opérations de FAMOUS CHOLLIMA semblent être motivées par l'aspect financier, car elles impliquent systématiquement le vol de cryptomonnaies de faible valeur ou la fraude à la carte de crédit, ainsi que la perception de salaires illicites. FAMOUS CHOLLIMA utilise des appâts liés à des offres d'emploi pour inciter les cibles à télécharger et à exécuter des charges actives malveillantes hébergées sur GitHub et Bitbucket. Le cyberadversaire incite également les cibles à visiter des infrastructures malveillantes se faisant passer pour des plateformes d'entretien virtuel ou d'évaluation des compétences.

Des particuliers européens ont également contribué à faciliter les opérations de menace interne de FAMOUS CHOLLIMA. En mai 2024, le ministère américain de la Justice a inculpé et coordonné l'arrestation d'un ressortissant ukrainien pour avoir dirigé un service qui exploitait trois parcs d'ordinateurs portables et vendait des profils sur des sites web de freelancing populaires, permettant aux opérateurs de FAMOUS CHOLLIMA de falsifier leur identité.

En outre, CrowdStrike Intelligence a identifié un parc d'ordinateurs portables basé en Pologne que le cyberadversaire a utilisé en juin 2025. Le ministère américain de la Justice a également sanctionné un ressortissant russe pour avoir travaillé avec un agent consulaire de la Corée du Nord basé en Russie afin de faciliter les paiements à une entité employant des informaticiens de Corée du Nord en Russie et au Laos.

En septembre 2024, l'Office britannique chargé de la mise en œuvre des sanctions financières (OFSI) a publié un avis décrivant les premières opérations connues de FAMOUS CHOLLIMA visant le Royaume-Uni. Depuis lors, CrowdStrike Intelligence a observé plusieurs opérations de menace interne visant des entités basées en Europe.

