



CERT-IST

INDUSTRIE | SERVICES | TERTIAIRE

Bilan Cert-IST 2026 sur les failles et attaques de 2025

Publié en mars 2026

Table des matières

1	Introduction.....	3
2	Analyse des phénomènes les plus marquants de 2025	4
2.1	Les 3 événements de l'année	4
2.1.1	La crise ToolShell : l'Alerte Rouge SharePoint	4
2.1.2	Le ciblage des « Gardiens » : F5 et Red Hat Consulting	4
2.1.3	La compromission de l'identité déléguée : la vague Salesforce.....	5
2.2	Les acteurs à l'origine des attaques	6
2.2.1	Groupes étatiques : espionnage, pré-positionnement et opérations hybrides.....	6
2.2.2	Cybercriminalité : extorsion, paralysie industrielle et vols de données.....	7
2.2.3	Hactivisme : volume massif, impact informationnel	8
2.2.4	Des frontières floues entre ces groupes.....	8
2.3	L'intégrité de la Software Supply Chain mise à l'épreuve	8
2.4	Infiltration humaine et menace interne.....	9
2.5	Zéro-days et Exploitation des équipements de bordure.....	10
2.6	DDoS : franchissement d'un seuil de puissance	11
2.7	Ingénierie sociale : automatisation et nouvelles techniques.....	11
2.8	Intelligence artificielle : accélérateur opérationnel	12
2.9	Les vols de cryptoactifs toujours importants	12
3	Productions du Cert-IST en 2025.....	14
3.1	Veille sur les vulnérabilités et les menaces	14
3.1.1	Nombre d'avis de sécurité (et de CVE) publiés par an	14
3.1.2	Les alertes Cert-IST pour 2025	15
3.2	Veille sur les attaques et IOC.....	16
3.2.1	Campagnes et IOC, en quelques chiffres.....	16
3.2.2	Fiches attaques publiées en 2025	17
3.3	Veille technologique.....	17
4	Conclusions.....	18

1 Introduction

Comme chaque année, le Cert-IST propose un bilan de l'année écoulée afin de mettre en évidence les tendances sur l'évolution des vulnérabilités et attaques et aider la communauté à mieux se protéger.

L'année 2025 ne marque pas une rupture technologique, mais plutôt une forme « d'aboutissement » dans l'industrialisation des capacités des attaquants. L'effondrement du périmètre traditionnel se confirme : l'attaquant s'installe dans la durée en compromettant les « gardiens » de l'infrastructure ou même en s'infiltrant physiquement au sein des équipes IT via des méthodes de recrutement détournées. Ce bilan souligne également la maturité des agents d'intelligence artificielle, passés du stade d'assistants à celui d'opérateurs autonomes.

Nous analysons dans un premier temps les phénomènes les plus marquants de l'année (cf. chapitre 2). Nous fournissons ensuite un récapitulatif des différentes productions du Cert-IST (cf. chapitre 3).

La conclusion (cf. chapitre 4) donne une synthèse du paysage actuel de la cybermenace et des challenges auxquels les entreprises doivent faire face en 2026.

➤ A propos du Cert-IST

Le Cert-IST (Computer Emergency Response Team - Industrie, Services et Tertiaire) est un centre d'alerte et de réaction aux attaques informatiques destiné aux entreprises. Créé en 1999, il aide ses adhérents à identifier les menaces en analysant quotidiennement les nouvelles vulnérabilités, leurs criticités et les moyens de protection pour s'en protéger. En cas d'incident de sécurité touchant l'un de ses adhérents, le Cert-IST peut apporter son aide dans l'investigation et permettre une remise en service opérationnelle et sécurisée.

Bilan Cert-IST 2026 sur les failles et attaques de 2025		Page : 3 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-FR	1.0

2 Analyse des phénomènes les plus marquants de 2025

2.1 Les 3 événements de l'année

L'année 2025 marque un certain changement dans la nature des cibles : après les équipements de bordure mis en avant dans le bilan sur les failles de 2024 (qui restent malgré tout, toujours d'actualité en 2025), ce sont les infrastructures critiques on-premises, les « gardiens » détenteurs de secrets clients, et les identités déléguées du SaaS, qui nous paraissent avoir concentré les attaques les plus stratégiques.

Trois crises illustrent cette évolution.

2.1.1 La crise ToolShell : l'Alerte Rouge SharePoint

L'événement le plus important, en termes de vulnérabilité « traditionnelle », a été l'exploitation durant l'été 2025 de la chaîne [ToolShell](#) affectant **Microsoft SharePoint Server on-premises**. Cette faille d'exécution de code à distance sans authentification a conduit le Cert-IST à déclencher une [Alerte Rouge](#) le 24 juillet, une mesure exceptionnelle qui n'avait pas été prise depuis la crise [ProxyLogon](#) / [ProxyShell](#) de 2021 visant les serveurs Microsoft Exchange.

La chronologie de cette crise illustre bien la rapidité de militarisation d'une vulnérabilité aujourd'hui. Démontrée à la conférence Pwn2Own en mai, elle a été patchée par Microsoft le 8 juillet, puis reproduite le [14 juillet par Code White](#). Trois jours plus tard, le 17 juillet, des attaques exploitaient déjà un contournement du correctif initial. Microsoft a dû réagir en urgence le 19 juillet avec un second correctif renforcé. Ce cycle complet s'est ainsi bouclé en moins de dix jours.

Mais l'aspect le plus redoutable de ToolShell résidait probablement dans le vol des clés cryptographiques SharePoint permettant de forger des jetons d'authentification légitimes. Une fois ces clés exfiltrées, l'attaquant disposait d'un accès persistant, même après l'application des correctifs. La seule remédiation fiable consistait alors en une rotation complète et manuelle des clés sur l'ensemble de la ferme SharePoint, une opération complexe dans un environnement de production.

2.1.2 Le ciblage des « Gardiens » : F5 et Red Hat Consulting

L'année 2025 a confirmé une évolution notable des intrusions initiales : l'attaque directe contre les prestataires qui détiennent les plans d'infrastructure ou les accès privilégiés de leurs clients. Ces attaques illustrent une mutation des risques liés à la supply chain. Au-delà du code logiciel piégé à la manière de SolarWinds, ce sont de plus en plus les prestataires de services eux-mêmes (consultants et fournisseurs d'équipements) qui deviennent des cibles stratégiques.

