CERT-IST

INDUSTRIE | SERVICES | TERTIAIRE

Bilan Cert-IST des failles et attaques de 2023

Publié en Février 2024

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 d'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 2024.

> ➢ **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 2023

Nous traitons d'abord les phénomènes les plus importants pour les entreprises :

- Les 4 attaques les plus marquantes : **Barracuda ESG** (CVE-2023-2868), **MOVEit Transfer** (CVE-2023-34362), **3CX** (CVE-2023-29059) et **Citrix NetScaler** (juillet et octobre)
- L'augmentation des 0-day,
- Les attaques sur les équipements de bordure,
- Les nouvelles attaques cybercriminelles (en plus des ransomwares et des attaques BEC) : attaques du type MOVEit, l'ingénierie sociale avancée et la chasse aux données d'accès,
- Et les autres faits remarquables : DDOS pro-russe, utilisation d'outil de RMM, attaques contre VMware ESXi et les phishings OneNote ou Teams.

Nous passons ensuite en revue les autres éléments marquants :

- Crypto-monnaies : cible favorite pour de nombreux attaquants,
- Cyberguerre : l'importance croissant de l'arme cyber pour les états,
- L'omniprésence de la Chine sur le domaine cyber-offensif se poursuit,
- Pegasus et Predator : les usages abusifs des outils de surveillance continuent.

2.1 Faits marquants pour les entreprises

2.1.1 Les attaques les plus marquantes de 2023

Les attaques sont présentées par ordre d'importance, en commençant par la plus marquante. Nous rappelons ensuite dans un tableau récapitulatif, toutes les alertes émises par le Cert-IST en 2023.

Mai 2023 : Attaque contre les équipements **Barracuda ESG** (CVE 2023 2868)

En bref : En mai 2023 Barracuda découvre qu'une vulnérabilité 0-day a permis à un attaquant chinois (le groupe UNC4841 selon Mandiant) de compromettre les passerelles de messageries Barracuda Email Secure Gateway (ESG) de 5% de ses clients. L'attaque a débuté en octobre 2022. Lorsque Barracuda analyse l'attaque en mai 2023, il se rend compte que les équipements compromis ont été profondément modifiés par l'attaquant et recommande de les changer plutôt que de tenter de les réparer !

A retenir : Outre cette recommandation inédite (cela ne s'était jamais produit à notre connaissance), cette attaque est remarquable parce qu'elle réunit beaucoup d'éléments caractéristiques des attaques vues en 2023 (que nous développons plus loin dans ce rapport) :

- C'est une attaque au moyen d'une **0-day** (cf. § 2.1.2)
- Qui vise un équipement de bordure (cf. 2.1.3) et le **compromet en profondeur** (dissimulation de backdoors, résistance aux tentatives de désinfection et effacement des logs),
- Elle est réalisée par un groupe étatique **chinois** (cf. § 2.2.3).

Mai 2023 : Attaque **MOVEit Transfer** (CVE 2023 34362)

En bref : Des cybercriminels associés au groupe Cl0p utilisent une vulnérabilité 0-day dans le produit MOVEit Transfer (qui permet de partager des fichiers avec des tiers) pour voler tous les documents qu'ils peuvent, dans les entreprises qui utilisent ce produit. Ils font ensuite du chantage et menacent de rendre publics ces documents.

A retenir : Le nombre de victimes de cette attaque est impressionnant (2600 sociétés auraient été impactées) ; certaines sont des victimes directes (elles utilisent le produit MOVEit Transfer) et d'autres sont des victimes indirectes (des données qui les concernent ont été volées chez les victimes directes).

Le fait d'utiliser une vulnérabilité 0-day est une tendance nouvelle chez les cybercriminels, car jusqu'à maintenant ils utilisaient plutôt des vulnérabilités déjà connues (des 1-day ou des n-days) pour organiser des campagnes d'attaques massives. Ces attaques 0-day avaient déjà été vues en janvier 2021 (attaque visant Accellion FTA), mais la tendance s'est accélérée en 2023 avec les attaques Aspera Faspex (Janvier 23), GoAnywhere MFT (Février 23), PaperCut (avril 23).

Avril 2023 : Attaque "double-Supply Chain" contre les **soft-phones 3CX** (CVE-2023-29059)

En bref : En avril 2023 des alertes EDR montrent que l'application de téléphonie 3CX sur PC a été piégée à l'insu de 3CX (attaque de la Supply Chain logicielle chez 3CX). L'enquête montrera que l'attaque a visé d'abord MacOS (avant Windows) et que 3CX a été infectée plusieurs mois auparavant parce qu'un employé a téléchargé un logiciel financier (X_TRADER) qui avait été lui aussi piégé par une attaque de la Supply Chain (attaque du fournisseur de X_TRADER, probablement en février 2022). Toute cette série d'attaques est attribuée à un groupe dépendant du gouvernement de Corée du Nord.

A retenir : Outre la double attaque de la Supply Chain (qui est le point le plus intéressant de cette attaque), on retrouve ici des motivations et modes opératoires bien connus : la Corée du Nord vise souvent les crypto-monnaies, et piéger un logiciel financier est donc logique. Comme beaucoup d'attaquants d'une certaine envergure, elle sait aussi s'adapter en fonction des résultats obtenus et progresser de cible en cible sur plusieurs années.

Juillet et octobre 2023 : Attaques contre **Citrix NetScaler**

En bref : Les équipements Citrix Netscaler ont subi 2 fois en 2023 des attaques massives qui ont permis de compromettre un grand nombre d'équipements. Il s'agit d'attaques classiques, où la majorité des compromissions sont arrivées alors que les correctifs étaient disponibles.

A retenir : Pour l'attaque de juillet, il ne s'agit pas d'une 0-day, mais les premières attaques se sont produites 2 jours seulement après l'annonce des correctifs. La rapidité s'explique sans doute par le fait que des attaques massives visant le même type d'équipements s'étaient déjà produites en janvier 2020 ; certains attaquants connaissent donc bien cette cible et savent déployer des attaques éclairs. Sur beaucoup de machines, les patches ont été déployés trop tard : une backdoor avait déjà été déposée et elle n'a pas été détectée lors de l'application des patches.