ACTIVITÉ DANS LE RESTE DU MONDE

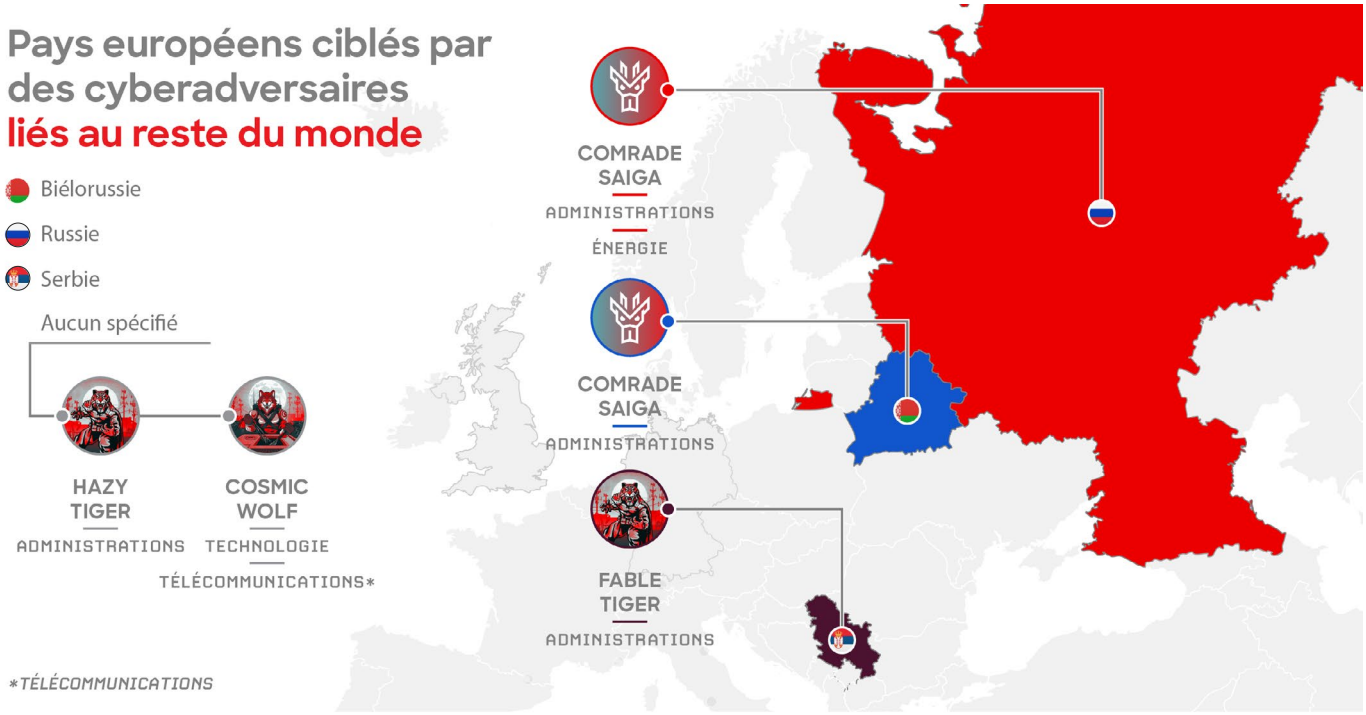


Figure 12. Pays européens ciblés par le reste du monde

Entre janvier 2024 et septembre 2025, CrowdStrike Intelligence a observé peu de cas de cyberadversaires dans le reste du monde ciblant des entités européennes. Cependant, deux cyberadversaires, COSMIC WOLF et COMRADE SAIGA, restent des cybermenaces importantes pour des secteurs spécifiques en fonction de leur activité historique, de leur profil de cible et de leurs motivations.

Cyberadversaires présentant des liens avec la Turquie

Malgré une activité minimale observée depuis le début de l'année 2024, le cyberadversaire en lien avec la Turquie COSMIC WOLF reste une cybermenace importante pour les entités européennes, en particulier pour les entités du secteur des technologies et des télécommunications. En décembre 2023, COSMIC WOLF a déployé l'implant Linux *Torchlight* et utilisé des techniques LOTL (living off the land) auprès d'une entreprise technologique basée en Europe. Bien que la méthode d'accès initial du cyberadversaire soit inconnue, les recherches menées par CrowdStrike Intelligence révèlent qu'il aurait obtenu une clé SSH privée pour accéder à un serveur dans l'environnement cible.

Sur la base de l'activité de COSMIC WOLF depuis 2022, le cyberadversaire se concentre probablement sur les entités européennes du secteur des technologies et des télécommunications. La compromission de ces entités permet probablement à COSMIC WOLF de cibler des entités en aval plus directement liées aux besoins de la Turquie en matière de renseignements, tels que les groupes minoritaires et les dissidents politiques en Turquie.

Cyberadversaires présentant des liens avec le Kazakhstan

Le cyberadversaire en lien avec le Kazakhstan COMRADE SAIGA n'a pas été observé en train de cibler des entités européennes entre janvier 2024 et septembre 2025. Cependant, il constitue une cybermenace importante pour les ministères des Affaires étrangères européens, notamment ceux ayant une représentation diplomatique au Kazakhstan. En dehors de la Russie, COMRADE SAIGA cible principalement des entités gouvernementales et énergétiques associées ou opérant dans la région de la CEI.

Parmi les entités gouvernementales, COMRADE SAIGA cible le plus souvent les ministères des Affaires étrangères, presque certainement dans le but de collecter des renseignements sur des questions diplomatiques pertinentes pour le Kazakhstan et la région de la CEI. Fin janvier 2023, COMRADE SAIGA a probablement ciblé une ambassade européenne à Astana, au Kazakhstan, à l'aide d'un e-mail de phishing contenant une pièce jointe malveillante. L'accent mis par le cyberadversaire sur les ministères des Affaires étrangères, chose qui n'a pas été observée à l'encontre des entités européennes depuis 2023, indique très probablement que COMRADE SAIGA vise à collecter des renseignements sur les efforts diplomatiques du Kazakhstan.