En l'occurrence, en août, l'équipementier **F5** a découvert une [intrusion de longue durée](#) menée par le groupe chinois [UNC5221 \(CERT-IST/INFO-2025.026\)](#). Les attaquants, présents dans les systèmes pendant plus d'un an, ont exfiltré du code source de BIG-IP ainsi que des informations sur des vulnérabilités internes non encore corrigées. Cet incident a contraint F5 à publier [44 correctifs](#) en urgence en octobre (il n'y en avait eu que six au trimestre précédent) pour parer à d'éventuelles attaques en zéro-day.

De manière quasi-concomitante, début octobre, la **division conseil de Red Hat** a [subi une exfiltration](#) de 570 Go de données depuis son instance GitLab interne ([CERT-IST/INFO-2025.024](#)). Le groupe [Crimson Collective](#) a dérobé plus de 28 000 dépôts contenant environ 800 « Customer Engagement Reports »

Bilan Cert-IST 2026 sur les failles et attaques de 2025	Page : 4 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-FR
	1.0

(CERs). Ces rapports de mission renfermaient les schémas réseau, les jetons d'authentification, les clés API et les configurations d'infrastructure de clients critiques parmi lesquels figuraient HSBC, Walmart, Bank of America, Verizon, JP Morgan et la U.S. Navy.

En ciblant le prestataire, l'attaquant obtient facilement une visibilité totale sur les défenses de centaines d'organisations à la fois. Un seul point de compromission se transforme ainsi en risque de supply chain généralisé, chaque client du « gardien » devenant potentiellement accessible sans attaque directe.

2.1.3 La compromission de l'identité déléguée : la vague Salesforce

La crise Salesforce de 2025 a touché des centaines d'organisations sans pourtant qu'aucune faille de cette plateforme CRM ne soit exploitée. En ciblant les applications tierces intégrées à Salesforce, les attaquants ont déclenché une série de compromissions en cascade.

Les attaquants, a priori le groupe d'extorsion **ShinyHunters** ([UNC6395](#) pour Google), ont d'abord compromis l'[environnement GitHub de Salesloft](#) entre mars et juin, puis accédé à son infrastructure AWS. Celle-ci hébergeait notamment des jetons OAuth associés à Drift, une plateforme d'automatisation marketing et de chat conversationnel connectée à Salesforce. En utilisant ces jetons pour s'authentifier sur les environnements clients, ils ont exfiltré, entre le 8 et le 18 août, des données appartenant à plus de 700 organisations, dont Google, Cisco, Cloudflare et Gainsight.

Cette compromission de Gainsight s'est révélée stratégique : en novembre, les attaquants ont utilisé les identifiants volés lors de l'attaque d'août pour compromettre l'infrastructure même de Gainsight, leur permettant d'accéder aux jetons OAuth que cette société utilisait pour ses propres intégrations avec Salesforce. [Environ 285 instances supplémentaires](#) ont ainsi été compromises, touchant d'autres sociétés comme Verizon, GitLab, F5 et SonicWall.

Parallèlement à ces attaques de supply chain, **ShinyHunters** a mené une campagne de [vishing](#) ciblant directement les employés d'entreprises utilisatrices de Salesforce. En se faisant passer pour le support technique, les attaquants ont convaincu leurs victimes d'autoriser des applications OAuth frauduleuses, obtenant ainsi un accès direct à leurs instances Salesforce. En octobre, le groupe a lancé un [site d'extorsion](#) listant 39 victimes (FedEx, Disney, Toyota, Marriott, Air France-KLM, LVMH, Chanel) et fixé un ultimatum au 10 octobre, menaçant de publier environ 1 milliard d'enregistrements volés.

Ces intrusions illustrent la dangerosité des jetons OAuth : une fois compromis, ils contournent l'authentification multi-facteurs, génèrent un trafic API apparemment légitime, et permettent d'opérer pendant des semaines sans déclencher d'alerte.

Bilan Cert-IST 2026 sur les failles et attaques de 2025		Page : 5 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-FR	1.0

2.2 Les acteurs à l'origine des attaques

L'année 2025 confirme l'hybridation entre espionnage étatique, cybercriminalité et hacktivisme. Cette convergence s'observe concrètement dans les cibles, les outils et les modes opératoires.

2.2.1 Groupes étatiques : espionnage, pré-positionnement et opérations hybrides

Les attaques réalisées par des États sont de toutes natures, mais se différencient des autres par leurs capacités d'un haut niveau de sophistication et leurs discrétions, avec l'objectif de rester longtemps au sein de l'organisation attaquée (attaque de pré-positionnement).

Les États les plus cités dans les rapports sont inchangés (les BIG-4) : Chine, Russie, Corée du Nord et Iran. On notera comme en 2024 que l'on parle peu des autres, et en particulier des activités offensives des pays occidentaux.

La Chine, [désignée par le renseignement américain](#) comme «la menace cyber la plus active et persistante», a mené plusieurs campagnes d'envergure. En [juillet](#), trois groupes chinois ont exploité les vulnérabilités zero-day de la campagne ToolShell (évoquée à la section 2.1.1) pour compromettre [plus de 400 organisations](#) à travers le monde. Le groupe **Storm-2603** s'est distingué en déployant le ransomware Warlock sur des serveurs gouvernementaux américains, touchant notamment la National Nuclear Security Administration, les National Institutes of Health et le Department of Homeland Security. Parallèlement, **Salt Typhoon** a poursuivi sa [campagne d'espionnage des télécommunications](#) en compromettant au moins 200 entreprises dans 80 pays. En [décembre](#), le groupe a compromis les systèmes de messagerie du personnel de plusieurs commissions de la Chambre des représentants américaine. L'autre groupe chinois majeur, **Volt Typhoon** [a poursuivi en 2025](#) ses opérations de pré-positionnement dans les infrastructures critiques, visant particulièrement les systèmes énergétiques, de transport et de télécommunications en vue d'un sabotage potentiel lors d'une crise géopolitique.

La Russie a poursuivi ses campagnes hybrides. Le groupe **APT28** a mené une [campagne prolongée](#) contre des entités logistiques et technologiques occidentales. **Sandworm** a [tenté fin décembre](#) une attaque contre le réseau électrique polonais, déployant le malware destructeur DynoWiper. Parallèlement, le pays a intensifié ses opérations d'influence via [Doppelgänger](#), campagne de désinformation ciblant notamment les élections allemandes.

L'Iran s'est montré très actif en 2025, avec une [augmentation de 133%](#) des cyberattaques en mai-juin dans le cadre du conflit avec Israël et des frappes américano-israéliennes. Le groupe **MuddyWater** a mené une [campagne d'espionnage](#) visant plus de 100 entités gouvernementales au Moyen-Orient et en Afrique du Nord. Le groupe a démontré une [évolution significative](#) de ses capacités offensives avec entre autres le déploiement de la nouvelle backdoor MuddyViper.