L'attaque d'octobre est une attaque 0-day (car les premières cas d'attaques ont été datée d'août 2023), mais la majorité se sont produites 15 jours après la publication des correctifs. La chronologie des événements est ici très classique :

- annonce de la vulnérabilité lors de la publication des correctifs,
- puis publication des détails techniques et d'un programme d'exploitation quelques jours plus tard,
- et enfin attaques par un grand nombre d'acteurs différents (ruée).

Cette vulnérabilité permet de voler à distance des fragments de mémoires qui contiennent en clair des jetons de sessions avec lesquels on peut ensuite se connecter sur l'équipement vulnérable. Elle a été surnommée **CitrixBleed**, en référence à la célèbre attaque HeartBleed dans OpenSSL survenue en 2014, et qui était elle aussi une fuite mémoire révélant des données critiques (clés cryptographiques).

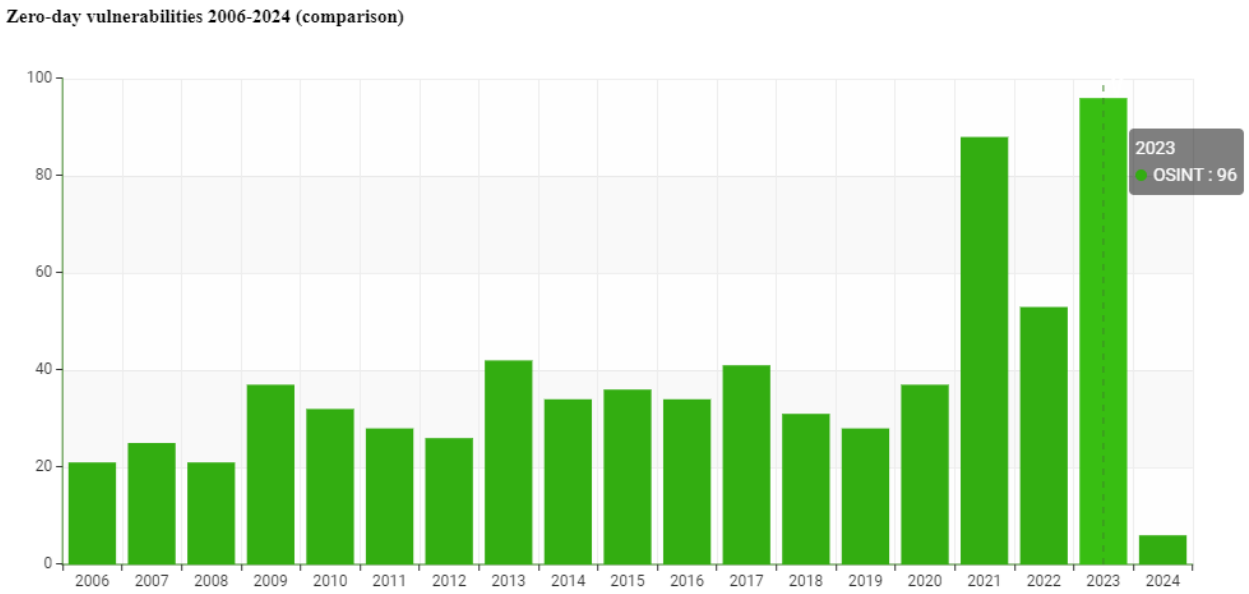
Les autres attaques de 2023

Le tableau ci-après détaille les 20 alertes émises par le Cert-IST en 2023. En plus des attaques déjà mentionnées ci-dessus, les attaques les plus marquantes ont été celles sur les produits **Fortinet**, **Outlook**, **Ivanti EPMM**, **Atlassian Confluence** et **Cisco IOS XE**.

Alerte	Référence	Description	Date
Jaune	CERT-IST/AL-2023.001	Attaques en cours via la vulnérabilité dans **SugarCRM** (CVE-2023-22952)	12-janv-23
Jaune	CERT-IST/AL-2023.002	Attaques en cours visant **Cacti** (CVE-2022-46169)	17-janv-23
Orange	CERT-IST/AL-2023.003	Attaques en cours visant des produits **ManageEngine** (CVE-2022-47966)	20-janv-23
Orange	CERT-IST/AL-2023.004	Attaques en cours visant **VMware ESXi** (ransomware ESXiArgs)	06-févr-23
Jaune	CERT-IST/AL-2023.005	Risque d'attaques visant **Fortinet FortiNAC** (CVE-2022-39952)	22-févr-23
Jaune	CERT-IST/AL-2023.006	Attaques détectées pour **Barracuda** Email Security Gateway (CVE-2023-2868)	31-mai-23
Jaune	CERT-IST/AL-2023.007	Attaques en cours visant les équipements fonctionnant sur **FortiOS** (CVE-2023-27997)	13-juin-23
Jaune	CERT-IST/AL-2023.008	Attaques en cours via une vulnérabilité visant **Microsoft Office / Outlook** (CVE-2023-36884)	13-juil-23
Orange	CERT-IST/AL-2023.009	Attaques en cours visant **Netscaler** Application Delivery Controller (ADC) et Netscaler Gateway (CVE-2023-3519)	19-juil-23
Jaune	CERT-IST/AL-2023.010	Attaques en cours visant **Ivanti Endpoint Manager Mobile** (EPMM) (CVE-2023-35078, CVE-2023-35081)	25-juil-23
Orange	CERT-IST/AL-2023.011	Attaques en cours visant **Ivanti Sentry** (CVE-2023-38035)	25-août-23
Orange	CERT-IST/AL-2023.012	Attaques en cours visant **Juniper Junos** (CVE-2023-36844 à CVE-2023-36847)	28-août-23
Jaune	CERT-IST/AL-2023.013	Attaques en cours visant **Apple iOS** (CVE-2023-41061, CVE-2023-41064)	8-sep-23
Jaune	CERT-IST/AL-2023.014	Risque d'attaques visant **Microsoft SharePoint** (CVE-2023–29357 & CVE-2023–24955)	29-sep-23
Jaune	CERT-IST/AL-2023.015	Attaques en cours visant les serveurs **Confluence** (CVE-2023-22515)	12-oct-23
Orange	CERT-IST/AL-2023.016	Attaques en cours visant **Cisco IOS XE** (CVE-2023-20198 & CVE-2023-20273)	17-oct-23
Orange	CERT-IST/AL-2023.017	Attaques en cours visant **Netscaler** Application Delivery Controller (ADC) et Netscaler Gateway (CVE-2023-4966)	24-oct-23
Jaune	CERT-IST/AL-2023.018	Attaques en cours visant **F5 BIG-IP** (CVE-2023-46747 et CVE-2023-46748)	6-nov-23
Jaune	CERT-IST/AL-2023.019	Attaques en cours visant **Apache ActiveMQ** (CVE-2023-46604)	7-nov-23
Jaune	CERT-IST/AL-2023.020	Risque d'attaques contre **Apache Struts 2** (CVE-2023-50164)	14-déc-23

