CERT-IST

INDUSTRIE | SERVICES | TERTIAIRE

Bilan Cert-IST 2025 sur les failles et attaques de 2024

Publié en Février 2025

Table des matières

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.

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 2025.

> ➢ **A propos du Cert-IST**
>
> Le Cert-IST (**C**omputer **E**mergency **R**esponse **T**eam - **I**ndustrie, **S**ervices et **T**ertiaire) 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.

2 Analyse des phénomènes les plus marquants de 2024

2.1 Les 3 événements de l'année

Voici les 3 événements qui nous paraissent les plus marquants pour l'année 2024.

2.1.1 Les Jeux Olympiques et Paralympiques

Tout le monde s'accorde à dire que les Jeux Olympiques et Paralympiques de Paris ont été un grand succès et cela est vrai sur le plan cyber aussi !

Aucune panne n'a perturbé significativement le déroulement de ces événements. Le grand public retiendra donc plutôt les attaques physiques survenues au moment de l'ouverture des jeux (sabotages d'équipements TGV-SNCF et coupures de fibres Internet), que les attaques cyber (attaques DDOS principalement mais aussi le ransomware ayant bloqué les boutiques des Musées de France, dont le Grand Palais) qui n'ont pas créé de perturbations significatives.

C'est une grande réussite parce que les attaques étaient attendues et que même si on ne connait pas les détails, on imagine bien qu'elles se sont effectivement produites et que l'activité pour y répondre a été intense pour le CERT des JO, l'ANSSI et toutes les équipes sécurité des parties prenantes. Un travail colossal de préparation et de mobilisation a été réalisé pour atteindre ce résultat.

La France a démontré à cette occasion son savoir-faire en matière de cyber-sécurité et n'a pas démenti la bonne réputation qu'elle avait déjà dans ce domaine. Tous les participants à cet effort ont sans aucun doute acquis une expérience précieuse (un savoir-faire) et renforcé leur niveau de sécurité. Il reste donc maintenant à pérenniser ces efforts et à trouver les moyens de diffuser ce savoir-faire plus largement vers le plus grand nombre.

2.1.2 La panne CrowdStrike du 19 juillet 2024

Le 19 juillet 2024 une mise à jour défectueuse de l'EDR Falcon de CrowdStrike a causé un arrêt brutal de plus de 8 millions de systèmes Windows dans le monde. Cela a entrainé des pannes importantes pour les organisations qui utilisent ce produit, dont des compagnies aériennes et des hôpitaux.

Ce blocage rappelle des incidents similaires que l'on avait déjà vus plusieurs fois il y a longtemps (dans les années 2010) lorsque des mises à jour des signatures antivirus avaient provoqué par erreur la mise en quarantaine de fichiers vitaux sur les systèmes Windows. La solution la plus souvent adoptée depuis, est le déploiement par palier des mises à jour, d'abord sur des systèmes non critiques, pour limiter l'ampleur de l'incident en cas de mise à jour défectueuse.

Suite à cet incident de 2024, CrowdStrike a renforcé ses procédures de qualification et Microsoft a annoncé qui allait modifier Windows (et proposer des API spécifiques) pour protéger le cœur de son système d'exploitation contre des mises à jour directes par des produits tiers.

Le déploiement des mises à jour par palier (en laissant aux entreprises la responsabilité de définir à quel palier chaque système est affecté) nous semble dans tous les cas une mesure indispensable. Nous ne connaissons pas suffisamment le produit Falcon pour savoir si cela est prévu.

2.1.3 Les attaques sur les équipements de bordure

Nous avions déjà fait ce constat en 2023, et la situation est identique en 2024 : les équipements de bordure de type Firewall ou serveurs VPN sont sous un feu incessant d'attaques :

- Ils semblent **trop fragiles** (en 2020 nous les avions qualifiés de « dur dehors, mais mous dedans »). Les vulnérabilités exploitées en 2024 sont souvent simples et font penser que les produits sont de conceptions anciennes, non conformes avec les pratiques actuelles. Le terme de « vulnérabilité impardonnable » est devenu à la mode en 2024.
- Ils sont **difficiles à surveiller** (pas d'EDR)
- Ils sont **difficiles à désinfecter** car l'attaquant s'installe profondément dans la plate-forme sous-jacente (souvent un système Linux ou FreeBSD).

Voici les 9 attaques de ce type survenues en 2024 (il y en avait eu 7 en 2023)

- **Ivanti** Connect Secure CVE-2023-46805 (janvier)
- **Fortinet** VPN SSL CVE-2024-21762 (février)
- **Cisco** ArcaneDoor CVE-2024-20359 (avril)
- **Palo Alto Networks** GlobalProtect gateway CVE-2024-3400 (avril)
- **Check Point** VPN CVE-2024-24919 (mai)
- **SonicWall** CVE-2024-40766 (août)
- **Ivanti** Cloud Services Appliance CVE-2024-8963 (octobre)
- **Fortinet** FortiManager CVE-2024-47575 (octobre)
- **Palo Alto Networks** CVE-2024-0012 (novembre)

Ces attaques ont montré que :

- **Les infections tout en mémoire sont devenus la norme** pour les attaquants avancés. Ou plus exactement les attaques sont simples et précises : l'attaquant installe un malware minimal en mémoire (dans un processus existant) qui exécute les commandes (ou les modules binaires additionnels) qui lui sont ensuite envoyés. Cela est vrai pour les attaques étatiques (par exemple ArcaneDoor sur Cisco), mais aussi pour certains attaques cybercriminelles.
- **Les attaquants s'installent sur les équipements moins surveillés.** Paradoxalement il s'agit par exemple des Firewalls et Appliances de sécurité qui sont des équipements sans EDR, et avec peu de mécanismes de surveillance interne (peu de logs sur le fonctionnement de l'appareil). On a vu aussi cette année des attaquants s'installer sur des équipements Big-IP mal sécurisés. Les IOT (Internet des Objets) présents dans l'entreprise seraient aussi de bons candidats.
- **Les malwares Linux/Unix augmentent.** Ceci est probablement simplement l'effet du constat précédent car beaucoup d'appliance fonctionnent sur Linux/Unix. On ne peut pas dire pour autant qu'il y a une baisse des infections visant Windows.