Enfin, la Corée du Nord continue de brouiller les frontières entre cyberespionnage et cybercriminalité. L'attaque de la plateforme d'échange [Bybit en février](#), attribuée au groupe **Lazarus**, a permis le vol d'environ 1,5 milliard de dollars en cryptomonnaies, s'inscrivant dans une logique de financement étatique par le cybercrime, avec un niveau de sophistication comparable aux opérations d'espionnage classiques.

Bilan Cert-IST 2026 sur les failles et attaques de 2025		Page : 6 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-FR	1.0

2.2.2 Cybercriminalité : extorsion, paralysie industrielle et vols de données

Les ransomwares, et plus généralement les tentatives d'extorsion, [demeurent la menace la plus impactante](#) pour les entreprises en 2025, mais leur paysage connaît une recomposition certaine. Les grandes opérations policières coordonnées par Europol depuis 2024 ([Cronos contre LockBit](#) et [Endgame contre les botnets de distribution, loaders et infostealers](#)) ont provoqué une fragmentation de cet écosystème. **RansomHub**, qui avait comblé le vide laissé par **LockBit**, [a disparu fin mars 2025](#), probablement suite à des dissensions internes. [LockBit est revenu en septembre 2025](#) avec LockBit 5.0, annonçant [la formation d'un cartel avec Qilin et DragonForce](#) pour partager techniques, ressources et infrastructures.

Le cybercrime se restructure aussi du fait d'une plus grande sensibilisation des entreprises : le taux moyen de paiement des rançons [a chuté à 23% au 3^{ème} trimestre 2025](#), un plancher historique.

Les grands RaaS laissent place à une myriade de petits groupes (entre 126 et 141 actifs en 2025 contre 70 en 2023) tandis que des groupes fermés comme **Akira** et **Play** survivent avec une stratégie volume/rançons plus modestes ciblant des entreprises intermédiaires moins matures. L'expansion géographique s'accroît : le ransomware représente désormais [51% des incidents en Asie-Pacifique](#), région auparavant moins exposée que l'Amérique du Nord ou l'Europe.

Sur le plan tactique, 2025 continue avec de l'extorsion sans chiffrage. La campagne menée par **CIOp** contre la solution Oracle E-Business Suite en est emblématique : [exploitation en zero-day](#) de vulnérabilités, vols atteignant jusqu'à 180 Go par victime, et plus d'une centaine d'organisations touchées dont Harvard, Dartmouth, Logitech et Korean Air. La gestion chaotique de la communication par Oracle (correction silencieuse en juillet, alertes d'urgence en octobre) a offert aux attaquants une fenêtre d'exploitation de trois mois pendant laquelle beaucoup d'organisations ignoraient être vulnérables.

Le cas Jaguar Land Rover illustre par ailleurs l'ampleur des pertes financières engendrées par une attaque sur un environnement sensible. Menée par [Scattered Lapsus\\$ Hunters Spider](#), elle a provoqué un arrêt de production de cinq semaines pour un coût total dépassant les [2,5 milliards de dollars](#), démontrant comment une intrusion IT peut facilement paralyser des environnements OT sans sabotage direct. D'autres secteurs ont été touchés par des attaques similaires, dont l'impact opérationnel, associé aux sanctions gouvernementales, peut coûter plusieurs centaines de millions d'euros : [Bouygues Telecom](#), [Marks & Spencer](#) et [SK Telecom](#) en sont de bons exemples.

Dans le domaine de la santé, l'incident chez [Change Healthcare](#) de février 2024 a été confirmé en 2025 comme la plus grande fuite de données jamais enregistrée, exposant les données de 192,7 millions d'Américains. L'impact a dépassé la fuite d'informations, bloquant les paiements médicaux à l'échelle nationale pendant plusieurs mois et révélant même une dépendance systémique dangereuse à un système très centralisé.

Sur le plan technique, les cybercriminels ont délaissé selon nous quelque peu les attaques en zero-day au profit du phishing et de l'utilisation d'identifiants volés (voir aussi la section 2.7). Les malwares voleurs d'informations alimentent un écosystème de courtiers d'accès (Initial Access Brokers) qui revendent les identifiants compromis aux groupes de ransomware.

Enfin, le phishing-as-a-service (avec des kits clé en main comme Tycoon 2FA, FlowerStorm et Darcula) facilite toujours plus le contournement de l'authentification multi-facteurs via des techniques adversary-in-the-middle.

Bilan Cert-IST 2026 sur les failles et attaques de 2025		Page : 7 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-FR	1.0

2.2.3 Hactivisme : volume massif, impact informationnel

Selon l'ENISA, l'hactivisme a compté pour [80% des incidents européens](#) en 2025. Les groupes pro-russes dominant, avec **NoName057(16)** responsable de plus de 60% des revendications DDoS via sa plateforme DDoSia. [L'Opération Eastwood](#) en juillet 2025, coordonnée par Europol, a temporairement perturbé son infrastructure, Mais n'a malheureusement pas empêché sa reprise rapide.

En France, [le collectif NoName057\(16\) a revendiqué](#) l'attaque contre La Poste le 22 décembre, perturbant services bancaires et postaux en pleine période de Noël. L'impact technique reste généralement limité, mais ces opérations s'inscrivent dans une logique de pression informationnelle continue, amplifiée par les réseaux sociaux et les canaux de revendication publics.

L'hactivisme évolue également au-delà du simple DDoS. Des groupes comme [Z-Pentest](#) ciblent par exemple les systèmes industriels. Des chercheurs notent une [multiplication par 2](#) de ces attaques sur Q3 2025 dont pas loin d'un quart visant tout ce qui est OT (Operational Technologies), notamment dans les secteurs de l'eau, l'agriculture et l'énergie.

Au Moyen-Orient, le groupe pro-israélien **Predatory Sparrow** a frappé en juin [Nobitex, la plus grande plateforme crypto iranienne](#), drainant 90 millions de dollars. Les fonds ont été transférés vers des adresses inaccessibles, rendant leur récupération impossible (destruction délibérée à visée politique). Nobitex, représentant 87% du volume crypto iranien, était accusée de faciliter le contournement des sanctions et le financement de groupes affiliés au Corps des gardiens de la révolution islamique (IRGC).

2.2.4 Des frontières floues entre ces groupes

La distinction traditionnelle entre acteurs étatiques, cybercriminels et hactivistes se brouille plus que jamais. La Russie [finance et dirige directement](#) des groupes cybercriminels et hactivistes : le GRU contrôle **NoName057(16)** et **CARR** via des officiers dédiés, tandis que le FSB [recrute des hackers condamnés](#) pour les transformer en assets opérationnels.

