CERT-IST

INDUSTRIE | SERVICES | TERTIAIRE

Bilan Cert-IST des failles et attaques de 2022

Publié en Février 2023

Table des matières

1 Introduction 3
2 Cela s'est passé en 2022 3
3 Analyse des phénomènes les plus marquants de 2022 7
3.1 Les principales vulnérabilités 7
3.2 Les malwares Infostealer dominent l'actualité 2022 9
3.3 Une année de stabilisation pour les ransomwares ? 11
3.4 La guerre RU-UA redéfinit le rôle du cyber dans un conflit 13
3.5 La menace SCADA augmente avec le malware PIPEDREAM 14
3.6 Les attaques de la Supply-Chain visent aussi les activités externalisées 16
3.7 La montée des Hackers-for-hire et des produits offensifs pour les états 17
3.8 Les autres phénomènes observés 19
4 Productions du Cert-IST en 2022 24
4.1 Veille sur les vulnérabilités et les menaces 24
4.2 Veille technologique 26
5 Conclusions 27

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 présentons dans un premier temps une rétrospective de l'actualité de 2022 (cf. chapitre 2), puis nous analysons les éléments les plus significatifs (cf. chapitre 3). Nous fournissons ensuite un récapitulatif des différentes productions du Cert-IST au cours de cette année (cf. chapitre 4).

La conclusion (cf. chapitre 5) donne une synthèse du paysage actuel de la cybermenace et des challenges auxquels les entreprises doivent faire face en 2023.

➢ **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 Cela s'est passé en 2022

Le tableau ci-dessous récapitule des événements marquants de 2022, qui se sont distingués soit parce qu'ils ont été fortement médiatisés, soit parce que ce sont des marqueurs de la progression de la menace cyber.

Janvier 2022	Le FSB russe arrête les membres du groupe **REvil.** Le FSB aurait agi suite aux demandes pressantes des Etats-Unis ; il s'agit probablement d'une manœuvre politique visant à monter la bonne volonté de la Russie. Cela marque l'arrêt de ce groupe de ransomware qui avait marqué 2021 avec les attaques ColonialPipe et Kaseya. Il avait déjà été partiellement neutralisé en octobre 2012.
	LAPSUS$, un groupe cybercriminel probablement composé de jeunes de 14 à 18 ans réussit à pirater une série de sociétés majeures, dont NVIDIA, Microsoft, Samsung, T-Mobile et Uber. Les attaques ne sont pas forcément très évoluées, mais les attaquants ont beaucoup d'audace et n'hésitent pas à appeler leurs victimes au téléphone pour les convaincre de se connecter à de faux sites.
Février 2022	325 millions de dollars sont détournés dans une attaque de la **plate-forme de crypto-monnaie Wormhole**. C'est un des plus gros incidents de l'année. Mais le record 2022 est l'incident **Ronin** en mars (625 millions) qui est attribué au groupe Nord-Coréen Lazarus. Et lors de la **banqueroute de FTX** (en novembre 2022) 477 millions de dollars ont aussi disparu. **Globalement en 2022 plus de 2 milliard de dollars ont été détournés sur le marché de la crypto-monnaie**.