Les attaques incessantes sur les équipements de bordure, génèrent des crises et une fatigue croissante pour les équipes d'exploitation et les équipes sécurité. Cela a provoqué en 2024 un mouvement de réaction qui demande un changement de la part des éditeurs de logiciels. Nous traitons ce point à la section 2.6.

2.2 Les acteurs à l'origine des attaques

En 2024, c'est les attaques étatiques qui ont le plus attiré notre attention, et nous leurs consacrons la section 2.3. Mais bien sûr tous les acteurs ont été présents. Voici une revue sur chacun d'eux.

2.2.1 Etatiques

2.2.1.1 Attaques sophistiquées et discrètes

Les attaques réalisées par des Etats sont de toutes natures, mais se différentient des autres parce qu'elles sont :

- capables d'un haut niveau de sophistication,
- souvent discrètes et profondes, avec l'objectif de rester longtemps au sein de l'organisation attaquée (attaque de pré-positionnement).

Les Etats les plus cités dans les rapports sont inchangés (**les BIG-4**) : Chine, Russie, Corée du Nord et Iran.

Plusieurs personnes (exemple) ont fait remarquer en 2024 que l'on parlait peu des autres, et en particulier des activités offensives des pays occidentaux. Les raisons avancées sont d'une part le fait que ces attaques seraient plus discrètes, et d'autre part que cela pourrait générer des conflits d'intérêts (il serait délicat pour une société française de publier sur une attaque étatique française).

2.2.1.2 Désinformation et Info-Ops : un domaine à part entière de la trilogie offensive

2024 confirme une tendance apparue en 2016 (avec l'opération d'influence Russe sur les élections américaines) : les opérations d'influences malveillantes (parfois appelé « Malign Information Operation », **FIMI**, ou simplement **Info-Ops**) sont **de plus en plus présentes**, et la prise en compte de cette arme (d'un point de vue défensif au moins) est devenue indispensable pour les Etats.

La Russie est depuis plusieurs années le pays le plus cité pour ses opérations offensives dans ce domaine. **En 2024, on a aussi parlé de l'Iran, de la Chine et de l'Azerbaïdjan.**

Les capacités offensives des Etats

- D'un point de vue offensif, on observe généralement 3 capacités offensives utilisés par les Etats : les attaques cyber (DOS, sabotage, etc.), le cyber-espionnage et les opérations d'influence (guerre informationnelle).

- En France, la stratégie de défense définit 3 domaines pour le cyber : Lutte Informatique Défensive (LID) Lutte Informatique Offensive (LIO) et Lutte Informatique d'Influence (L2I).

2.2.2 Cyber-crime

2.2.2.1 Attaques éphémères guidées par le gain financier

Les cybercriminels cherchent avant tout le gain d'argent. Contrairement aux attaques étatiques, la discrétion ou les opérations de long terme ne les intéressent pas vraiment puisque la tactique la plus commune pour un groupe est de s'auto-dissoudre s'il devient trop visible, puis de renaitre sous une autre forme.

Les principaux domaines d'activité sont les escroqueries, les fraudes (fraudes bancaires, FOVI, attaques BEC, etc.) et le ransomware qui domine depuis 2019 les autres activités. Le vol de crypto-monnaie est aussi depuis plusieurs années un domaine extrêmement actif mais qui vise des cibles spécifiques (les détenteurs de crypto-actifs et les plateformes d'échange).

Depuis 2022, les Infostealers sont devenus un phénomène très répandu qui se maintient en 2024, sans évolution significative.

Nota : le terme de ransomware est utilisé désormais couramment pour désigner les attaques chiffrant les données de l'entreprise, aussi bien que celles où l'attaquant vol simplement les données (data exfiltration) et menace ensuite de les publier.

2.2.2.2 Quoi de neuf pour le ransomware ?

Les attaques de ransomware continuent d'augmenter, mais depuis 2 ans, il s'agit d'une **croissance linéaire, plutôt qu'exponentielle** (comme cela était le cas dans les années 2020/2021). En 2024, de l'ordre de 300 à 400 nouvelles victimes ont été annoncées chaque mois.

Les grands groupes de ransomware ont tendance à disparaitre, souvent suite à des opérations judiciaires lancées contre eux (voir ci-dessous), mais d'autres plus petits apparaissent sans cesse. C'est un peu comme si les opérations lancées contre un gros groupe ne faisaient que le fragmenter en une série de groupes plus petits.

Les groupes sur le déclin en 2024 : **LockBit 3.0** (quasiment à l'arrêt depuis août 2024, mais qui a annoncé un retour fin 2024 avec LockBit 4.0), **Cl0p** (qui a été très peu actif en 2024, jusqu'à son retour fin 2024 avec l'attaque Cleo) et **ALPHV/BlackCat** (qui s'est auto-dissous en mars 2024).

Du côté des groupes qui montent on trouve **RansomHub** qui est cité par tous les analystes comme le groupe le plus présent en 2024. D'autres groupes comme **PLAY**, **Medusa** et **Akira** sont également cités par certains analystes.

2.2.2.3 Un nombre sans précédent d'arrestations et de démantèlements

La lutte contre les ransomwares, et les malwares en général, a commencé à s'intensifier à partir de mai 2021 suite à l'attaque Colonial Pipeline. Ce phénomène n'a cessé de s'accroitre et **2024 a été une année record dans ce domaine** (SOCRadar donne une liste de 32 opérations judiciaires de premier plan réalisées en 2024).

Nous retiendrons en particulier :

- **Operation Cronos** (février) contre LockBit,
- **Operation Endgame** (mai) contre les Loaders IcedID, Pikabot, Trickbot, Bumblebee, Smokeloader, et SystemBC,
- Arrestation au Brésil du hacker nommé **USDoD** (octobre),
- **Operation Serengeti** (novembre) : arrestation de plus de 1000 cybercriminels en Afrique (action coordonnée par Interpol and Afripol),
- **Operation Passionflower** (décembre) démantèlement en Europe de la messagerie chiffrée MATRIX (coordonnée par Europol et Eurojust),
- **Operation PowerOFF** (décembre) contre 27 services de DDOS (opération conjointe impliquant 15 pays).

2.2.2.4 Nouvelle tendance : le Phishing as a Service (PhaaS)

Apparu en 2022 (avec des outils comme Caffeine et EvilProxy) le Phishing as a Service a fait une progression importante en 2024 avec des outils comme **Tycoon2FA**, **Rockstar 2FA** ou **SniperDZ**.