Cyberadversaires présentant des liens avec l'Inde

De janvier 2024 à septembre 2025, les cyberadversaires associés à l'Inde n'ont mené qu'un seul incident visant des entités européennes. En novembre 2024, HAZY TIGER a ciblé des entités diplomatiques en Chine, y compris les représentants d'une délégation commerciale européenne, probablement par le biais d'e-mails de harponnage (spear phishing) comprenant des fichiers de connecteur de recherche liés à des répertoires WebDAV malveillants. HAZY TIGER poursuivait certainement ses efforts de collecte de renseignements sur les relations diplomatiques chinoises, sans cibler spécifiquement la délégation commerciale.

Fin 2023, FABLE TIGER a probablement ciblé une entité gouvernementale serbe en utilisant un site web de collecte d'identifiants usurpant la page de connexion à la messagerie web de l'organisation. FABLE TIGER cible généralement des entités sud-asiatiques, et CrowdStrike Intelligence ne peut actuellement pas évaluer la motivation du cyberadversaire pour cette activité.

L'activité liée à l'Inde dans la région restera très probablement occasionnelle ou tangentielle au cours de l'année prochaine. Cette évaluation est réalisée avec un degré de confiance élevé sur la base de l'accent prédominant mis par le cyberadversaire sur les cibles d'Asie du Sud et du Sud-Est, avec une activité minimale à l'encontre des entités européennes.

Portrait du cyberactivisme et des acteurs non étatiques

Entre janvier 2024 et septembre 2025, CrowdStrike Intelligence a observé de nombreux groupes cyberactivistes affirmant cibler des systèmes de contrôle industriels (ICS) à travers l'Europe, à la fois en réponse à des conflits et dans le cadre d'activités annexes. Le groupe cyberactiviste pro-russe *Z-Alliance* a mené la plupart de ces opérations à l'encontre des pays perçus comme hostiles à la Russie. L'intérêt croissant des cyberactivistes pour le ciblage des ICS est probablement dû à l'impact significatif potentiel et à l'attention médiatique associée.

Au cours de la période considérée, les forces de l'ordre internationales, notamment les autorités européennes, ont perturbé l'infrastructure de plusieurs groupes cyberactivistes et procédé à l'arrestation de différents membres. Cette action des forces de l'ordre s'inscrit dans les objectifs plus larges de l'Europe en matière de lutte contre la cybercriminalité, tels que la classification de la cybercriminalité comme une priorité élevée par la Plateforme multidisciplinaire européenne contre les cybermenaces criminelles (EMPACT), selon l'EMPACT 2022-2025[25].

25 https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact

Ciblage des systèmes de contrôle industriels

Entre janvier 2024 et septembre 2025, de nombreux groupes cyberactivistes ont affirmé cibler les ICS, les systèmes SCADA, les terminaux IoT (Internet des objets) et les technologies opérationnelles (OT) à travers l'Europe. L'activité présumée consistait principalement en la manipulation des paramètres des appareils, la dégradation de sites web, les attaques DDoS contre des systèmes externes et le vol d'identifiants.

Les cyberactivistes ont déclaré que les griefs politiques étaient le principal moteur des attaques visant les ICS, *Z-Alliance* étant à l'origine du plus grand nombre de revendications pendant cette période. Le groupe aurait utilisé des outils accessibles au public tels que Shodan et RealVNC Viewer dans leurs attaques.

D'autres groupes cyberactivistes (notamment *APT Iran*, *Cyber Av3ngers*, *Infrastructure Destruction Squad (IDS)*, *GhostSec*, *Golden Falcon Team*, *Maxious Greyhat*, *Russian Partisan* et *Laneh | Dark*), ont également prétendu cibler des ICS pendant cette période. Bien que leur activité présumée se soit concentrée sur des entités non européennes, ces allégations ont mis en évidence l'intérêt croissant des cyberactivistes pour le ciblage des ICS.