	24/02/2022 : Entrée en guerre de la Russie contre l'Ukraine.
	Fuite de données chez **CONTI** : Suite à l'entrée en guerre de la Russie, et à une dispute entre les membres Russes et Ukrainiens du groupe, un grand nombre de données internes sont rendues publiques. Elles montrent que CONTI fonctionne comme une entreprise : une centaine d'employés, un service RH, etc. Cette fuite de données est détaillée au §3.3.2.
	Microsoft annonce qu'il bloque les macros pour les documents Office chargés depuis Internet (il n'y aura plus de bouton pour les débloquer dans le message de sécurité signalant ces macros). Mais début juillet Microsoft fait marche arrière … pour finalement réactiver le blocage fin juillet. Par la suite, les discussions se tournent vers « Comment contourner le **MOTW** (Mark of the Web) ? » que Microsoft utilise pour déterminer qu'un document vient d'Internet, ou sur d'autres méthodes de contournement (cf. Follina ci-dessous, en mai).
Mars 2022	**Spring4Shell** : Après Log4Shell (vulnérabilité dans la librairie Log4J), voilà une nouvelle vulnérabilité dans une librairie Java. Elle touche cette fois le Framework Spring.io. Moins d'attaques que Log4Shell seront observées (probablement parce que la librairie est moins utilisée) mais le botnet Mirai semble l'avoir utilisée en avril. En octobre, une 3eme vulnérabilité Java sera médiatisée : **Text4Shell** qui concerne cette fois la librairie Apache Commons Text. A notre connaissance, il n'y a pas eu d'attaques réussies avec cette vulnérabilité, car la vulnérabilité n'existerait que dans des configurations très spécifiques.
	OKTA annonce qu'il a été lui-aussi victime du groupe LAPSUS$. L'attaque a eu lieu en janvier, chez un sous-traitant chargé d'assurer le support technique pour les clients OKTA. Cela met en évidence les attaques visant les activités externalisées (cf. § 3.6).
	La CISA indique observer des **attaques visant des équipements de courant secouru UPS** (Uninterruptible Power Supply) connectés à Internet, qui utilisent les mots de passe par défaut. Cette alerte arrive quelques semaines après la publication d'une étude de la société Armis nommée **TLStorm** qui a révélé des vulnérabilités TLS/SSL dans des UPS de la marque APC. Hormis le type d'équipements visés, il n'y a cependant pas de rapport entre les 2 annonces.
Avril 2022	**PIPEDREAM** : C'est le nom donné par la société Dragos (Mandiant l'a de son côté baptisé **Incontroller**) à des outils d'attaques (probablement Russes) visant les systèmes industriels (SCADA, OT, …). C'est une découverte d'importance majeure et comparable à Stuxnet (cf. § 3.5).
	Le **Costa Rica** est victime d'une série d'attaques du ransomware CONTI. Le désordre créé amène le président du Costa Rica à déclarer l'état d'urgence début mai.
Mai 2022	Vulnérabilité Office "**ms-msdt**" (aka "**Follina**"). Un chercheur montre qu'il est possible de déclencher une exécution de code au moyen d'un document Word piégé grâce au handler "ms-msdt:". Cette vulnérabilité sera très largement médiatisée (peut-être parce que l'attaque se fait sans macro) et des attaques seront observées.
	Le malware **Raspberry Robin** est découvert par Red Canary. Il sera très actif tout au long de l'année. Il se propage (entre autre) en infectant des clés USB : cette méthode beaucoup vue dans le passé avait presque disparu. Selon les dernières analyses Raspberry Robin serait un botnet de type pay-per-install : il installe à la demande des malwares sur les machines qu'il a infectées.