Les PhaaS sont des sites web payants (des services en mode SaaS) qui proposent une série d'outils pour réaliser une campagne de phishing : construction du mail de phishing, diffusion des mails et capture des mots de passe au travers de fausses pages web de login. Ils sont réputés être capables de contourner l'authentification 2FA car ils implémentent les attaques AiTM (Adversary in The Middle, technique où la victime se connecte sur un faux site web qui relaie le trafic vers le site légitime). Cette attaque fonctionne sur les systèmes MFA simples (SMS ou OTP) mais pas sur les systèmes plus avancés (que l'on qualifie de « Phishing résistant ») qui font de l'authentification mutuelle.

2.2.3 Hacktivisme

2.2.3.1 Très instrumentalisés par les attaquants étatiques

Les Hacktivistes sont très présents dans l'actualité 2024, surtout avec des attaques DDOS (typiquement les attaques pro-russes du groupe **NoName057**) et parfois aussi avec des attaques Hack&Leak ou même destructives (Ransomware, Wiper). Nous n'avons pas noté d'évolution technique significative par rapport en 2023.

La très grande majorité de ces attaques sont liées à des conflits armés : guerre de la Russie contre l'Ukraine (depuis 2022) et conflit entre le Hamas et Israël (depuis octobre 2023). Ces mouvements hacktivistes sont encouragés par les états (par exemple, la Cyber Army of Ukraine a été créée en 2022 par le gouvernement Ukrainien).

Créer ou influencer des groupes Hacktivistes est sans doute un des vecteurs utilisés par les Etats pour mener des actions cyber offensives (tout comme l'organisation d'actions de type Info-Ops).

2.2.3.2 Faible visibilité pour les groupes hacktivistes traditionnels (noyés dans la masse)

En dehors des actions hacktivistes liées aux conflits armés, les autres groupes hacktivistes (traditionnels) ont été peu vus dans l'actualité 2024, et n'ont pas eu d'effet significatif. On peut citer néanmoins par exemple l'action « Operation Free Durov » qui a été lancée suite à l'arrestation en France du PDG de Telegram. Il s'agissait d'une campagne d'attaques DDOS qui a duré plusieurs jours, mais qui ne s'est pas vraiment distinguées des attaques DDOS pro-russes réalisées par NoName057 à la même époque.

2.2.4 Des frontières floues entre ces groupes

Il devient parfois difficile de tracer une frontière entre les actions des différentes catégories d'attaquants :

- Les attaquants étatiques (surtout la Russie) cherchent à contrôler ou à influencer les actions de groupes cybercriminels ou de groupes hacktivistes,
- Certains Etats (surtout la Corée du Nord et l'Iran) réalisent des attaques dans un but financier (comme les cybercriminels).

Une 4eme catégorie est souvent aussi ajoutée aux 3 autres : les **« Hackers for Hire »** qui peuvent travailler soit pour des cybercriminels (en fournissant leur service à n'importe quel payeur), soit pour les Etats (en réalisant des attaques sur mesure et à la demande).

2.3 Zoom sur la menace étatique

Voici quelques-unes des attaques étatiques survenues en 2024 qui montrent le niveau de sophistication que peuvent atteindre ces attaquants.

2.3.1 Compromission de la messagerie interne de Microsoft par le groupe russe APT-29

En janvier 2024, Microsoft a annoncé que son système de mail Exchange Online interne avait été compromis en novembre 2023 par le groupe russe APT-29. Ce groupe (aussi appelé Midnight Blizzard ou Nobelium) dépend du SVR (le Service de Renseignement extérieur russe) et est considéré comme le groupe le plus avancé techniquement en Russie.

Cette attaque a permis à APT29 de voler les codes d'accès chez plusieurs clients Microsoft, y compris des agences gouvernementales américaines.

La technique d'attaque utilisée est remarquable par sa sophistication : elle montre que l'attaquant maitrise parfaitement l'environnement Cloud Azure, les mécanismes d'authentification et les droits d'accès associés :

- L'attaquant s'est introduit dans un tenant de test sur un compte ayant un mot de passe faible.
- Il a trouvé dans cet environnement une App de test qui avait été approuvée par un utilisateur privilégié dans l'environnement de production Microsoft.
- En réutilisant cette App approuvée, il a pu agir sur l'environnement de production, pour déclencher une série d'actions amenant à acquérir le droit d'accès sur toutes les boites à lettre Exchange.

Nota : Notre résumé ci-dessus est très schématique, mais montre bien la complexité de l'attaque et le fait qu'elle nécessite une parfaite connaissance des mécanismes d'authentification et des privilèges accordés aux Apps pour être mise en œuvre. SpecterOps et Wiz.io en donnent une description plus complète.

2.3.2 I-Soon, Pacific Rim et l'écosystème cyber offensif chinois

Tout comme en 2023, la Chine a été omniprésente dans l'actualité 2024 pour des attaques étatiques, principalement **Volt Typhoon** (Attaque contre les infrastructures critiques aux USA) et **Salt Typhoon** (Compromission de 9 opérateurs Télécom aux USA), mais aussi **Flax Typhoon** et **Silk Typhoon**.

[Taxonomie]

La plupart de ces groupes chinois étaient déjà connus avant sous d'autres noms, mais la nouvelle nomenclature Microsoft de 2023 les a rassemblés dans une famille utilisant le nom Typhoon. Ce changement renforce l'impression d'omniprésence de la Chine. CrowdStrike de son côté utilise la dénomination Panda (depuis 2015) mais elle est désormais moins courante que Typhoon.

Au-delà de ces attaques, plusieurs publications en 2024 ont montré comment l'Etat chinois a structuré son activité cyber-offensive. Voici les principales.

Fuite de données I-Soon. En février 2024 un inconnu a posté sur Github des documents volés à la société chinoise I-Soon. Ils montrent que cette société travaille principalement pour le gouvernement chinois. I-Soon fournit des services d'intrusion et d'espionnage et met en avant sa capacité à analyser et synthétiser les documents volés. Elle n'aurait pas de capacités d'attaques avancées et se contenterait d'attaques simples au moyen de phishing. Les documents I-Soon montrent aussi que le gouvernement chinois distribue les 0-days découverts lors des concours nationaux comme Tianfu Cup, à toute une série de sociétés cyber-offensives chinoises.