[La Corée du Nord a volé](#) \$2,02 milliards en cryptomonnaies en 2025 pour financer en particulier son programme nucléaire, effaçant toute frontière entre espionnage et cybercriminalité.

L'Iran présente un modèle hybride : [le groupe Pioneer Kitten mène des opérations d'espionnage puis vend les accès](#) à des groupes de ransomware russes pour monétiser ses intrusions.

Enfin, une quatrième catégorie se renforce : les « **Hackers for Hire** », mercenaires cyber travaillant indifféremment pour États, cybercriminels ou entreprises. [74 gouvernements](#) ont fait appel à des mercenaires cyber rien que pour la mise en place de logiciels espions, un marché déjà valorisé à \$12 milliards dès 2019. Ces acteurs, dont la sophistication vaut largement celle des services étatiques, créent une confusion croissante dans l'attribution des attaques.

2.3 L'intégrité de la Software Supply Chain mise à l'épreuve

Le développement logiciel est de plus en plus au cœur des stratégies d'intrusion. L'année 2025 révèle une diversification méthodique des vecteurs d'attaque, dont l'efficacité repose sur un effet multiplicateur : compromettre un mainteneur ou un outil permet d'atteindre des milliers d'organisations simultanément.

Bilan Cert-IST 2026 sur les failles et attaques de 2025	Page : 8 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-FR
	1.0

D'un côté, on a pu observer un phishing ultra-ciblé de certains mainteneurs de packages / modules. En septembre par exemple, [Josh Junon \(Qix-\)](#), responsable de bibliothèques **NPM** totalisant 2,6 milliards de téléchargements hebdomadaires dont **chalk** et **debug**, est victime d'une campagne contournant son authentification à deux facteurs. Pendant les deux heures de compromission, 2,5 millions de téléchargements distribuent du code malveillant, chaque installation représentant potentiellement une application en production infectée.

De l'autre, des techniques d'auto-propagation amplifie ces compromissions. [Le ver Shai-Hulud](#) a réutilisé les identifiants volés lors de [l'incident S1ngularity](#) d'août pour s'injecter automatiquement dans des centaines de paquets. Il vole ensuite clés API, secrets AWS et tokens GitHub de nouveaux développeurs, créant un cycle d'infection exponentiel.

Enfin, les ordinateurs de développeurs sont devenus eux-mêmes des têtes de pont, après des intrusions dont la sophistication va grandissant. A ce titre, [la campagne GlassWorm](#) d'octobre a transformé des extensions Visual Studio Code (l'éditeur de code de Microsoft) en chevaux de Troie déployant des fonctions d'accès distants et de proxies.

Mais l'effet multiplicateur évoqué plus haut atteint son paroxysme lorsque les attaquants ciblent directement les infrastructures cloud mutualisées. En mars, [CloudSEK révèle](#) ce qu'elle qualifie de plus grosse attaque supply chain de 2025 : 6 millions d'enregistrements volés depuis les serveurs d'authentification d'[Oracle Cloud](#). Les données compromises incluent mots de passe chiffrés, certificats et clés d'accès de 140 000 locataires, un effet domino permettant l'accès aux environnements cloud de milliers d'entreprises. [Oracle a contesté fermement](#) malgré les preuves publiées, créant une incertitude inédite sur l'ampleur réelle de l'incident.

Pour réduire l'impact de futures attaques semblables, on a vu se succéder les réponses techniques, essentiellement de la part des plateformes d'hébergement de code. GitHub a déployé en septembre l'authentification par jetons temporaires pour NPM, une mesure qui aurait grandement pu limiter les campagnes S1ngularity et Shai-Hulud si déployée plus tôt. **PyPI**, le dépôt de code Python, accélère ses mécanismes de quarantaine automatique des paquets suspects.

Mais ces protections au niveau des dépôts publics ne sont pas toujours suffisantes, et nous estimons que les entreprises doivent aujourd'hui prendre en compte ce risque. Les mesures à envisager peuvent inclure le scan / la validation des dépendances open source par un système indépendant (pourquoi pas utilisant de l'IA), et le maintien de son propre registre de code en internes.

2.4 Infiltration humaine et menace interne

Plusieurs incidents marquants de 2025 ont illustré l'exploitation de la confiance organisationnelle comme vecteur d'intrusion.

Tout d'abord, en termes d'**infiltration**, nous nous devons de mentionner une continuité dans la campagne nord-coréenne [Wagemole](#). Pour rappel, on constate depuis quelques années que des agents nord-coréens se font embaucher sous de fausses identités au sein d'entreprises occidentales, utilisant l'IA générative pour créer CV et photos de profil convaincants. Lors des visioconférences de recrutement, des deepfakes vidéo en temps réel substituent les visages.

Les autorités américaines ont découvert des « laptop farms » [dans au moins 16 États](#) : des complices locaux réceptionnent les équipements professionnels, qui après une configuration adéquate, permettent

Bilan Cert-IST 2026 sur les failles et attaques de 2025	Page : 9 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-FR
	1.0

l'accès à distance depuis la Corée du Nord. Les salaires détournés financent de fait le régime de Pyongyang.

La campagne [Contagious Interview](#), toujours nord-coréenne, exploite quant à elle les processus de recrutement des sociétés occidentales pour piéger des candidats externes. Des développeurs sont attirés vers de faux entretiens où ils installent des "tests techniques" ou exécutent des commandes pour "réparer" une webcam défectueuse. Entre juin et juillet 2025, plus de 17 000 téléchargements de paquets NPM piégés ont été attribués à cette campagne.

Côté **menace interne**, l'incident de la société Coinbase, une grosse entreprise financière spécialisée dans les cryptomonnaies, est symptomatique de scénarios de plus en plus préoccupants. [Un employé du support](#) a été arrêté pour avoir facilité l'accès aux données de 69461 clients.

[Chez CrowdStrike](#), un employé a vendu des captures d'écran de systèmes internes pour 25000 dollars.

À [la Banque centrale du Brésil](#), des identifiants vendus 920 dollars ont permis un vol de 140 millions.

Enfin, une [intrusion chez Coupang](#) (équivalent d'Amazon en Corée du sud) provenait d'un ancien employé ayant conservé ses accès après son départ.

Ces compromissions montrent que, bien que les techniques de détection s'améliorent en permanence, l'ingénierie sociale les contourne quelle que soit leur sophistication. Par conséquent, les processus de recrutement, la vérification d'identité continue et la révocation stricte des accès constituent des enjeux de sécurité aussi critiques que la détection d'événements de sécurité et les protections périmétriques.