Les groupes cyberactivistes continueront probablement à manifester leur intérêt pour le ciblage des ICS à l'échelle mondiale au cours des 12 prochains mois. Cependant, la plupart d'entre eux démontreront probablement des capacités techniques limitées et s'appuieront sur des revendications exagérées ou des logiciels malveillants accessibles au public conçus pour cibler les ICS. Ces évaluations sont réalisées avec un degré de confiance modéré sur la base d'une augmentation observée de l'activité revendiquée par des cyberactivistes visant ces appareils et systèmes au cours de la période de référence, ainsi que du désir d'attention des cyberactivistes.

Réponse des cyberactivistes aux actions des forces de l'ordre européennes

Entre janvier 2024 et septembre 2025, les forces de l'ordre européennes ont mené de nombreuses opérations contre des groupes cyberactivistes, qui ont abouti à des centaines d'arrestations et à d'importantes saisies d'infrastructures dans plusieurs pays. Les cyberactivistes ont répondu aux actions des forces de l'ordre par des campagnes de représailles visant des entités dans les pays ciblés, des ajustements des protocoles OPSEC et des messages stratégiques sur les réseaux sociaux pour minimiser l'impact des opérations menées par les forces de l'ordre.

Pendant ce temps, de multiples opérations menées par les forces de l'ordre ont ciblé BOUNTY JACKAL. En juillet 2024, les autorités espagnoles ont arrêté des membres de BOUNTY JACKAL. Ces arrestations ont incité le cyberadversaire à mettre en œuvre des nouveaux protocoles OPSEC et à lancer des attaques DDoS coordonnées contre des sites web espagnols.

De même, après que l'opération Eastwood menée par Europol a perturbé l'infrastructure de BOUNTY JACKAL en juillet 2025, le cyberadversaire a rapidement lancé l'opération Time of Retribution. Ce dernier a ciblé des pays associés à l'opération Eastwood par des attaques DDoS, des dégradations de sites web et des intrusions présumées dans des infrastructures, tout en affirmant que l'opération menée par Europol n'avait eu qu'un impact restreint sur le groupe.

Alors que les forces de l'ordre internationales poursuivent leurs efforts contre la cybercriminalité, les cyberactivistes continueront probablement à répondre par des campagnes de représailles, des changements opérationnels et des messages sur les réseaux sociaux.

Conclusion

À court terme, il est presque certain que les cyberactivistes continueront à cibler en priorité les entités basées en Europe pour des raisons financières. Il est très probable que l'extorsion de données et les ransomwares restent la cybermenace la plus critique pour l'Europe, compte tenu de l'impact des intrusions réussies et de l'intérêt constant que les cyberadversaires spécialisés dans la chasse au gros gibier portent à la région.

Bien que l'impact potentiel des intrusions réussies reste élevé, les cyberadversaires bénéficient de techniques d'accès initial et de diffusion de logiciels malveillants, à la fois éprouvées et en constante évolution, comme en témoigne leur adoption soudaine et généralisée des appâts de vishing et des faux CAPTCHA. La popularité de l'IA favorisera probablement cette évolution.

Depuis 2024, les opérations des forces de l'ordre internationales ont eu un impact sur les actions des cyberadversaires, les forums (par exemple, BreachForums et XSS) et les services facilitateurs. Cependant, les écosystèmes clandestins anglophones et russophones restent résilients, car ils sont décentralisés et regroupent des cybercriminels qui agissent sans être inquiétés, depuis des pays apparemment refuges.

Par conséquent, les cybercriminels basés en Europe et ciblant l'Europe continueront de bénéficier d'un écosystème propice à l'émergence d'acteurs aux niveaux de sophistication divers, tout en réduisant les obstacles à l'entrée dans la cybercriminalité. Compte tenu de l'anonymat de l'écosystème et de la nature indiscriminée des services qui le rendent possible, les cybermenaces non liées à la cybercriminalité (notamment le cybercriminel hybride RENAISSANCE SPIDER et le groupe associé à la Russie EMBER BEAR) tirent également parti de ces réseaux.

Il est presque certain que les cyberadversaires à la solde d'États continueront à collecter des renseignements pour influencer les politiques nationales et les relations avec les entités européennes. Les États antagonistes sont très motivés à cibler les entités européennes, probablement parce qu'elles offrent des informations politiques, économiques et technologiques lucratives qui peuvent être exploitées pour promouvoir des intérêts stratégiques.