Botnets ORB chinois. On a beaucoup parlé en 2024 de ces botnets mis en place par la Chine. Chaque nœud du botnet est un ORB (Operational Relay Box), c'est-à-dire une machine compromise qui sert à masquer l'attaquant. **KV-Botnet** (vu lors d'attaques Volt Typhoon), **ORBWEAVER** et **Raptor Train** (vus lors d'attaques Flax Typhoon) sont 3 exemples de botnets ORB chinois révélés en 2024. Ce type de botnet a aussi été mis en place par d'autres Etats. En 2014, après l'affaire Snowden, on avait parlé de projets similaires : **HACIENDA** (Royaume-Uni) et **LANDMARK** (Canada). En 2028 le botnet Russe **VPNFilter** (mis en place pour attaquer l'Ukraine) avait été découvert.

Sophos Pacific Rim. Fin octobre 2024, Sophos a publié une série d'articles intitulée « Pacific Rim » qui décrit 5 années d'attaques (de 2018 à 2023) par des acteurs étatiques chinois contre les Firewall de Sophos. Cette publication montre en particulier l'organisation de l'écosystème offensif :

- Les exploits 0-days contre Sophos Firewall ont été développés au sein d'une université chinoise (l'université technologique UESTC de la ville de Chengdu dans la province du Sichuan).
- Ils ont ensuite été utilisés par plusieurs groupes chinois (Volt Typhoon, APT31 et APT41/Winnti).

2.3.3 9 opérateurs Télécom aux Etats-Unis compromis par le groupe chinois Salt Typhoon

En octobre 2024 il a été annoncé que le groupe chinois **Salt Typhoon** avait réussi à s'installer dans les réseaux internes de plusieurs opérateurs de Télécommunication aux Etats-Unis et en particulier chez AT&T, Verizon et Lumen. Les attaquants auraient (selon les déclarations officielles) :

- Eu accès aux données relatives aux écoutes légales des communications (ce qui permet de savoir qui a été placé sous écoute par le gouvernement américain),
- Espionné les communications d'un nombre limité de personnes (des personnalités politiques),
- Volé les métadonnées relatives aux appels des abonnés téléphoniques (customer call records).

L'attaque aurait duré un an ou plus et serait due (en partie au moins) à un niveau de sécurité insuffisant dans les infrastructures des opérateurs Télécom.

C'est l'une des attaques les plus marquante de l'année et elle a été très médiatisée jusqu'à la fin de l'année 2024.

2.4 Les attaques dans le Cloud

2.4.1 SaaS, IaaS, M365 et On-Premise : une architecture complexe

Pour les entreprises, le Cloud actuel est le plus souvent constitué de 3 composants, avec chacun ses spécificités en termes de sécurisation.

- **SaaS** : l'ensemble des services SaaS utilisés par l'entreprise. Par exemple ServiceNow, SalesForce, etc. C'est sans doute le composant le plus facile à gérer en termes de sécurité car c'est le fournisseur SaaS qui a la responsabilité du maintien du niveau de sécurité de la solution. Par contre l'entreprise utilisatrice n'a en général que très peu de visibilité sur les événements de sécurité qui s'y produisent (pas de supervision).
- **IaaS** : les applications de l'entreprise déployées dans le Cloud avec Azure, AWS et Google Cloud. On retrouve ici à peu près les mêmes problèmes, pour le maintien du niveau de sécurité, que dans le cas des applications on-premise. L'attaque la plus courante est l'exploitation d'une vulnérabilité.
- **M365** : l'environnement de bureautique et de collaboration. La principale difficulté ici est sans doute de gérer les identités et les droits d'accès. Le vol de comptes (phishing) est l'attaque la plus courante.

En plus de ces composants Cloud, les entreprises ont aussi des services on-premise qui correspondent soit à des applications historiques, soit à des besoins spécifiques. Ces services peuvent aussi avoir besoin d'interagir avec l'infrastructure Cloud.

2.4.2 Des attaquants de plus en plus compétents

Le nombre d'attaques affectant les infrastructures Cloud augmente. Nous n'avons pas de chiffre précis sur ce phénomène, mais nous l'observons au travers des rapports que nous analysons dans le cadre de notre service de « Veille sur les attaques et IOC ». Et cette augmentation est plutôt logique puisque le Cloud représente une part croissante des systèmes d'information des entreprises.

Crowdstrike fournit des chiffres intéressants sur ce sujet dans son rapport Global Threat Report 2024 (traitant des incidents 2023) :

- Il indique une **croissance de + 75 %** des intrusions dans les environnements Cloud
- Dans la majorité des cas, l'attaquant ne sait même pas qu'il est dans le Cloud : il a exploité une vulnérabilité à distance et a compromis une machine hébergée dans le Cloud. Il n'a tenté aucune attaque contre l'environnement Cloud lui-même.
- Mais un nombre croissant d'attaquants ont conscience qu'ils sont dans le Cloud et tentent d'exploiter ses spécificités. Ils peuvent par exemple obtenir des privilèges pour accéder à d'autres ressources Cloud, créer leurs propres VM, etc. Ces attaquants, que CrowdStrike qualifie de **« Cloud-conscious » sont en croissance de 110 %** par rapport à l'année précédente alors que les « Cloud-agnostics » (la catégorie précédente) sont en croissance de 60 %.

Nota : l'année 2023 (couverte dans le rapport de Crowdstrike) nous semble une année charnière où on a vu des attaquants très agiles dans des environnements Cloud (comme par exemple Scattered Spider)

réaliser des attaques spectaculaires que l'on qualifie désormais de « Cross-domain » : une attaque débute sur un poste de travail Windows compromis (domaine 1) puis se propage sur un serveur Linux dans le Cloud (domaine de compétence 2) puis parvient à prendre pied dans la couche de gestion du Cloud (domaine de compétence 3), etc.

2.5 Les attaques de la Supply-chain

Depuis 2020 au moins (et l'attaque SolarWinds au moyen d'une mise à jour piégée), le danger des attaques de la Supply-chain est bien connu. Ces attaques peuvent prendre de multiples formes mais ce sont **les attaques de la supply-chain logicielle** qui sont les plus fréquentes. En 2024 on a vu à nouveau de multiples cas où des bibliothèques logicielles mises à disposition sur Internet avaient été piégées avec un malware. Le plus souvent il s'agit de packages NPM (packages JavaScript pour Node.js).