2.5 Zéro-days et Exploitation des équipements de bordure

Comme en 2024, l'exploitation des vulnérabilités des équipements de bordure s'est poursuivie à un rythme soutenu en 2025. Sur les **27** alertes émises par le CERT-IST au cours de l'année, **16 concernaient de tels équipements** (59,3%), confirmant que VPN, pare-feux et appliances diverses restent non seulement le terrain de chasse privilégié des attaquants, mais aussi le sujet principal des déclenchements de crise au Cert-IST.

Cette concentration n'a rien de surprenant : ces équipements sont exposés sur Internet par fonction et rarement équipés de solutions EDR, ce qui complique les analyses forensiques et facilite des compromissions durables.

L'[ENISA](#) confirme que **l'exploitation de vulnérabilités** représente 21,3% des vecteurs d'intrusion en Europe (on rappelle que l'essentiel des intrusions est attribué au phishing et à l'ingénierie sociale). Un [rapport de NSHC ThreatRecon](#) observe par ailleurs qu'environ la moitié des vulnérabilités exploitées en 2025 étaient nouvelles, et que près d'un tiers sont armées le jour même de la publication dans CVE voire avant (zéro-day).

Les cibles habituelles n'ont pas changé : Ivanti Connect Secure ([AL-2025.001](#), [AL-2025.008](#)), Fortinet FortiOS et FortiWeb ([AL-2025.002](#), [AL-2025.016](#)), Cisco ASA/FTD ([AL-2025.019](#)), Palo Alto Networks ([AL-2025.003](#)), NetScaler ([AL-2025.014](#), [AL-2025.018](#)), SonicWall ([AL-2025.010](#)).

Cette industrialisation de l'exploitation des vulnérabilités, accessible à des acteurs de tous niveaux, continue d'imposer aux entreprises une grande réactivité et une visibilité permanente sur leurs actifs exposés.

Bilan Cert-IST 2026 sur les failles et attaques de 2025		Page : 10 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-FR	1.0

2.6 DDoS : franchissement d'un seuil de puissance

Ici, l'année 2025 marque un changement d'échelle. Les attaques DDoS, dont on avait enregistré un pic à **5,6 Tbps** fin 2024, ont atteint de nouveaux records : **29,7 Tbps** en septembre 2025, puis **31,4 Tbps** en décembre, soit une multiplication par six en un an. Le botnet [Aisuru](#), fort de 1 à 4 millions d'objets connectés compromis, a été le principal vecteur de ces records.

Cette montée en puissance va de pair avec l'explosion du nombre d'attaques : Cloudflare a enregistré **47,1** millions d'attaques en 2025, contre **21,3** millions en 2024. Mais ces chiffres impressionnants ne doivent pas masquer la réalité opérationnelle : la plupart des attaques restent très courtes (souvent moins d'une minute) et sont bloquées automatiquement par les fournisseurs de protection spécialisés.

Nous dirons donc ici que l'enjeu réside plutôt dans l'accessibilité de ces attaques. Grâce aux services DDoS-for-hire, n'importe qui peut louer une capacité multi-Tbps pour quelques centaines de dollars. Les forces de l'ordre réagissent bien sûr, avec par exemple l'[Opération PowerOFF](#) (27 plateformes démantelées en décembre 2024) et l'[Opération Eastwood](#) (perturbation du groupe NoName057(16) en juillet 2025). Ces succès tactiques ralentissent ponctuellement les opérations, mais ils n'arrivent pour ainsi dire jamais à éradiquer un botnet dans son ensemble.

Pour les entreprises, la question n'est donc pas tant la puissance maximale des attaques que la préparation : disposer d'une protection adaptée, automatisée, et capable d'absorber des volumes multi-Tbps reste le seul rempart efficace face à une menace industrialisée et quotidienne.

2.7 Ingénierie sociale : automatisation et nouvelles techniques

L'ingénierie sociale demeure le premier **vecteur d'intrusion**, représentant **60% des incidents** recensés par l'ENISA en 2025. Au-delà du phishing classique, l'année a vu émerger des techniques qui contournent les défenses traditionnelles en exploitant directement la confiance ou les processus internes.

Le phénomène [ClickFix](#), observé pour la première fois au printemps 2024, a connu une explosion en 2025 (**+517%**). Ces attaques affichent de fausses erreurs (mises à jour Windows, CAPTCHAs, avertissements de sécurité) et invitent l'utilisateur à exécuter lui-même des commandes pour "résoudre" le problème. Résultat : la victime installe un malware sans que l'attaquant ait besoin de contourner de quelconques protections. Initialement ciblant Windows, ClickFix s'est étendu à MacOS et Linux, déployant infostealers, RATs et backdoors. Des variantes comme [ConsentFix](#) ont même détourné l'authentification OAuth d'Azure pour obtenir des tokens d'accès. En fin d'année, la plateforme payante ErrTraffic a commercialisé l'automatisation de ces campagnes.

Parallèlement, le [vishing ciblé des helpdesks](#) est devenu une méthode d'intrusion privilégiée. Le groupe **Scattered Spider** a systématisé cette approche en se faisant passer pour des employés légitimes auprès des services support, obtenant ainsi des réinitialisations de comptes ou des accès sans avoir à compromettre de système. Cette technique a permis des intrusions majeures chez Marks & Spencer, Co-op et dans des compagnies d'assurance américaines. L'affaire **Cognizant**, poursuivi pour 380 millions de dollars par Clorox après qu'un attaquant a dupé son helpdesk, illustre les conséquences financières de ces défaillances procédurales.

Enfin, la publication d'un [Mega-Leak de 16 milliards de credentials](#), agrégation massive de fuites passées issues de services comme Google, Apple ou Facebook, a transformé des années de réutilisation de mots

Bilan Cert-IST 2026 sur les failles et attaques de 2025		Page : 11 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-FR	1.0

de passe en un réservoir mondial pour des attaques par « **credential stuffing** ». Cette base de données, qui était facilement accessible, a amplifié mécaniquement toutes les attaques basées sur l'identité, rendant la compromission de comptes encore plus triviale.

2.8 Intelligence artificielle : accélérateur opérationnel

L'IA passe peu à peu du rôle d'assistant à celui d'acteur opérationnel dans les intrusions. En septembre, Anthropic a divulgué les attaques **GTG-1002**, attribuée à un groupe chinois étatique : en détournant Claude Code via des techniques de roleplay (convainquant le modèle qu'il effectuait des tests de sécurité légitimes), ce groupe a automatisé 80 à 90% des opérations tactiques visant une trentaine d'organisations.