2.1.2 *Augmentation des 0-day*

Selon le site zero-day.cz, 96 vulnérabilités 0-day ont été découvertes en 2023, ce qui dépasse le record précédent de 2021 (88 vulnérabilités 0-day en 2021).



Nombre de 0-day identifiées par le site www.zero-day.cz (société Cybersecurity-Help)

Plus globalement on voit sur cette courbe un changement net de tendance en 2021 : alors que jusque -là le nombre de 0-day était de l'ordre de 40 par an, il est passé ensuite plutôt autour de 80 par an.

Nous pensons que cette augmentation est due à 3 phénomènes :

- Augmentation des **0-days du type Pegasus** visant les iPhone et Android : de l'ordre de 20 0-days iOS/iPhone ont été découvertes en 2023.
- Les **attaques étatiques chinoises** : selon Recorded Future, depuis 2021, la Chine utilise de l'ordre de 10 vulnérabilités 0-days par an dans des campagnes d'attaques massives.
- L'utilisation de **0-days par les cybercriminels**.

Les 2 dernières catégories sont des cas où une vulnérabilité 0-day est utilisée pour attaquer un grand nombre de cibles (campagne d'attaques) alors que jusqu'à présent les 0-days étaient plutôt réservées à des cibles de grandes valeurs (attaques visant un nombre réduit de cibles). Cela signifie que pour une organisation normale (non qualifiée "de grande valeur"), le risque de subir une attaque 0-day augmente.

Faut-il s'inquiéter de cette augmentation ?

Oui et Non, car le risque 0-day existe depuis toujours. Mais outre la pression que cela peut créer sur les équipes d'exploitation (les 0-day déclenchant souvent le déploiement urgent de correctifs), l'augmentation des 0-day met en évidence que l'élément le plus important n'est pas simplement de "d'empêcher les 0-day", mais plutôt de savoir maîtriser la situation une fois que l'on a été touché par une 0-day. Cela nécessite 2 compétences :

- Détection : Savoir détecter que l'on a été infecté, et cela n'est pas facile lorsque l'attaquant sait se dissimuler.
- Remise en état : Savoir désinfecter l'équipement touché ou le remplacer si ce n'est pas possible.

2.1.3 Attaques sur les équipements de bordure

Depuis l'été 2019, les attaques visant les équipements de bordure (typiquement les accès VPN et les Appliances exposées sur Internet) sont en augmentation. Cette tendance se poursuit en 2023 et 8 de nos 20 alertes concernent des produits de ce type : **Fortinet** (2 fois), **Barracuda**, **Citrix Netscaler** (2 fois), **Juniper**, **Cisco IOS XE** et **F5 BIG-IP**.

Nous avions relevé cette tendance dans notre bilan 2020 et qualifié certains de ces équipements de "durs dehors, mais mous dedans"). Au-delà de la fragilité, l'année 2023 montre 3 nouveaux aspects importants pour ces attaques :

- Les compromissions profondes,
- La difficulté à surveiller les équipements,
- La difficulté à les désinfecter.

Les compromissions profondes et difficulté à surveiller les équipements

Article publiée en Une dans le bulletin mensuel Cert-IST de mars 2023

Plusieurs exemples récents montrent que certains attaquants sont capables, après avoir exploité une vulnérabilité, de modifier profondément les équipements qu'ils ont compromis, de façon à rester longtemps sur ces équipements et ne pas être détectés. Mandiant décrit cela sur un firewall SonicWall SMA et Fortinet sur un firewall FortiGate. On y voit :

- des techniques pour survivre à une montée de version,
- le remplacement de librairies systèmes,
- l'installation de filtres réseaux déclenchant une backdoor à l'arrivée d'un paquet ICMP particulier,
- l'effacement des logs,
- etc.

Il s'agit dans les 2 cas d'appliances basées sur des systèmes comme Linux ou FreeBSD, ce qui offre de grandes possibilités d'adaptation. Et visiblement les attaquants connaissent très bien le fonctionnement de ces plates-formes. Mandiant fait aussi remarquer que ces appliances sont difficiles à surveiller (pas d'EDR, pas de détection d'anomalies de fonctionnement, pas d'antivirus) et que l'OS sous-jacent est masqué ce qui peut rendre difficile la détection d'un processus anormal ou même la collecte des logs.

Ces constats sont inquiétants. Il faut peut-être améliorer les appliances. Mais il faut aussi activer les mécanismes de surveillance qui existent (Fortinet dit que c'est le contrôle d'intégrité du mode FIPS qui a permis de découvrir la compromission), et surveiller les anomalies qui sont détectées. Bien sûr, il faut aussi appliquer scrupuleusement les correctifs de sécurité et ré-installer complètement l'équipement si une attaque a réussi.