Ci-dessous nous donnons 3 exemples d'attaques de la supply-chain vues en 2024 qui nous paraissent les plus intéressantes. Les 2 premières appartiennent à la catégorie des attaques de la supply-chain logicielle.

2.5.1 Attaque XZ-Utils

Cette attaque est considérée comme l'une des plus marquantes de l'année2024.

Fin mars 2024, il a été découvert qu'un attaquant nommé **Jia Tan** (probablement un nom d'emprunt) avait piégé le **projet open-source « XZ Utils »** (qui fournit la libraire de compression « liblzma », utilisée par de nombreux logiciels) pour introduire une backdoor dans le serveur OpenSSH sur un grand nombre de systèmes Linux. Cette attaque est remarquable parce que :

- Elle visait OpenSSH de façon détournée (via une librairie),
- Elle a été longue et discrète : Jia a commencé à contribuer au projet XZ Util en 2021, d'abord de façon très modeste, puis ensuite a introduit sa backdoor progressivement dans la chaine de fabrication de la librairie,
- La backdoor est sophistiquée et l'OPSEC (les mesures de sécurité pour ne pas laisser de traces permettant de remonter à l'attaquant) très soignée.

Ces différents éléments font penser qu'il s'agit d'une mission réalisée par un groupe d'attaquants très avancé.

Malheureusement pour eux (et heureusement pour nous !), après presque 3 ans d'efforts (de 2021 à 2024), la backdoor a été découverte 20 jours après l'introduction dans le projet du dernier élément permettant de la rendre active. Le développeur **Andres Freund** l'a découverte parce qu'il a remarqué que son serveur OpenSSH consommait trop de CPU …

Cet exemple montre à la fois la faiblesse des logiciels open-source (qui peuvent être compromis par des contributeurs malveillants) **et sa force** aussi puisque l'examen du code par un passionné a permis de mettre à jour rapidement la malveillance.

2.5.2 *Attaque Polyfill.io*

Polyfill.js est une librairie JavaScript assez populaire utilisée par environ 4% des sites web. Elle est distribuée par plusieurs sources mais beaucoup de sites web utilisent le site de distribution cdn[.]polyfill[.]io

En février 2024, la société chinoise Funnull a racheté le domaine polyfill[.]io et, en juin des chercheurs se sont rendu compte que la librairie Polyfill.js distribuée par ce domaine était désormais malveillante (renvoi vers des sites publicitaires, et injection de malwares sur les téléphones mobiles).

Tous les sites web qui faisaient directement référence à cdn[.]polyfill[.]io se sont alors mis à distribuer des contenus malveillants à leurs propres visiteurs.

Cet incident illustre un cas d'attaque de la supply-chain logicielle qui (à notre connaissance) n'avait pas été vue auparavant.

2.5.3 *Attaques SaaS contre Snowflake et BlueYonder*

Il s'agit de 2 attaques qui ont visé des solutions SaaS, ce qui est nouveau dans le paysage de la cybermenace.

Snowflake.com, qui propose des services de stockage et d'analyse de données dans le Cloud, a subi une série d'attaques visant ses clients. Fin mai 2024, c'est d'abord des données de **TicketMaster** (vente de places de spectacle) et **Santander** (banque espagnole) qui ont été volées chez Snowflake. L'analyse publiée par Mandiant montrera que plus de 165 clients de Snowflake ont été affectés, et **AT&T** annoncera en juillet qu'elle est une des victimes. Il a d'abord été soupçonné que Snowflake était responsable de l'intrusion (un compte d'employé aurait été piraté et des vulnérabilités exploitées) mais ce point a été démenti par Mandiant qui a analysé l'incident. Ce sont en fait des comptes de clients qui ont été volés (via des Infostealers puis postés sur de sites de revente underground) et utilisés pour accéder à leurs données stockées chez Snowflake. Mandiant précise que certaines victimes étaient des sous-traitants qui géraient plusieurs clients (compromettre un sous-traitant permet alors de lui voler les compte Snowflake de tous ses clients). Les attaquants ont été identifiés et arrêtés en fin d'année.

BlueYonder.com, qui propose des services Cloud pour gérer et optimiser la Supply-chain (fabrication, acheminement et points de vente), a subi en novembre 2024 une attaque de ransomware qui a rendu son service SaaS indisponible pour plusieurs clients comme par exemple **Starbucks** aux Etats-Unis, des chaines de supermarchés au Royaume-Uni (**Morrisons** et **Sainsbury's**) ou **BIC** en France. L'attaque a été attribuée au groupe Termite et pourrait être liée aux attaques Cleo revendiquées par le groupe ClOp en fin d'année 2024 (mais ce point est démenti par BlueYonder).

Les services SaaS sont des proies intéressantes pour les cybercriminels car ils peuvent faire pression à la fois sur les clients mais aussi sur le fournisseur de la solution Cloud. Après ces 2 attaques vues en 2024, Il est probable que ce type d'attaque augmente dans les années à venir.

2.6 La nécessaire responsabilisation des éditeurs

La multiplication des compromissions sur des équipements de bordure en 2024 (cf. § 2.1.3) a fait monter le mécontentement dans les entreprises qui utilisent ces produits : dans les équipes qui gèrent ces équipements (qui doivent trop souvent appliquer des nouveaux correctifs urgents) et dans les équipes CERT responsables de la sécurité de l'entreprise.

Ce mouvement rejoint une protestation plus ancienne et plus large (non limitée aux failles sur les équipements de bordure), face au flux incessant des correctifs publiés par les éditeurs. Face à ce « trop de correctifs de sécurité » les responsables des systèmes en opération demandent aux éditeurs une plus grande qualité (fiabilité) dans les logiciels qu'ils commercialisent.

Ces sujets ont beaucoup été abordé en 2024 dans les discussions entre les CERT. Et les instances gouvernementales semblent aussi partager ces préoccupations : l'Europe travaille depuis plusieurs années sur le cadre réglementaire et les Etats-Unis, avec une approche tout à fait différente, ont lancé l'initiative « Secure By Design » de la CISA.

Nous développons ces sujets ci-dessous.

2.6.1 Le renforcement progressif du cadre légal européen

Voilà ci-dessous ce que nous disions dans la Une du bulletin mensuel Cert-IST d'octobre 2024.