Juin 2022	**OT:ICEFALL** : Forescout publie sous ce nom une étude qui identifie 56 vulnérabilités impactant une dizaine de constructeurs SCADA. C'est pour nous un des événements marquants de l'année pour le domaine de la sécurité des systèmes industriels (cf. § 3.5.1).
Juillet 2022	Un vol de données **affectant un milliard de citoyens chinois** est découvert : Sur le forum de pirates "Breach Forums", un utilisateur sous le nom de ChinaDan a mis en vente 23To d'informations liées à près d'un milliard de Chinois, pour la somme de 10 bitcoins.
	Zimbra Collaboration (logiciel de Webmail) est victime d'une série d'attaques en juillet et en août au moyen des vulnérabilités CVE-2022-27925 et CVE-2022-37042. En octobre de nouvelles attaques sont signalées pour cette fois la vulnérabilité CVE-2022-41352.
	Pig Butchering scam: Le FBI alerte contre ce type d'arnaque qui consiste à convaincre des victimes de rejoindre un groupe d'investisseurs en crypto-monnaie.
Août 2022	**LastPass** (un service en ligne de coffre de mots de passe) annonce qu'il a subi une intrusion et que des codes sources ont été volés. Fin décembre LastPass annoncera que les pirates sont revenus et ont volé cette fois des données utilisateurs (données chiffrées mais des attaques hors-lignes sont possibles). LastPass n'apporte peu de précision ce qui pousse beaucoup d'utilisateurs à critiquer l'outils et à appeler à son abandon.
	Log4J : la CISA américaine publie le rapport de la CSBR (comité créé par le gouvernement des Etats-Unis après l'attaque SolarWinds en 2020 pour analyser les attaques majeures) sur Log4J. Cette vulnérabilité découverte en décembre 2021 est restée très active en 2022 (cf. § 3.1.1) avec surtout des attaques étatiques.
	TLP 2.0 : La version 2 du protocole TLP est publiée par le FIRST. TLP est un protocole qui définit les règles de diffusion pour un document. Nota : Il existe un autre protocole très utilisé dans la communauté des CERT : le PAP. Il définit ce que l'on a droit de faire avec une information reçue. Le TLP définit la diffusion autorisée, alors que le PAP définit l'usage autorisé.
Septembre 2022	Vulnérabilités **ProxyNotShell** dans Exchange. Après ProxyLogon et ProxyShell en 2021, cette 3eme série de vulnérabilités a été découverte en 2022. Nous en parlons (brièvement) au § 3.1.1.
	Attaque **MFA Fatigue** : Un employé d'**Uber** a été visé au moyen d'une nouvelle technique d'attaque appelée « MFA fatigue ». Nous la décrivons au § 3.8.1.
	Deadbolt : ce ransomware apparu en janvier 2022 attaque plus particulièrement les serveurs NAS **QNAP** (et ASUSTOR) exposés sur Internet. Il fera beaucoup parler de lui tout au long de l'année et en particulier en septembre.
	Optus, un des principaux opérateurs Télécom en Australie annonce avoir subi un vol de données (10 millions de comptes clients). Le vol est dû à une **absence de protection sur les API.** Les attaquants réclament une forte rançon pour ne pas publier les données, puis finalement abandonnent, probablement de peur des poursuites possibles.
	Edward Snowden obtient la nationalité Russe. Il reçoit son passeport Russe en décembre. Depuis ses révélations sur la NSA en 2013, Snowden est réfugié en Russie.
Octobre 2022	**Fortinet** est touché par plusieurs vulnérabilités critiques. En octobre c'est la vulnérabilité CVE-2022-40684 : elle concerne l'interface d'administration Fortinet qui ne devrait jamais être exposée sur Internet, mais ShadowServer indique que 17 415 sont dans ce cas ! En décembre, c'est la vulnérabilité CVE-2022-42475 qui est découverte dans le service très sensible de VPN SSL. Fortinet est critiqué à cette occasion car il n'a diffusé l'information qu'à ses clients « premium », laissant les

	autres clients dans l'ignorance de cette faille pendant un laps de temps non négligeable (que des attaquants peuvent exploiter).
	Fuite de donnée **BlueBleed** chez Microsoft: La société **SocRadar.io** a découvert que Microsoft avait mal sécurisé un espace de stockage Cloud (un "Azure Blob Storage") que Microsoft utilise pour stocker des données clients. Cela pouvait permettre à un tiers d'accéder illégalement à ces données.
Novembre 2022	**Opera1er** : GroupIB et Orange dévoilent l'existence d'un groupe de pirates francophones visant des banques en Afrique, qui aurait dérobé plus de 30 millions de dollars au cours de 30 attaques menées de 2019 à 2021.
Décembre 2022	**ChatGPT** montre les capacités d'un moteur d'IA. Parmi les multiples usages possibles certains s'inquiètent qu'il puisse être utilisé pour écrire des logiciels malveillants.

3 Analyse des phénomènes les plus marquants de 2022

Dans ce chapitre nous analysons les phénomènes les plus marquants de l'année :

- Les principales vulnérabilités
- Les malwares Infostealer dominent l'actualité 2022
- Une année de stabilisation pour les ransomwares ?
- La guerre RU-UA redéfinit le rôle du cyber dans un conflit
- La menace SCADA augmente avec le malware PIPEDREAM
- Les attaques de la Supply-Chain visent aussi les activités externalisées
- La montée des Hackers-for-hire et des produits offensifs pour les Etats
- Les autres phénomènes observés :
    - Attaques sur les MFA
    - Attaques visant les satellites ?
    - BruteRatel et les nouveaux outils offensifs
    - Windows : Bring Your Own Vulnerable Driver
    - Moins d'Exploits publiés avant les attaques

3.1 Les principales vulnérabilités

3.1.1 En bref

Les attaques les plus marquantes de l'année 2022 concernent les produits suivants :