Les développements géopolitiques peuvent rapidement transformer les besoins en matière de renseignements et la portée opérationnelle d'un cyberadversaire. Pour des pays comme la Russie et l'Iran, les cybercapacités font partie intégrante de la réponse aux conflits perçus comme des menaces pour leur souveraineté. Les deux pays mènent un large éventail d'opérations, allant de campagnes d'espionnage et de reconnaissance passives à des campagnes destructrices de « hack-and-leak » déguisées en cyberactivisme et en attaques ouvertement destructrices. Ces opérations offrent une dénégation plausible, entravent les efforts d'attribution et réduisent les coûts financiers et humains, permettant à ces États de projeter leur puissance et leur influence au-delà des capacités conventionnelles.

En outre, d'autres cybercriminels à la solde d'États ciblent des entités européennes pour des motifs économiques et financiers. Les cyberadversaires en lien avec la Chine commettent souvent des vols de propriété intellectuelle pour renforcer l'avantage concurrentiel international de la Chine et éviter une R&D interne coûteuse. En plus des efforts de collecte de renseignements, les cyberadversaires en lien avec la Corée du Nord mènent souvent des activités opportunistes génératrices de revenus (telles que le vol de cryptomonnaies) pour financer le régime de la Corée du Nord.

Les conflits mondiaux continueront probablement à motiver l'activité cyberactiviste contre les entités européennes au cours des 12 prochains mois. Pour maximiser leur impact public, certains groupes cyberactivistes prétendront probablement cibler les OT critiques, y compris des ICS et des systèmes SCADA, à travers l'Europe et dans le monde. Alors que les forces de l'ordre internationales intensifient leurs opérations contre la cybercriminalité, les cyberactivistes répondront probablement par des campagnes de représailles, des changements tactiques et une activité coordonnée sur les réseaux sociaux.

Recommandations

1 Adopter l'IA agentique pour faire évoluer les opérations de sécurité

Alors que les cybercriminels utilisent l'IA pour frapper plus rapidement, intensifier leurs opérations et échapper à la détection, les équipes de sécurité font face à une pression croissante pour suivre le rythme. Elles sont déjà très sollicitées, font face à des alertes de plus en plus nombreuses, à des pénuries de compétences et doivent réagir toujours plus rapidement. Pour combler ce retard, les équipes de sécurité doivent opérationnaliser l'IA agentique, des agents spécialisés capables de raisonner, de s'adapter et d'agir tout en respectant des garde-corps définis et les politiques de l'entreprise. L'IA agentique permet aux équipes d'appliquer un raisonnement professionnel à grande vitesse pour accélérer les résultats et autonomiser les tâches. Ces capacités peuvent faire évoluer les opérations orientées sur le renseignement en utilisant le renseignement et l'expertise émergents pour trier les alertes, mener des enquêtes et réaliser des interventions. En se déchargeant des tâches chronophages et répétitives, l'IA agentique permet aux analystes humains de se concentrer sur le Threat Hunting proactif et les investigations partant d'une hypothèse, ce qui améliore à la fois l'impact stratégique et l'efficacité opérationnelle.

2 Sécuriser l'ensemble de l'écosystème des identités

Les cyberadversaires ciblent de plus en plus les identités en utilisant le vol d'identifiants, le contournement de l'authentification multifacteur et l'ingénierie sociale, tout en se déplaçant latéralement entre les environnements sur site, cloud et SaaS au moyen de relations de confiance. Cela leur permet d'usurper l'identité d'utilisateurs légitimes, d'intensifier les privilèges et d'échapper à la détection.