De plus en plus de voix demandent que soient définies des obligations légales pour les fournisseurs sur la fiabilité (en particulier en termes de sécurité) de leurs solutions logicielles et matérielles.
Par exemple, l'association InterCERT France (à laquelle le Cert-IST participe activement) a publié mi-octobre, un communiqué et un article sur ce sujet. Partant du constat des multiples vulnérabilités de certaines appliances de sécurité (on peut penser par exemple à Ivanti ICS), l'association appelle à légiférer pour engager la responsabilité des éditeurs. Elle propose aussi d'autres pistes (en alternative à l'utilisation de produits peu robustes) : utiliser des produits qualifiés ou dans certains cas, des solutions Open-sources.
D'autres initiatives vont aussi dans ce sens. Par exemple, au niveau européen :

- L'obligation de signalement à l'ANSSI des vulnérabilités 'significatives' (issue de la loi de programmation militaire), publié en mai 2024, qui oblige les constructeurs à signaler à l'ANSSI les vulnérabilités et incidents les plus graves.
- La directive du Conseil de l'Europe publiée en octobre 2024 qui propose d'inclure les logiciels et matériels dans la protection du consommateur en cas de produit défectueux.
- Le règlement Européen CRA (EU Cyber Resilience Act) qui devrait entrer en vigueur en 2027, et dont l'objectif est de rééquilibrer les responsabilités entre les fournisseurs et les utilisateurs finaux.

Comme le dit cette analyse (intitulée « The EU Throws a Hand Grenade on Software Liability »), l'Europe est plus active que les Etats-Unis sur ce domaine.

On pourra noter cependant qu'en octobre 2024, la SEC américaine a condamné Unisys, Avaya, Check Point et Mimecast pour avoir minimisé l'ampleur des intrusions qu'elles ont subies en 2020 lors de l'attaque SolarWinds. Le domaine est ici différent (on condamne un manque de loyauté vis-à-vis des

actionnaires). Certains ont fait remarquer aussi que les montants des amendes (de l'ordre de 1 million de dollars) sont faibles pour ces grandes sociétés.

On peut citer aussi l'initiative « Secure By Design » de la CISA, qui encourage les vendeurs à mettre en place une série de bonnes pratiques de sécurité. Plutôt que d'assigner une responsabilité légale, cette approche plus douce demande aux vendeurs d'adhérer volontairement à un modèle vertueux. Près de 300 sociétés s'y sont déjà engagées

2.6.2 Les efforts entrepris par certains éditeurs

Les éditeurs d'équipements de sécurité sont bien sûr conscients que les multiples attaques observées depuis 2019 sur les équipements de bordure (et en particulier les serveurs VPN) sont un problème. Ils sont d'ailleurs soumis à une forte pression quand ils doivent fournir dans l'urgence des solutions suite à une attaque touchant leurs équipements.

Comme nous le disions plus haut, un grand nombre d'entre eux ont pris des engagements (moraux) pour fournir des solutions plus sures. Sans minimiser l'importance de tels engagements, nous avons aussi noté d'autres actions plus concrètes qui vont dans le sens d'une amélioration :

- **Sophos** a expliqué dans son étude **« Pacific Rim »** (que nous avons déjà citée au § 2.3.2 et à laquelle nous avons consacré un article de notre bulletin mensuel) qu'il pourrait protéger plus efficacement ses clients s'il avait plus de contrôle sur les équipements Sophos Firewall de ses clients (en termes de télémétrie, de supervision et même de déploiement de correctifs urgents). L'éditeur est en effet bien placé pour observer et contrer les attaques « globales » qui sont lancées contre un type d'équipement (cas d'une vague d'attaques 0-day). Cette proposition soulève plusieurs problèmes (par exemple la perte de souveraineté pour l'entreprise et le risque de panne en cas de mise à jour inopinée). Cependant, elle peut être comparée à l'approche Cloud où la responsabilité du maintien de la plate-forme est confiée au fournisseur : si un cadre (contractuel, technique, …) est clairement défini, et si les clients ont confiance a priori en leur fournisseur de firewall, celui-ci pourrait s'engager à gérer les firewalls installés chez ses clients (maintien du niveau de sécurité).

- **Palo Alto Networks** a indiqué à l'occasion des attaques au moyen de la vulnérabilité 0-day CVE-2024-0012 (en novembre 2024, cf. notre alerte **CERT-IST/AL-2024.019**) qu'il fait régulièrement des scans sur Internet pour identifier les équipements Palo Alto Networks dont l'interface d'administration est accessible sur Internet (ce qui est un risque de sécurité), et qu'il prévient les clients concernés. Cette démarche pro-active pour protéger ses clients nous semble nouvelle et appréciable.

3 Productions du Cert-IST en 2024

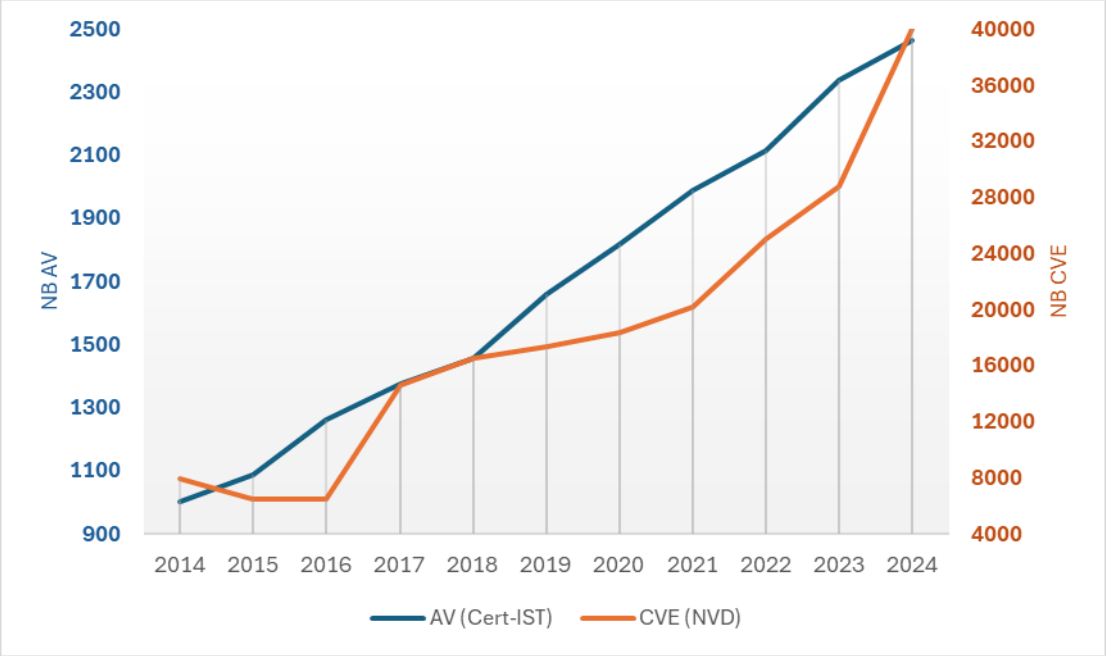
3.1 Veille sur les vulnérabilités et les menaces

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 2024.