La difficulté à les désinfecter

Dans le cas d'attaquants aguerris, il peut être difficile d'identifier toutes les modifications qui ont été faites et de remettre le système dans un état sain. Il est courant désormais que ces attaquants mettent en place des mécanismes pour résister aux montées de versions. De façon plus rare, il y a aussi quelques témoignages de cas où l'attaquant a altéré des logiciels de bas niveau (par exemple attaques UEFI ou infection de firmwares de cartes réseaux). Il existe de nombreuses autres possibilités, par exemple des attaques via le BMC des cartes mères, mais pas de témoignage d'attaques réelles pour ces cas. Depuis 2021, la CISA américaine désigne ces attaque sous le terme de VBOS (Vulnerability Below the OS) et attire l'attention sur le besoin de se protéger.

Les VBOS sont à notre connaissance des cas exceptionnels, réservés à acteurs étatiques avancés. Par contre, l'exemple vu en 2023 avec Barracuda ESG (cf. § 2.1.1) montre que la situation « on ne sait pas réparer » pourrait devenir courante.

Nota : Il n'y a pas d'élément pouvant faire penser que dans le cas Barracuda il y a eu une attaque VBOS.

Remplacer plutôt que réparer ?

La recommandation de Barracuda a beaucoup étonné, mais s'est sans doute la seule approche permettant d'être sûr de repartir sur des bases saines, et on peut se demander, en faisant abstraction des éléments financiers, s'il ne faudrait pas l'utiliser plus souvent.

Remplacer un équipement de bordure est une opération délicate :

- Sa disponibilité est généralement critique,
- Sa configuration (en termes de paramétrages) doit être parfaitement maitrisée pour pouvoir être reproduite sur l'équipement de remplacement sans avoir à recopier ce qui est sur l'équipement infecté (danger de réinfection).

Cependant tout cela est possible sans difficulté majeure si cela a été préparé (en disposant d'une copie saine de la configuration de l'équipement) et évalué.

Par analogie avec la recommandation « Faire des sauvegardes » que l'on donne souvent pour lutter contre les attaques de ransomwares, nous pensons qu'il faut aussi recommander de « Faire des procédures de remplacement pour les équipements » pour lutter contre les attaques sur les équipements de bordure.

2.1.4 Attaques par les cybercriminels

2.1.4.1 Ransomware et BEC restent la menace principale

Indépendamment des nouvelles tendances que nous décrivons dans la suite, il est important de rappeler que pour les entreprises la majorité des attaques cybercriminelles restent :

- Les ransomwares : réservés à l'origine pour désigner les attaques qui bloquent en masse les ordinateurs d'une entreprise, le terme englobe aussi désormais le chantage à la diffusion de données volées.
- Les attaques BEC (Business Email Compromise) : le terme est souvent utilisé au sens large pour désigner toutes les tentatives d'escroqueries financières réalisées par email. Par exemple : faux ordre de virement, fausse commande au nom d'une entreprise de tiers, etc.

2.1.4.2 Campagnes d'attaques du type MOVEit

L'attaque MOVEit Transfer (cf. § 2.1.1) montre que les cybercriminels cherchent sans cesse de nouveaux moyens pour attaquer les entreprises, et donc de nouveaux moyens de voler des documents ou de créer des perturbations dans l'entreprise.

Ils se sont intéressés en 2023 :

- Aux logiciels de la catégorie des MFT (Managed File Transfer) à laquelle MOVEit appartient. Nous avons déjà cité dans cette catégorie (au § 2.2.1) **Accellion FTA**, **Aspera Faspex**, et **GoAnywhere MFT**. On peut y ajouter aussi les attaques vues contre les logiciels suivants : **HCP Anywhere** d'Hitachi Vantara (incident AP-HP en septembre 2021), **Serv-U** de SolarWinds (en octobre 2021), **Citrix ShareFile** (août 2023).
- A la solution d'impression d'entreprise **PaperCut** (attaque en avril 2023). A ce jour, c'est le seul logiciel de cette catégorie à avoir été attaqué.

Quel sera le prochain type d'attaque ?

Difficile de le savoir… Nous avons cependant observé une nouvelle tactique qui pourrait probablement se généraliser dans le futur : **l'intrusion dans les espaces de support réservés aux clients**.

En octobre 2023, Okta a subi une intrusion dans son espace « Support clients » : l'attaquant a volé les fichiers HAR que les clients avaient transmis au support technique d'Okta. Ces fichiers de debug contiennent des jetons de session que l'attaquant a pu réutiliser pour se connecter chez les clients concernés.

En extrapolant cet incident, on peut penser que les espaces « Support clients » sont une cible intéressante pour les attaquants : ils contiennent des données clients qui pourraient faire l'objet de chantage. Pour limiter les conséquences d'une attaque de ce type, il est important de limiter la durée de conservation des données stockées dans ces espaces.

2.1.4.3 Attaques avancées en ingénieries sociale

Article publié en Une dans le bulletin mensuel Cert-IST de novembre 2023

La CISA a publié en novembre un bulletin d'alerte à propos du groupe **Scatter Spider**. Début septembre, ce groupe était suspecté avoir attaqué deux casinos et hôtels de Las Vegas : le MGM Resorts puis le Ceasar Palace. Il fait partie des quelques groupes connus pratiquant des attaques très avancées en ingénierie sociale.

Ce groupe est par exemple capable de :

- Rechercher sur LinkedIn un ingénieur système travaillant pour une entreprise visée,
- Puis collecter sur Internet des informations personnelles (date de naissance, etc.) sur cette personne,
- Voler les comptes et mots de passe, via des attaques de phishing par mail ou SMS,
- Appeler le support technique de l'entreprise (le Help Desk) en se faisant passer pour un employé et obtenir la réinitialisation de ses jetons d'authentification Okta.

En plus de sa très bonne connaissance technique des méthodes d'authentifications, le groupe se caractérise par son habileté à manipuler ses victimes. Outre son audace (il peut par exemple démarrer une conversation WhatsApp avec sa victime pour le convaincre de réaliser une action), il peut même la menacer de représailles physiques, comme indiqué dans ce rapport de Microsoft. Début 2022, on observait des compétences similaires avec le groupe **Lapsus$** avec notamment l'attaque de type « MFA fatigue » contre Uber, puis avec l'attaque contre Twilio/Okta.