Les organisations doivent adopter des solutions d'authentification multifacteur résistantes au phishing, par exemple des clés de sécurité matérielles, pour empêcher tout accès non autorisé. Il est essentiel que des politiques d'identité et d'accès fortes soient mises en place, y compris les accès en flux tendu, les examens réguliers des comptes et les contrôles d'accès conditionnel. Les outils de détection des cybermenaces liées à l'identité doivent surveiller le comportement dans les environnements endpoint et sur site, cloud et SaaS pour signaler l'élévation des privilèges, l'accès non autorisé et la création de comptes de porte dérobée. L'intégration de ces outils à des plateformes de détection et de réponse étendues (XDR) permet une visibilité complète et une défense unifiée contre les cyberadversaires.

De plus, les organisations doivent former les utilisateurs à reconnaître les tentatives de vishing et de phishing, tout en maintenant une surveillance proactive pour détecter et répondre aux cybermenaces basées sur l'identité.

3 Éliminer les écarts de visibilité inter-domaines

L'utilisation croissante par les cyberadversaires de techniques « hands-on-keyboard » et d'outils légitimes rend la détection et la réponse plus difficiles. Contrairement aux logiciels malveillants traditionnels, ces méthodes permettent aux cyberattaquants de contourner les mesures de sécurité d'ancienne génération en exécutant des commandes et en se servant de logiciels légitimes pour imiter les opérations normales.

Pour faire face à cela, les organisations doivent moderniser leurs stratégies de détection et de réponse. Les solutions SIEM (gestion des événements et des informations de sécurité) de nouvelle génération offrent une visibilité unifiée sur les endpoints, les réseaux, les environnements cloud et les systèmes d'identité, ce qui permet aux analystes de corréler les comportements suspects et de voir le chemin d'attaque complet. Le tri et les enquêtes pilotés par l'IA agentique peuvent étendre ces capacités, en analysant de manière autonome les signaux à travers tous les domaines afin de faire apparaître des informations très fiables et hiérarchiser les cybermenaces réelles.

Le threat hunting proactif et la cyberveille viennent peaufiner la détection en identifiant les modèles d'attaque potentiels et en fournissant un aperçu des TTP des cyberadversaires. Les informations en temps réel permettent à l'organisation de surveiller l'apparition de cybermenaces, d'anticiper les cyberattaques et de hiérarchiser les efforts de sécurité critiques.

4 Défendre le cloud en tant qu'infrastructure centrale

Les cyberadversaires ciblant le cloud exploitent les erreurs de configuration, les identifiants volés et les outils de gestion cloud pour infiltrer les systèmes, se déplacer latéralement et maintenir un accès persistant pour des activités malveillantes telles que le vol de données et le déploiement de ransomware.

Les plateformes de protection des applications cloud native (CNAPP, Cloud-Native Application Protection Platform) dotées de capacités de détection et de réponse cloud (CDR) sont essentielles pour contrer ces cybermenaces. Ces solutions offrent aux opérateurs une vue unifiée de leur posture de sécurité du cloud, ce qui les aide à détecter, à hiérarchiser et à remédier rapidement aux erreurs de configuration, aux vulnérabilités et aux cybermenaces. De plus, la mise en application de contrôles d'accès stricts, tels que l'accès basé sur les rôles et les politiques conditionnelles, limite l'exposition aux systèmes critiques tout en surveillant continuellement les anomalies, y compris la connexion à partir d'emplacements inattendus.

Des audits réguliers sont également essentiels pour maintenir la sécurité. Les outils automatisés peuvent révéler des paramètres de stockage trop permissifs, des API exposées et des vulnérabilités non corrigées. Des examens fréquents des environnements cloud permettent aux équipes de traiter rapidement les autorisations inutilisées et les configurations obsolètes.

5 Prioriser les vulnérabilités avec une approche centrée sur les cyberadversaires

Les cyberadversaires exploitent de plus en plus publiquement les vulnérabilités et utilisent l'enchaînement d'exploits, en combinant plusieurs vulnérabilités pour obtenir un accès rapide, élever les privilèges et contourner les défenses. Ces attaques en plusieurs étapes s'appuient souvent sur des ressources publiques, telles que des exploits de preuve de concept et des blogs techniques, ce qui permet aux cyberadversaires de créer des charges actives efficaces et difficiles à détecter.