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 2024

Alerte	Référence	Description	Date
Orange	CERT-IST/AL-2024.001	Attaques en cours visant **Ivanti Connect Secure** (ICS) (CVE-2023-46805, CVE-2024-21887, etc.)	11-janv-24
Jaune	CERT-IST/AL-2024.002	Attaques en cours visant **GitLab** (CVE-2023-7028)	12-janv-24
Jaune	CERT-IST/AL-2024.003	Attaques en cours visant **Atlassian Confluence** (CVE-2023-22527)	23-janv-24
Jaune	CERT-IST/AL-2024.004	Risque d'attaques visant les équipements fonctionnant sur **FortiOS** (CVE-2024-21762)	08-févr-24
Orange	CERT-IST/AL-2024.005	Attaques en cours visant les équipements fonctionnant sous **PAN-OS** (CVE-2024-3400)	12-avr-24
Orange	CERT-IST/AL-2024.006	Attaques en cours visant **CrushFTP** (CVE-2024-4040)	26-avr-24
Orange	CERT-IST/AL-2024.007	Attaques en cours visant les **VPN Check Point** (CVE-2024-24919)	30-mai-24
Jaune	CERT-IST/AL-2024.008	Attaques en cours visant **PHP sur Windows** (CVE-2024-4577)	11-juin-24
Jaune	CERT-IST/AL-2024.009	Risque d'attaques contre **OpenSSH** (CVE-2024-6387)	02-juil-24
Jaune	CERT-IST/AL-2024.010	Risque d'attaques visant les équipements **Cisco Secure Email Gateway** (CVE-2024-20401)	18-juil-24
Jaune	CERT-IST/AL-2024.011	Risque d'attaques contre **SPIP** (CVE-2024-7954)	30-août-24
Jaune	CERT-IST/AL-2024.012	Risque d'attaques visant **Microsoft Windows** (CVE-2024-43491)	11-sept-24
Jaune	CERT-IST/AL-2024.013	Risque d'attaques visant **Ivanti Endpoint Manager** (EPM) (CVE-2024-29847)	16-sept-24
Jaune	CERT-IST/AL-2024.014	Risque d'attaques sur les produits utilisant la **librairie Ruby-SAML dont GitLab** (CVE-2024-45409)	19-sept-24
Jaune	CERT-IST/AL-2024.015	Risque d'attaques visant les systèmes Linux/Unix utilisant **CUPS** (CVE-2024-47176, CVE-2024-47177, etc.)	27-sept-24
Jaune	CERT-IST/AL-2024.016	Attaques en cours visant **Zimbra Collaboration Suite** (CVE-2024-45519)	02-oct-24
Orange	CERT-IST/AL-2024.017	Attaques en cours visant **Fortinet FortiManager** (CVE-2024-47575)	24-oct-24
Jaune	CERT-IST/AL-2024.018	Risque d'attaques sur **Citrix Virtual Apps and Desktops** (anciennement XenApp et XenDesktop) avec CVE-2024-8068 et CVE-2024-8069	14-nov-24
Orange	CERT-IST/AL-2024.019	Attaques en cours visant les pares-feux de **Palo Alto Networks** (CVE-2024-0012)	18-nov-24
Jaune	CERT-IST/AL-2024.020	Risque d'attaques contre **Apache Struts 2** (CVE-2024-53677)	17-déc-24
Jaune	CERT-IST/AL-2024.021	Risque d'attaques contre **Beyond Trust Remote Support** (CVE-2024-12356)	20-déc-24

3.1.3 Les fiches attaques pour 2024 (hors menaces récurrentes)

Fiche	Nom	Description
CERT-IST/ATK-2024.008	**UNC4841**	Un groupe de cyber-espionnage potentiellement lié à l'Etat chinois
CERT-IST/ATK-2024.012	**BianLian**	Un groupe cybercriminel spécialisé en vol et extorsion de données
CERT-IST/ATK-2024.013	**VexTrio**	Un important programme d'affiliation cybercriminel basé sur la redirection de trafic web (TDS)
CERT-IST/ATK-2024.014	**Blackwood**	Un groupe de cyber-espionnage ciblant des individus et des entreprises en Chine et au Japon
CERT-IST/ATK-2024.035	**Magnet Goblin**	Un acteur cybercriminel expert dans l'exploitation de vulnérabilités 1-day
CERT-IST/ATK-2024.039	**Earth Krahang**	Un groupe d'origine chinoise peut-être lié à I-Soon et spécialisé dans l'obtention d'accès initiaux
CERT-IST/ATK-2024.047	**CoralRaider**	Un acteur à motivation financière avec des origines vietnamiennes
CERT-IST/ATK-2024.056	**Black Basta**	Un groupe de ransomware visant les infrastructures critiques en Europe et aux Etats Unis
CERT-IST/ATK-2024.057	**Ebury**	Une menace persistante pour les serveurs Linux, ciblant les cryptomonnaies et les données financières
CERT-IST/ATK-2024.058	**Void Manticore**	Un acteur iranien combinant des opérations de destruction et d'influence
CERT-IST/ATK-2024.060	**Doppelganger**	Campagne de désinformation prorusse ciblant l'Allemagne, la France et d'autres pays européens
CERT-IST/ATK-2024.070	**SneakyChef**	Un groupe de cyberespionnage exploitant les RAT Gh0st et SpiceRAT
CERT-IST/ATK-2024.082	**NullBulge**	Un groupe cybercriminel prétendant défendre les artistes contre l'IA
CERT-IST/ATK-2024.083	**Stargazer Goblin**	Un acteur organisant la distribution de malware via Github
CERT-IST/ATK-2024.092	**Silver Fox**	Un groupe cybercriminel ciblant des secteurs critiques en Chine
CERT-IST/ATK-2024.103	**Earth Baxia**	Attaques chinoises sophistiquées contre des gouvernements et entreprises en région APAC
CERT-IST/ATK-2024.104	**SloppyLemming**	un groupe cybercriminel utilisant le cloud pour de l'espionnage en Asie du Sud et de l'Est
CERT-IST/ATK-2024.114	**UAC-0184**	Campagnes de spear-phishing visant la défense ukrainienne
CERT-IST/ATK-2024.125	**Emennet Pasargad**	Société iranienne proche de l'IRGC menant des opérations de désinformation et de déstabilisation incluant le hack-and-leak
CERT-IST/ATK-2024.126	**Mysterious Elephant**	Un groupe de type APT ciblant gouvernements et populations en Asie du Sud
CERT-IST/ATK-2024.137	**Head Mare**	Groupe hacktiviste ciblant la Russie et la Biélorussie avec des ransomwares