Ces attaques avancées en ingénierie sociale deviennent de plus en plus fréquentes, critiques et réussies. D'ailleurs, Okta a publié deux articles durant l'été sur le sujet (en juillet et en août), car ces attaquants ont réussi plusieurs fois à convaincre des équipes Help Desk d'entreprises victimes de leur donner accès à des comptes d'administrateurs Okta.

Nota : Scatter Spider est connus sous de multiples noms (cf. notre fiche attaque **CERT-IST/ATK-2023.010**) : **Octo Tempest** pour Microsoft, **0ktapus** pour Group-IB, **Scatter Swine** pour Okta, **Muddled Libra** pour Palo Alto Networks, **UNC3944** pour Mandiant. Mais il n'est pas complètement certain que tous ces noms désignent exactement le même groupe. Certains analystes en CTI disent avoir du mal à cerner le contour de certains groupes, qu'ils qualifient de fluides (cf. cette présentation de la conférence SLEUTHCON 2023).

2.1.4.4 La chasse aux données d'accès (mot de passe, Okta, etc.)

Depuis longtemps les pirates cherchent à voler les données d'authentification (mots de passe, jetons de session, etc.) qui leurs permettent de prendre le contrôle de comptes d'utilisateurs. Cette catégorie d'attaques est généralement appelée **ATO** : Account Take Over.

Certaines méthodes sont connues depuis très longtemps :

- Deviner les mots de passe : **brute-force**, **Password Spraying**, etc.
- Ou les demander à l'utilisateur : **phishing**

Plus récemment, sont apparues les méthodes suivantes :

- Voler le mot de passe à l'utilisateur : **Infostealer**
- Contourner les MFA : **SIM-swap**, **MFA-fatigue**, **Pass-the-cookie**

En 2023, deux nouvelles tendances prennent de l'importance :

- Le vol chez les fournisseurs de solutions d'authentification, comme chez **Okta** (octobre 2023) et sur le coffre à mots de passe **1Password**. En 2022, **LastPass** (autre coffre à mots de passe) avait subi une attaque majeure. On a aussi plusieurs fois discuté en 2023 de vulnérabilités **KeePass**. Aucun de ces sujets n'est complétement nouveau, mais 2023 montre que ce type d'attaques est très présent et se diversifie. Voler des mots de passe est l'activité principale de certains cybercriminels et ils cherchent à les récupérer partout où ils sont stockés.
- Les appels au Help Desk de l'entreprise pour prendre le contrôle d'un compte. On retrouve ici les attaques avancées en ingénierie sociale que nous évoquons dans le point précédent.

2.1.5 Quid des attaques étatiques ?

Les attaques étatiques représentent une part importante de la menace. C'est même les attaquants les plus dangereux. Les états peuvent employer des techniques d'attaques non encore connues ou hors de portée des autres attaquants. Et les techniques qu'ils utilisent sont ensuite parfois reprises par les cybercriminels.

Pour l'année 2023, les acteurs étatiques ont été très présents. On a vu des attaques chinoises, russes, iraniennes et même américaines (avec la découverte en Russie de l'attaque iPhone nommée « **Operation Triangulation** »).

Nous n'avons cependant pas noté d'événement en 2023 qui pourrait concerner les entreprises et que nous n'avons pas déjà été couverts dans d'autres parties de notre bilan.

Nota : Certains points du paragraphe 2.2 complète cette analyse en abordant des attaques domaine des attaques étatiques.

2.1.6 Autres tendances remarquables

Voici des faits techniques marquants que nous avons vus en 2023.

2.1.6.1 Attaques DDOS du type NoName057 ou Anonymous Sudan

Apparues en mars 2022, au début de guerre RU-UA, les attaques en déni de service du groupe hacktiviste pro-russe **NoName057** (et de quelques autres groupes similaires comme **Killnet**) se sont poursuivies en 2023. Le groupe **Anonymous Sudan** (initialement non directement lié à la guerre RU-UA mais proche de groupes pro-russes) s'est particulièrement fait remarquer (par exemple avec une série d'attaques visant la France fin février 2023) et a même réussi à bloquer certains services Azure et Outlook du Cloud Microsoft en juin.

A notre connaissance, ces attaques DDOS n'ont pas eu de conséquences graves. Elles ont cependant causé des indisponibilités de plusieurs heures sur les sites visés et induit un surcroit de travail important pour les équipes d'exploitation mobilisées pour y répondre.

2.1.6.2 Utilisation des outils de RMM

En 2023, la CISA américaine a publié plusieurs fois des mises en garde (voir cette annonce en janvier et cette autre en juin) indiquant que des outils légitimes de la catégorie des RMM (**Remote Monitoring and Management**) sont souvent utilisés par les attaquants pour contrôler à distance les ordinateurs compromis. Par exemple des logiciels commerciaux de prise de main à distance comme **ScreenConnect** (désormais appelé **ConnectWise Control**) ou **AnyDesk** ont souvent été utilisés dans des escroqueries visant le grand public (par exemple les « Faux supports techniques ») ou même les entreprises. **TeamViewer** est aussi régulièrement utilisés.

La CISA recommande donc aux entreprises de surveiller si ce type d'outils apparait sur le réseau interne et a lancé une initiative avec les fabricants et les MSSP pour protéger les outils RMM contre un usage cybercriminel.

2.1.6.3 Attaques visant VMware ESXi

Les solutions de virtualisation proposées par VMware sont des composants très répandus dans les entreprises et sont donc des cibles attractives pour les attaquants :

- Les ransomwares ciblent beaucoup VMware (chiffrer un hyperviseur ESXi permet de chiffrer d'un coup toutes les VM gérées par ce dernier). Recorded Future annonçait début 2023 que ce type d'attaque avait triplé en 2022. VMWare a d'ailleurs une page dédiée à la défense contre les ransomwares.
- Les attaquants (étatiques ou les cybercriminels) connaissent très bien les chemins d'attaques classiques dans l'environnement vSphere : Attaquer le vCenter, puis prendre le contrôle des serveurs ESXi et finalement des VM (voir par exemple cette présentation de la conférence Typhooncon 2023 ou cette attaque chinoise au moyen de la CVE-2023-20867).
- En février 2023, une vulnérabilité dans le service SLP a permis de compromettre des milliers de serveurs ESXi avec un ransomware spécifique nommé **ESXiArgs**. Beaucoup étaient des serveurs installés sans sécurisation sur des systèmes "bare metal" (machines nues sur lesquelles le client doit installer un OS) hébergés chez OVH.