Afin de contrer ces cybermenaces, les organisations doivent donner la priorité à l'application régulière de correctifs ou à la mise à niveau des systèmes critiques, en particulier les services fréquemment ciblés sur Internet, tels que les serveurs Web et les passerelles VPN. La surveillance des signes subtils d'enchaînement d'exploits, tels que des plantages inattendus ou des tentatives d'élévation des privilèges, peut aider à détecter les attaques avant qu'elles ne progressent.

Les outils tels que CrowdStrike Falcon® Exposure Management, conçus avec une priorisation native de l'IA, permettent aux équipes de réduire les alertes pour se concentrer sur les vulnérabilités les plus importantes, en particulier celles qui affectent les systèmes critiques et à haut risque. En adoptant des approches de sécurité proactives, en découvrant les expositions de la surface d'attaque et en tirant parti de l'automatisation, les organisations atténuent les cybermenaces sophistiquées et limitent les opportunités des cyberadversaires.

6 Cerner le cyberadversaire et se préparer

Lorsqu'une cyberattaque se déroule en quelques minutes, voire en quelques secondes, la préparation peut faire une grande différence entre confinement et catastrophe. Une approche axée sur le renseignement permet aux équipes de sécurité d'aller au-delà de la défense réactive et de comprendre quels cyberadversaires les ciblent, comment ils opèrent et leurs objectifs. Grâce à la recherche de menaces, au profilage des cyberadversaires et à l'analyse des techniques d'attaque, les équipes de sécurité peuvent prioriser les ressources, adapter les défenses et surveiller activement les cybermenaces avant qu'elles ne s'intensifient. La cyberveille CrowdStrike ne se limite pas à la détection de cybermenaces connues, elle anticipe les techniques d'attaque nouvelles et évolutives, ce qui permet aux équipes de sécurité d'avoir toujours une longueur d'avance. En intégrant de manière transparente les renseignements dans les workflows de sécurité, les organisations peuvent accélérer les délais de réponse, contrer les cyberadversaires et transformer les renseignements en actions.

Si la technologie joue un rôle essentiel dans la détection et la neutralisation des intrusions, l'utilisateur final reste un maillon essentiel de la chaîne pour mettre fin aux compromissions. Les organisations doivent mettre en place des programmes de sensibilisation à l'égard des utilisateurs pour combattre la menace persistante associée au phishing et aux techniques d'ingénierie sociale connexes. Pour les équipes de sécurité, c'est en forgeant qu'on devient forgeron. Mettez en place un environnement qui effectue régulièrement des exercices de simulation en salle et des exercices Red/Blue Team pour identifier les failles et éliminer les lacunes dans vos pratiques et interventions de cybersécurité.

À propos de CrowdStrike

CrowdStrike (Nasdaq : CRWD), leader mondial de la cybersécurité, redéfinit la sécurité avec sa plateforme cloud native la plus avancée au monde, conçue pour protéger les ressources critiques des entreprises, à savoir les endpoints, les workloads cloud, les identités et les données.

Optimisée par l'architecture de sécurité cloud de CrowdStrike et une IA de pointe, la plateforme CrowdStrike Falcon® s'appuie sur des indicateurs d'attaque en temps réel, la recherche de menaces, l'évolution des techniques des cybercriminels et des données télémétriques enrichies collectées à l'échelle de l'entreprise pour assurer une détection ultraprécise, une protection et une correction automatisées, un Threat Hunting de pointe et une observation priorisée des vulnérabilités.

Spécialement conçue dans le cloud au moyen d'une architecture à agent léger unique, la plateforme Falcon offre un déploiement rapide et évolutif, une protection et des performances de haut niveau, une complexité réduite et une rentabilité immédiate.

CrowdStrike : We stop breaches.

Pour en savoir plus : www.crowdstrike.com

Suivez-nous : Blog | X | LinkedIn | Facebook | Instagram | YouTube

Profitez sans plus tarder d'une évaluation gratuite :
www.crowdstrike.com/free-trial-guide