3.2 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

Un prolongement de l'année 2023

Globalement l'année 2024 confirme les tendances des années précédentes, avec néanmoins quelques évolutions notables.

L'attaque des équipements de bordures (comme Ivanti ICS ou Fortinet) reste le fait le plus marquant de l'année. En 2023 nous avions mis l'accent sur la difficulté à désinfecter les équipements attaqués et posé la question de « Remplacer plutôt que réparer ? ». En 2024, ces attaques profondes se sont poursuivies et même généralisées ; aucun constructeur ne semble épargné, avec cette année des attaques contre Check Point, Cisco, Fortinet, Ivanti, Juniper, Palo Alto Networks, SonicWall et Sophos. En réponse à cette tendance, nous avons observé en 2024 une demande croissante, de la part des utilisateurs mais aussi des instances gouvernementales, **pour que les éditeurs améliorent la qualité de leurs produits et prennent des mesures pour endiguer ces compromissions à répétition.** Cela se traduit en Europe par un appel pour une responsabilité légale des éditeurs, et aux Etats-Unis par un appel à un engagement des fournisseurs sur les bonnes pratiques (cf. l'initiative « Secure By Design » de la CISA). La section 2.6 développe ces 2 aspects.

Pour le cybercrime, les attaques ne faiblissent pas. Le ransomware (chiffrement de données ou menace de divulgation des données volées) reste la menace la plus présente et la plus médiatisée. Après une année au sommet en 2023, le groupe LockBit a largement décliné en 2024 (avec seulement 4 attaques revendiquées au dernier trimestre). C'est l'un des effets du **nombre record d'arrestations et d'opérations de démantèlement** menées par les autorités judiciaires en 2024. Le vide laissé par LockBit a malheureusement été rapidement comblé par d'autres groupes d'attaquants (en particulier **RansomHub**). Mais les actions judiciaires vues en 2024 mettent une pression certaine sur cet écosystème et inversent la tendance de quasi-impunité qui était présente il y a quelques années.

En plus des attaques par **Infostealers** (toujours très présents depuis 2022), l'année 2024 a été marquée par une augmentation des attaques de **phishing visant Microsoft 365** au moyen de services **PhaaS** (Phishing as a Service) tels que **Tycoon 2FA**. Ces outils sont capables de contourner les protections MFA standards en mettant en œuvre l'attaque **AitM** (Adversary in the Middle). Pour les empêcher, il nécessaire de renforcer la protection avec des solutions MFA dites « phishing resistant ».

Dans le domaine étatique, les attaques des **BIG-4 (Chine, Russie, Corée du Nord et Iran)** restent les plus médiatisées. Comme en 2023, la Chine a été omniprésente dans l'actualité 2024, et cette années c'est en particulier **l'écosystème offensif mis en place par le gouvernement chinois** qui a été décrit (collecte des 0-day, sociétés spécialisées cyber-offensives comme I-Soon, botnet ORB, etc. cf. § 2.3.2) .

2024 se caractérise aussi par le **grand nombre d'opérations d'influences** (attaques informationnelles appelée **FIMI** en Europe, et communément **Info-Ops**) qui ont été réalisées par certains Etats, en tout premier la Russie et la Biélorussie, mais aussi l'Iran, la Chine et l'Azerbaïdjan.

Les sujets d'attention pour 2025

Les 2 sujets qui retiendront probablement le plus l'attention des entreprises en 2025 seront selon nous :

- **Les attaques contre les appliances de sécurités** (tel que les firewalls et les VPN) et plus généralement contre les équipements moins surveillés (typiquement non équipés d'EDR) qui sont exposés sur Internet. Un des premiers objectifs ici est de s'assurer que ces équipements ne sont pas oubliés en termes de surveillance. La détection d'anomalies de fonctionnement, la surveillance de l'intégrité de la plate-forme et la surveillance des flux provenant de ces équipements (plutôt que les flux en transit) sont par exemple des points à renforcer.

- **La sécurité du Cloud.** Ce domaine vaste et complexe occupe de plus en plus une place centrale dans les systèmes d'information des entreprises. Les attaques sont ici en croissance avec de multiples domaines à couvrir, par exemple :

    - La gestion des identités et des accès,
    - La complexité technique des solutions déployées par l'entreprise,
    - Le niveau de sécurité des solutions SaaS utilisées.

Parmi les autres sujets importants nous avons noté pour 2025 :

- La sécurité de la Supply-Chain,
- La prise en compte des nouveaux cadre réglementaire (NIS2 et CRA),
- L'identification des menaces liés au déploiement des solutions d'Intelligence Artificielle

Renforcer la maîtrise des intrusions

2024 a montré à nouveau que certains attaquants peuvent être très forts (cf. certaines des attaques étatiques décrites à la section 2.3) et que certains des équipements de sécurité peuvent avoir des vulnérabilités 0-day faciles à exploiter (le terme de « vulnérabilité impardonnable » est de plus en plus utilisé). **Dans ce contexte, l'entreprise doit être prête à faire face à des intrusions réussies.**

Cela implique de renforcer la sécurité à chacune des étapes de l'intrusion :

- En amont en poursuivant les efforts de sécurisation, en particulier sur l'application des correctifs de sécurité,
- Sur la détection des intrusions réussies, par exemple au moyen de leurres (canary, honey-token, etc.),
- En aval, en s'entrainant à la gestion des crises cyber.

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