2.1.6.4 Phishing OneNote et Teams

Plus anecdotique, en 2023 nous avons noté 2 nouvelles techniques de phishing qui ont été utilisées :

- Le phishing OneNote : début 2023, des attaques par emails ont utilisé des attachements malveillants « .one » (fichiers Microsoft OneNote) pour tenter d'infecter les utilisateurs.
- Le phishing via Teams : en septembre 2023, plusieurs attaques ont été signalées. Le principe est d'envoyer à la victime un message de tchat Teams avec une pièce jointe piégée. L'attaque exploite une vulnérabilité révélée en juin, pour laquelle un outil nommé TeamPhisher avait été publié un mois plus tard.

2.2 Autres faits marquants concernant moins les entreprises

2.2.1 Crypto-monnaies : cible favorite pour de nombreux attaquants

Nous avions déjà mentionné dans notre bilan pour l'année 2021, que le vol de crypto-monnaies constitue une motivation forte pour les cybercriminels et pour des états comme la Corée du Nord et l'Iran. En 2023, on a vu par exemple que l'attaque 3CX (cf. § 2.1.1) avait pour origine des attaques de la Corée du Nord visant le monde financier. Et on sait que les attaques de SIM Swapping ont débuté en 2016 avec des attaques visant les crypto-monnaies.

Tout comme les Bankers des années 2015 (malware qui vole de l'argent sur les comptes en banques des victimes), il y a aujourd'hui de nombreuses attaques visant à siphonner l'argent des portefeuilles de crypto-monnaies. Selon la société Intel 471, le type de malware le plus vendu sur le marché underground au premier semestre 2023 était le **Crypto-drainer** (logiciel pour siphonner la crypto-monnaie).

Cette menace concerne surtout les particuliers et des entreprises qui détiennent des crypto-monnaies ou qui travaillent dans le domaine de la finance décentralisée (DeFi).

2.2.2 Cyberguerre : l'importance croissante de l'arme cyber pour les états

La guerre RU-UA a montré que les cyber-attaques étaient une arme à part entière complétant les armements conventionnels, et qu'elles étaient particulièrement efficaces pour la collecte de renseignement, la déstabilisation ou pour des opérations d'influence.

Ce constat fait augmenter pour les états le besoin de disposer d'outils cyber défensifs aussi bien qu'offensifs. Et il s'en suit une montée du cyber-armement :

- Après le « Hunt-forward » (la défense préventive) que nous avions mis en avant dans notre bilan 2022, on parle de plus en plus en 2023 de « Cyber Défense Active » (**Active Cyber Defense**).
- L'attaque **Volt Typhoon** de la Chine contre les Etats-Unis a été interprétée par plusieurs analystes comme une opération de pré-positionnement visant à placer des backdoors dans des installations de l'ile de Guam (dans le Pacifique), pour pouvoir éventuellement perturber les communications Internet sur la zone Pacifique en cas de conflit.
- Les analyses sur ce qu'est une cyberguerre et son impact sur les civils sont désormais présentés lors de conférences (voir par exemple ces 2 présentations lors de la conférence Hack.lu 2023 : Introduction to cyberwarfare et 8 rules for civilian hackers)

2.2.3 L'omniprésence de la Chine sur le domaine cyber-offensif se poursuit

Depuis 2021, la Chine a été pointée comme étant à l'origine de nombreuses attaques cyber. Pour l'année 2023, les événements les plus marquants sont :

- L'attaque Barracuda ESG (cf. § 2.1.1)
- L'attaque Volt Typhoon
- Le vol de clés cryptographiques chez Microsoft par le groupe **Storm-0558** (voir cet article TheRecord.media de juillet 2023 et le complément fourni par Microsoft en septembre).

En 2023, Mandiant et RecordedFuture ont également attribué à la Chine des attaques **Fortinet et VMware** (CVE-2022-41328 et CVE-2023-20867), **Citrix NetScaler** CVE-2023-3519 (juillet 2023) et **Atlassian Confluence** CVE-2023-22515 (octobre 2023).

2.2.4 Pegasus et Predator : les usages abusifs des outils de surveillance continuent

En juillet 2021, un groupe de journalistes avait révélé les usages abusifs de l'outil de cyber-surveillance Pegasus. Malgré les initiatives lancées à cette époque (procès contre NSO, commission PEGA au parlement Européen, etc.) de nouveaux usages abusifs ont été découverts en 2023 :

- De nouvelles attaques 0-click Pegasus ont été découvertes pour iOS : **PWNYOURHOME** (avril 2023) et **BLASTPASS** (septembre)
- Une enquête journalistique nommée « Predator files » a été publiée en octobre 2023 à propos du malware **Predator** (un équivalent de Pegasus) attribué au consortium **Intellexa**.