Le système orchestre la reconnaissance, la découverte de vulnérabilités, la génération d'exploits, la collecte d'identifiants et l'exfiltration de données, avec intervention humaine limitée aux escalades critiques. Le rythme d'exécution (des milliers de requêtes par seconde) rendait toute réponse manuelle impossible. Cette campagne constitue le premier cas documenté d'attaque cyber à grande échelle pilotée principalement par IA.

Du côté des entreprises, le déploiement massif de LLM ouvre de nouvelles surfaces d'attaque. Les attaques par prompt injection détournent le comportement des modèles, avec des vulnérabilités découvertes telles que :

- Une possibilité de fuite de données dans [Microsoft 365 Copilot](#) au moyen d'emails contenant des prompts cachés,
- Un risque d'exfiltration de données au travers de [Google Gemini](#) manipulé par des invitations de calendrier,
- Des risques liés aux assistants de code détournés, par exemple via la dissimulation de [prompts dans les fichiers README](#) de projets.

Le cas [Amazon Q](#) est quant à lui un véritable incident : une extension VS Code compromise, restée en ligne près de deux jours, contenait un prompt demandant la suppression des fichiers locaux et des ressources AWS accessibles par le développeur.

Ces changements imposent une révision des défenses : contrôles d'accès stricts pour les assistants IA en entreprise, et systèmes de détection adaptés à des rythmes d'attaque dépassant les capacités humaines d'analyse temps réel.

2.9 Les vols de cryptoactifs toujours importants

2025 marque la troisième année consécutive de record pour les vols de cryptomonnaies, avec [plus de \\$3.4 milliards dérobés](#) selon Chainalysis. Au-delà du hack de Bybit évoqué plus haut, les pertes se sont diversifiées : [Cetus](#) (\$223 millions), [Phemex](#) (\$85 millions), Nobitex (\$80-90 millions), tandis que [158000 portefeuilles individuels](#) ont été compromis pour \$713 millions via divers phishing et autres malwares ciblant directement les utilisateurs et leurs clés privées.

La Corée du Nord demeure l'acteur étatique dominant avec [\\$2.02 milliards volés](#) (59% du total), mais ses tactiques ont évolué : délaissant un peu les protocoles DeFi, le régime cible désormais les places de change

Bilan Cert-IST 2026 sur les failles et attaques de 2025		Page : 12 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-FR	1.0

centralisés via de l'ingénierie sociale et pratiquent l'[infiltration d'employés](#) sous de fausses identités, obtenant un accès légitime aux infrastructures de clés.

Le blanchiment des cryptomonnaies volées est lui aussi très organisé, via des réseaux d'intermédiaires basés en Asie du Sud-Est (courtiers effectuant des échanges hors plateformes officielles et circuits bancaires parallèles spécialisés dans la conversion en devises fiduciaires). Ces acteurs fragmentent les fonds via des échanges entre différents blockchains et des services de mixage, puis les convertissent progressivement sur plusieurs semaines, rendant leur traçabilité difficile en dépit de la transparence native des blockchains.

Au-delà des opérations étatiques, les attaques sur protocoles DeFi persistent : exploitation de vulnérabilités dans les smart contracts, manipulation d'oracles de prix, et compromission de pools de liquidité. La concentration des pertes s'accroît (les trois plus gros hacks totalisent 69% du montant des vols) mais le nombre d'incidents augmente, révélant une menace fragmentée entre acteurs étatiques sophistiqués et cybercriminels opportunistes exploitant la sécurité encore immature du secteur.

Bilan Cert-IST 2026 sur les failles et attaques de 2025		Page : 13 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-FR	1.0

3 Productions du Cert-IST en 2025

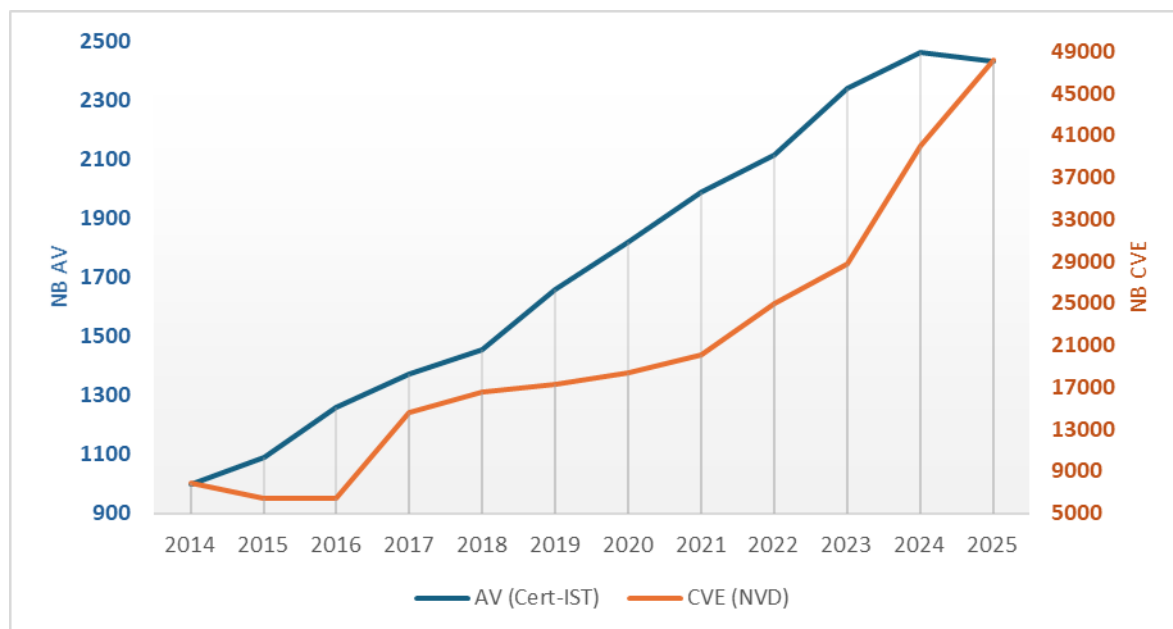
3.1 Veille sur les vulnérabilités et les menaces

Dans le cadre de son activité de veille sur les vulnérabilités et les menaces, le Cert-IST émet plusieurs types de publications dont :

- **Les Avis de sécurité (AV)** : ils décrivent les nouvelles vulnérabilités découvertes dans les produits suivis par le Cert-IST. Un avis traite un ensemble de CVE.
- **Les Alertes (AL)** qui sont émises lorsqu’il y a un fort risque d’attaques pour une vulnérabilité, et les **messages INFO** pour les événements notables mais moins dangereux (par exemple les failles médiatisées).
- **Les Fiches Attaques (ATK)** et des **indicateurs de compromission (IOC)**. Les fiches répertorient les attaques majeures et les groupes d’attaquants. Les IOC correspondants sont mis à disposition dans une base MISP. Cela concerne les menaces récurrentes (MalSpam, Botnets, Ransomware, etc.), ainsi que les attaques de cyber-espionnages (attaques APT) et les ransomware les plus importants.