3 Productions du Cert-IST en 2023

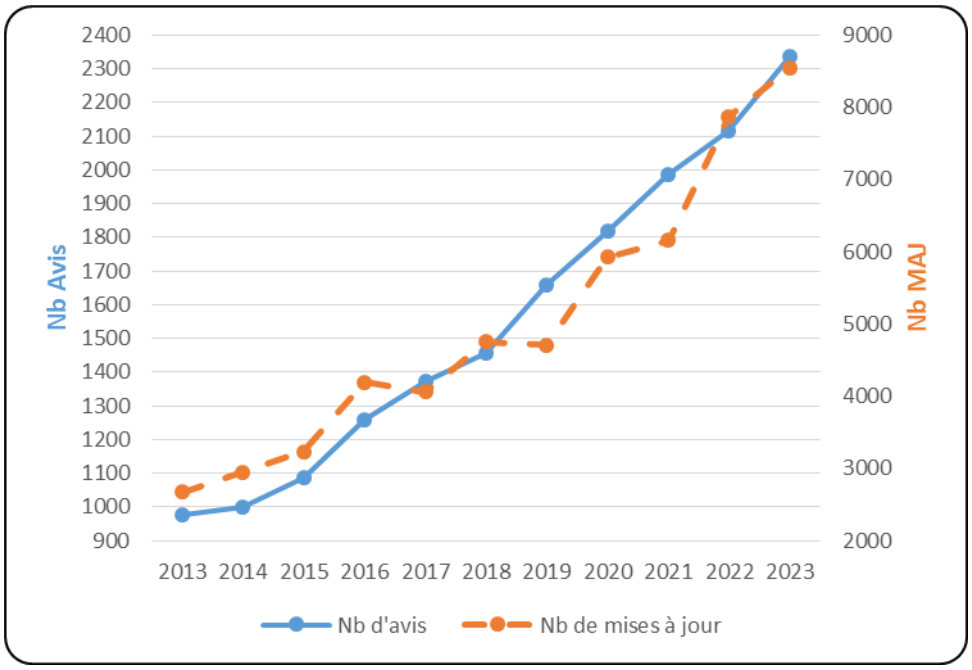
3.1 Veille sur les vulnérabilités et les menaces

Dans le cadre de son activité de veille sur les vulnérabilités et les menaces, le Cert-IST suit de façon continue différentes sources d'informations (annonces constructeurs, blogs sécurité, mailing-lists, échanges au sein des communautés cyber, etc.) afin d'être informé des nouvelles vulnérabilités. Ces informations sont analysées quotidiennement pour fournir à nos adhérents des informations triées, qualifiées et priorisées.

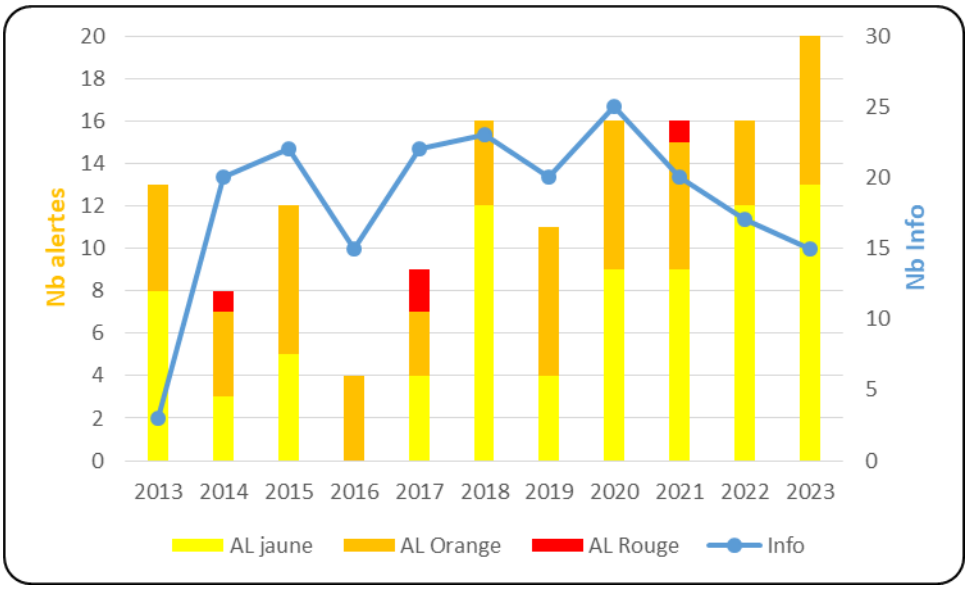
Le Cert-IST émet ainsi plusieurs types de publications :

- **Les Avis de sécurité (AV)** : ils décrivent les nouvelles vulnérabilités découvertes dans les produits suivis par le Cert-IST. Ces avis sont enrichis de façon continue avec des mises à jour mineures ou majeures. Ces dernières correspondent par exemple au cas où des programmes d'attaques – des "exploits" – sont publiés.
- **Les Alertes (AL)**, qui sont émises lorsqu'il y a un risque spécifique d'attaques et les **messages INFO** lorsqu'une menace existe (et qu'elle est médiatisée) mais d'une dangerosité immédiate plus faible. Ces 2 catégories sont axées sur les risques d'attaques alors que les avis de sécurité répertorient eux, de façon systématique, toutes les vulnérabilités (quelle que soit leur probabilité d'être utilisées dans des attaques).
- **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.

Les graphiques ci-dessous montrent la production du Cert-IST au cours des dernières années.



Nombre d'avis de sécurité (et de mises à jour) publiés par an



Nombre d'alertes publiées par an

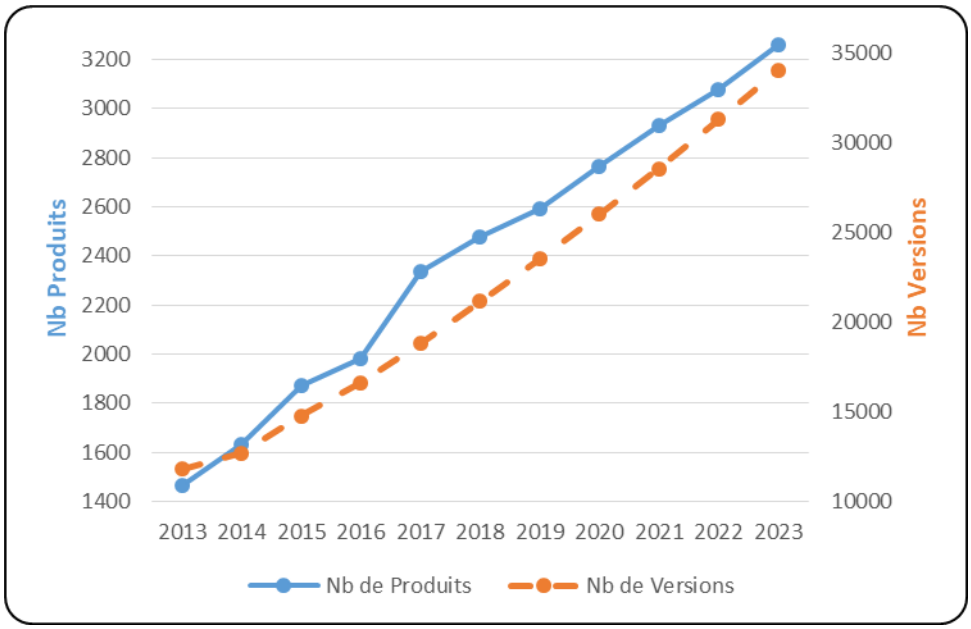
Ainsi, en 2023, le Cert-IST a publié :