La suite de cette section donne un bref aperçu des publications de 2025.

3.1.1 Nombre d’avis de sécurité (et de CVE) publiés par an



Nombre d’avis de sécurité (et de CVE) publiés par an

3.1.2 Les alertes Cert-IST pour 2025

Alerte	Référence	Description	Date
Orange	CERT-IST/AL-2025.001	Attaques en cours visant Ivanti Connect Secure (ICS) (CVE-2025-0282)	09 Jan 2025
Orange	CERT-IST/AL-2025.002	Attaques en cours visant Fortinet FortiOS (CVE-2024-55591)	15 Jan 2025
Jaune	CERT-IST/AL-2025.003	Attaques en cours visant Palo Alto Networks PAN-OS (CVE-2025-0108)	14 Fév 2025
Jaune	CERT-IST/AL-2025.004	Attaques en cours contre Apache Tomcat (CVE-2025-24813)	18 Mar 2025
Jaune	CERT-IST/AL-2025.005	Risque d'attaques contre GLPI	21 Mar 2025
Jaune	CERT-IST/AL-2025.006	Risque d'attaques contre le contrôleur Ingress-nginx pour Kubernetes (CVE-2025-1974)	26 Mar 2025
Jaune	CERT-IST/AL-2025.007	Attaques en cours contre CrushFTP (CVE-2025-31161)	01 Avr 2025
Orange	CERT-IST/AL-2025.008	Attaques en cours visant Ivanti Connect Secure (ICS) (CVE-2025-22457)	04 Avr 2025
Jaune	CERT-IST/AL-2025.009	Attaques en cours visant Erlang OTP	25 Avr 2025
Jaune	CERT-IST/AL-2025.010	Attaques en cours visant SonicWall SMA100 (CVE-2024-38475 et CVE-2023-44221)	02 Mai 2025
Jaune	CERT-IST/AL-2025.011	Attaques en cours visant Commvault software (CVE-2025-34028)	05 Mai 2025
Orange	CERT-IST/AL-2025.012	Attaques en cours visant Ivanti EPMM (CVE-2025-4427, CVE-2025-4428)	15 Mai 2025
Jaune	CERT-IST/AL-2025.013	Risque d'attaques contre Fortinet FortiMail	27 Mai 2025
Orange	CERT-IST/AL-2025.014	Attaques en cours visant NetScaler ADC et NetScaler Gateway (CVE-2025-6543, CVE-2025-5777)	25 Jun 2025
Jaune	CERT-IST/AL-2025.015	Risque d'attaques visant les équipements Cisco Unified Communications Manager (CUCM) (CVE-2025-20309)	03 Jul 2025
Jaune	CERT-IST/AL-2025.016	Attaques en cours visant Fortinet FortiWeb (CVE-2025-25257)	15 Jul 2025
Rouge	CERT-IST/AL-2025.017	Attaques en cours visant Microsoft Sharepoint (#ToolShell)	21-juil-25
Jaune	CERT-IST/AL-2025.018	Attaques en cours visant NetScaler ADC et NetScaler Gateway (CVE-2025-7775)	27-août-25
Orange	CERT-IST/AL-2025.019	Attaques en cours visant Cisco ASA et Cisco FTD (CVE-2025-20333, CVE-2025-20362)	26-sept-25
Orange	CERT-IST/AL-2025.020	Attaques en cours visant Oracle E-Business Suite (CVE-2025-61882)	06-oct-25
Jaune	CERT-IST/AL-2025.021	Attaques en cours visant le service Windows Server Update Service (WSUS)	27-oct-25
Jaune	CERT-IST/AL-2025.022	Attaques en cours visant Fortinet FortiWeb (CVE-2025-64446, CVE-2025-58034)	14-nov-25

Jaune	CERT-IST/AL-2025.023	Attaques en cours visant Oracle Identity Manager (CVE-2025-61757)	24-nov-25
Orange	CERT-IST/AL-2025.024	Attaques en cours visant les applications React / Next.js exposées à Internet (CVE-2025-55182) (React2Shell)	05-déc-25
Jaune	CERT-IST/AL-2025.025	Attaques en cours visant plusieurs produits Fortinet (CVE-2025-59718, CVE-2025-59719, CVE-2026-24858)	17-déc-25
Jaune	CERT-IST/AL-2025.026	Attaques en cours visant Cisco Secure Email Gateway et Cisco Secure Email and Web Manager (CVE-2025-20393)	18-déc-25
Jaune	CERT-IST/AL-2025.027	Attaques en cours visant MongoDB	29-déc-25

3.2 Veille sur les attaques et IOC

Le service de veille sur les attaques et IOC du Cert-IST répertorie les campagnes d'attaques connues, les groupes d'attaquants et leurs modes opératoires (TTP), et met à disposition des membres des indicateurs de compromission (IOC) qualifiés, accessibles via une instance MISP, pour alimenter leurs dispositifs de détection et d'investigation.

3.2.1 Campagnes et IOC, en quelques chiffres

En 2025, le Cert-IST a traité **21 161 événements MISP / campagnes**, un volume stable par rapport à 2024. Le nombre de **rapports OSINT** analysés a progressé à **1 770** (contre 1 489 en 2024), et **144 fiches attaques (ATK)** ont été produites, un niveau constant depuis plusieurs années.

Les vecteurs d'attaque des campagnes analysées par le Cert-IST restent largement dominés par l'ingénierie sociale : phishing (43,9 %), arnaques (21,3 %) et malspam (19,4 %) totalisent à eux trois plus de **84 %** des vecteurs observés.

Les malwares les plus fréquemment observés sont **Remcos** (12,1 %), **Formbook** (11,1 %) et **AgentTesla** (10,4 %) — trois outils sur étagère omniprésents dans l'écosystème cybercriminel.

Les stealers et RAT représentent respectivement 39 % et 36 % des types de malwares identifiés, confirmant une priorité donnée au vol d'informations et à la prise de contrôle à distance.

Enfin, parmi les **659 événements** attribués (pour lesquels un groupe d'attaquants a été identifié), **Gamaredon** (Russie) arrive en tête (9,9 %), devant les campagnes nord-coréennes **Contagious Interview** (5,2 %), **Lazarus** et **Kimsuky** (3,5 % chacun).