- **2 338** avis de sécurité (dont **136** avis SCADA), **8 544** mises à jour mineures et **166** mises à jour majeures.
  Le nombre d'avis est en augmentation constante depuis de très nombreuses années (cf. la courbe de la page précédente), avec en 2023 une augmentation de **10%** par rapport à 2022. Cette augmentation continue montre que la découverte de vulnérabilités est un phénomène en constante croissance. Le maintien du niveau de sécurité passe donc encore et toujours par une application régulière des correctifs de sécurité sur les produits présents dans le système d'information.

- **20** alertes et **15** messages Info. Il n'y a pas eu d'alerte rouge cette année. Les précédentes alertes rouges ont été émises en 2021 (Exchange) et 2017 (WannaCry et NotPetya). Ces dernières années le nombre d'alerte était plutôt stable, mais il a augmenté en 2023 (passage de 16 à 20 alertes dans l'année).

- **138** fiches attaques ont été publiées en 2023, avec dans la base de données MISP **7 181** évènements enrichis par l'équipe Cert-IST, et près de **400 000** marqueurs (IOC) ajoutés. Au total il y a **7,5 millions** de marqueurs dans la base MISP Cert-IST.

Concernant les produits et les versions suivis par le Cert-IST, fin 2023 le Cert-IST suivait **3 258** produits et **34 004** versions de produits. Le graphique suivant montre l'évolution du nombre des produits et des versions qui sont suivis par le Cert-IST.



Nombre de produits et de versions de produits suivis par le Cert-IST

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

Remplacer plutôt que réparer ?

Parmi l'ensemble des phénomènes observés en 2023, l'évolution la plus importante pour les entreprises est, selon nous, le fait que de plus en plus d'attaques altèrent en profondeur les équipements de bordure. L'attaquant ne se contente pas de prendre le contrôle de l'équipement : il s'y installe pour y rester le plus longtemps possible. Cela a été vu en particulier avec l'attaque Barracuda ESG, ou début 2024 avec l'attaque visant Ivanti Connect Secure. Dans ce cas, plutôt que de simplement désinfecter et appliquer des correctifs, il devient nécessaire de reconstruire le système. Cette approche est déjà pratiquée depuis longtemps sur les postes de travail (remplacement ou re-masterisation) mais sera sans doute désormais nécessaire aussi sur des équipements d'infrastructure et en particulier les équipements exposés sur Internet.

Les menaces cybercriminelles les plus présentes restent le Ransomware et les escroqueries BEC

On pourra cependant noter pour 2023 :

- une augmentation des attaques par ingénierie sociale (par exemple se faire passer pour un employé auprès du Helpdesk de l'entreprise et demander la remise à zéro du MFA),
- et la chasse constante pour voler les données d'accès (poursuite des attaques Infostealer vues en 2022 et augmentation des attaques visant OKTA ou les coffres à mots de passe).

Les axes d'amélioration à poursuivre

Trop de systèmes exposés sur Internet. A chaque nouvelle vulnérabilité critique, on observe des attaques de systèmes mal sécurisés exposés sur Internet. Et nous nous demandons souvent si ces systèmes ont réellement besoin d'être visibles de tous sur Internet. Ce sujet n'est pas nouveau mais semble s'accentuer avec l'adoption généralisée du Cloud et son modèle d'accès depuis n'importe où. Nous n'avons pas de solution à ce problème mais voici quelques propositions d'amélioration :

- Considérer un système exposé sur Internet comme critique. Il faut par exemple être capable de le mettre à jour de façon très rapide en cas de faille critique et mettre en place les processus adéquats pour cela.
- Ne pas exposer directement les fonctions d'administration. Celles-ci ne devraient être accessibles que depuis des points d'accès précis (par exemple des bastions, des jump-hosts, etc…).
- Mettre en place un mécanisme de contrôle d'accès en amont (IAM), distinct de l'application elle-même. Le contrôle d'accès est une fonction critique et il est donc préférable de la gérer avec une solution dédiée (comme les Application Gateway, les reverse-proxy d'authentification, etc.).

La grande complexité des environnements Cloud (Azure, AWS et GCP). Ces offres Cloud sont complexes techniquement et très dynamiques ce qui les rend difficiles à maîtriser. Il n'y a probablement pas de solution, hormis de faire le constat que la robustesse de ces offres dépend du fournisseur et en particulier de ses engagements contractuels vis-à-vis des risques cyber (qui est responsable de quoi ?), de sa transparence en cas d'événements cyber et de sa capacité à réagir lorsqu'une nouvelle technique d'attaque est découverte.

Il faut noter par ailleurs que s'appuyer sur des solutions Cloud (plutôt que d'implémenter soit même toute la pile technologique, du matériel jusqu'à l'applicatif) renforce plutôt le niveau de sécurité parce que le fournisseur Cloud prend en charge le maintien du niveau de sécurité de la solution qu'il propose. En définissant des domaines de responsabilité et des engagements de service, on permet à chacun des acteurs de se concentrer sur son métier.

Une actualité toujours très riche en événements

Comme chaque année, 2023 a été riche en événements dans le domaine des vulnérabilités et des attaques. Se tenir au courant quotidiennement, et identifier les tendances sont des activités primordiales pour maitriser sa défense. Le Cert-IST est dans ce domaine un partenaire privilégié des entreprises.

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