La Russie et la Corée du Nord concentrent la majorité des attributions étatiques, à laquelle on ajoutera toutefois une présence notable d'acteurs chinois (Mustang Panda, UNC5221).

3.2.2 Fiches attaques publiées en 2025

Fiche	Nom	Description
CERT-IST/ATK-2025.008	TA866	Un acteur hybride entre cybercriminalité et cyberespionnage depuis 2020
CERT-IST/ATK-2025.021	Contagious Interview	Une cybermenace nord-coréenne visant les développeurs et les recruteurs en informatique
CERT-IST/ATK-2025.031	RansomHub	Ransomware (RaaS) apparu en 2024, ciblant des entreprises via la double extorsion
CERT-IST/ATK-2025.032	MirrorFace	APT chinoise de cyber-espionnage ciblant principalement le Japon via du spear-phishing
CERT-IST/ATK-2025.045	TraderTraitor	Groupe nord-coréen visant la crypto via des leurres de recrutement et du code open source piégé
CERT-IST/ATK-2025.057	DOGE Big Balls	Groupe utilisant le ransomware Fog, combinant techniques avancées et provocations politiques
CERT-IST/ATK-2025.069	CyberVolk	Collectif hacktiviste pro-russe combinant ransomware, vol de données et attaques DDoS
CERT-IST/ATK-2025.071	UAC-0226	Opération de cyberespionnage visant l'Ukraine avec le malware GIFTEDCROOK
CERT-IST/ATK-2025.102	ShinyHunters	Un groupe de hackers spécialisé dans les méga-fuites de données et l'extorsion
CERT-IST/ATK-2025.103	Liminal Panda	un groupe de cyberespionnage d'origine chinoise ciblant les opérateurs de télécommunications mobiles depuis 2020
CERT-IST/ATK-2025.117	UNC5221	Un groupe chinois exploitant des failles 0-day d'appiances pour des intrusions furtives
CERT-IST/ATK-2025.119	UAC-0099	Des activités de spear-phishing ciblant l'Ukraine avec des messages à thème juridique
CERT-IST/ATK-2025.132	PlushDaemon	Un groupe APT chinois spécialisé dans le détournement de mises à jour logicielles
CERT-IST/ATK-2025.144	Earth Alux	Un groupe APT chinois spécialisé dans l'exploitation de serveurs IIS et SharePoint

3.3 Veille technologique

En plus de la veille sur les vulnérabilités, le Cert-IST publie également des bulletins de veille technologique :

- Un **bulletin quotidien de veille média (revue de presse)** recensant les articles les plus intéressants parus sur Internet, sur un ensemble de sites francophones et anglophones traitant de sécurité,
- Un **bulletin mensuel de veille SCADA** présentant une synthèse de l'actualité sur la sécurité des systèmes industriels,
- Un **bulletin mensuel** généraliste donnant une synthèse de l'actualité du mois (en termes d'avis et d'attaques) et traitant de sujets d'actualités au travers d'articles rédigés par l'équipe Cert-IST,
- Un **bulletin mensuel de veille sur les attaques et IOC** qui permet de synthétiser les événements les plus marquants dans le domaine des attaques.

4 Conclusions

L'année 2025 a agi comme un puissant révélateur des failles structurelles de notre écosystème numérique. Plus qu'à une simple évolution de la menace, nous avons assisté à une bascule vers l'industrialisation des capacités offensives, où la complexité des systèmes est devenue l'alliée la plus efficace de l'attaquant.

Pour orienter les stratégies de défense en 2026, trois enseignements importants se dégagent selon nous.

1. **L'effondrement de la "barrière" MFA et le pivot vers l'identité machine.** Le premier enseignement est la fin de l'immunité relative apportée par l'authentification multi-facteur (MFA) traditionnelle. Les incidents chez Salesforce et les attaques ToolShell contre SharePoint ont démontré que l'attaquant ne cherche pas tant à "casser" un mot de passe, qu'à "voler la confiance" déjà établie. En ciblant les jetons OAuth et les secrets cryptographiques, des groupes comme ShinyHunters ont contourné des systèmes MFA pour s'octroyer une persistance quasi-indétectable. La priorité de 2026 n'est donc plus seulement de protéger l'accès humain, mais d'instaurer une gouvernance stricte des identités non-humaines.
2. **Le défi du tempo : la défense à la vitesse de la machine.** Le second enseignement concerne l'accélération du cycle d'attaque. Avec l'émergence d'opérations comme celle de [GTG-1002](#), où des agents d'IA pilotent l'essentiel du travail tactique, le facteur temps est devenu asymétrique. Face à une machine capable d'automatiser reconnaissance et exploitation, la réponse humaine manuelle est condamnée à l'échec. Pour 2026, la réduction du temps de remédiation passera obligatoirement par l'automatisation de la défense : le triage par IA et l'orchestration ne sont plus des options, mais des nécessités opérationnelles.
3. **L'extension du "Zero Trust" à la Supply Chain et aux équipements de bordure.** La sécurité d'une organisation est strictement égale à celle du maillon le plus faible de sa chaîne de partenaires. La compromission de Red Hat Consulting ou l'émergence du [ver auto-réplicateur Shai-Hulud](#) rappellent que les **prestataires** et les **dépôts de code** sont devenus des concentrateurs de secrets critiques. Et en même temps, les équipements de bordure, souvent dépourvus d'EDR, restent des angles morts stratégiques.
En 2026, l'approche "Zero Trust" doit impérativement s'étendre aux accès tiers et à la surveillance de l'intégrité des équipements exposés.

L'expérience sur 2025 nous questionne enfin vis-à-vis de la culture de « l'empilement technologique ». Pour faire face à des menaces toujours plus convergentes, la résilience de demain pourrait reposer sur trois piliers :

1. **La Simplicité** : Réduire la surface d'attaque en épurant les interconnexions SaaS et les privilèges superflus.
2. **La Visibilité** : Éliminer les zones d'ombre, qu'il s'agisse des appliances de bordure non supervisées ou des jetons d'accès délégués aux applications tierces.
3. **L'Automatisation** : améliorer la détection et la réponse pour égaler le tempo des agents d'IA offensifs et protéger les actifs critiques en temps réel.

Bilan Cert-IST 2026 sur les failles et attaques de 2025		Page : 18 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-FR	1.0

Association Cert-IST

290 Allée du lac

31 670 Labège

France

info@cert-ist.com

<https://www.cert-ist.com>

05.34.39.44.88



Bilan Cert-IST 2026 sur les failles et attaques de 2025		Page : 19 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-FR	1.0