- **F5 BIG-IP** : vulnérabilité CVE-2022-1388, qui a donné lieu à l'alerte Orange CERT-IST/AL-2022.006 en mai 2022,
- **Atlassian Confluence Server** : vulnérabilité CVE-2022-26134, alerte Orange CERT-IST/AL-2022.008 en juin 2022,
- **Fortinet** : vulnérabilité CVE-2022-40684, avec une alerte Orange CERT-IST/AL-2022.012 en octobre 2022, puis CVE-2022-42475, avec une alerte Jaune CERT-IST/AL-2022.015 en décembre 2022,
- **Zimbra Collaboration**. vulnérabilités CVE-2022-27925 et CVE-2022-37042 (en août 2022) puis CVE-2022-41352 (en octobre). Nota : ce produit a été ajouté fin octobre au suivi Cert-IST et n'a donc pas donné lieu à des alertes Cert-IST. Par contre nous avons émis le message **INFO-2022.019**.

Il faut aussi ajouter à cette liste les vulnérabilités de 2021 qui sont restées très actives en 2022 :

- **Microsoft Exchange :** Après ProxyLogon et ProxyShell en 2021, une 3eme série de vulnérabilités, nommée **ProxyNotShell** a été découverte en 2022. Ces vulnérabilités ont été utilisées dans des attaques 0-day à partir de juillet 2022 par des attaquants étatiques (probablement chinois). Les correctifs Microsoft sont disponibles depuis octobre, mais les attaques ont augmenté fin 2022 après la publication d'un programme d'exploitation.
- **Log4J** : Cette vulnérabilité découverte en décembre 2021 a cessé d'être dans les phares de l'actualité fin janvier, mais son exploitation dans des attaques s'est poursuivie au-delà, avec par exemple des attaques étatiques signalées par Ahnlab (société Sud-Coréenne) en mai, par l'US-CERT en juin, et par Microsoft en août.

3.1.2 Les autres attaques de 2022

Le tableau ci-dessous détaille les 16 alertes émises par le Cert-IST en 2022.

Alerte	Référence	Description	Date
Jaune	CERT-IST/AL-2022.001	Risque d'attaques contre les systèmes Linux/Unix (vulnérabilité de l'outil pkexec du **package Polkit**)	26-janv-22
Jaune	CERT-IST/AL-2022.002	Risque d'attaques contre les **applications SAP** utilisant le composant Internet Communication Manager (ICM)	10-févr-22
Jaune	CERT-IST/AL-2022.003	Risque d'attaques **"Dirty Pipe"** contre les systèmes Linux (CVE-2022-0847)	10-mars-22
Jaune	CERT-IST/AL-2022.004	Attaques visant **VMware Workspace ONE Access et Identity Manager** (CVE-2022-22954)	14-avr-22
Jaune	CERT-IST/AL-2022.005	Risque d'attaques visant **Microsoft RPC** (CVE-2022-26809)	15-avr-2022
Orange	CERT-IST/AL-2022.006	Attaques en cours visant **F5 BIG-IP** (CVE-2022-1388)	09-mai-22
Jaune	CERT-IST/AL-2022.007	Risque d'attaques visant **VMware Access, vIDM, vRA et vRealize Suite Lifecycle Manager** (CVE-2022-22972)	27-mai-22
Orange	CERT-IST/AL-2022.008	Attaques en cours visant les serveurs **Confluence** (CVE-2022-26134)	03-juin-22
Jaune	CERT-IST/AL-2022.009	Attaques en cours via la vulnérabilité Windows MSDT **"Follina"** (CVE-2022-30190)	08-juin-22
Jaune	CERT-IST/AL-2022.010	Risque d'attaques visant **VMware Access, vIDM, vRA et vRealize Suite Lifecycle Manager** (CVE-2022-31656, CVE-2022-31659 et CVE-2022-31660)	11-août-22
Jaune	CERT-IST/AL-2022.011	Attaques 0-day visant **Microsoft Exchange** (variante de ProxyShell)	30-sept-22
Orange	CERT-IST/AL-2022.012	Attaques en cours visant les équipements fonctionnant sur **FortiOS** (CVE-2022-40684)	17-oct-22
Orange	CERT-IST/AL-2022.013	Attaques en cours visant **Adobe Commerce** (anciennement Magento Commerce) avec CVE-2022-24086	16-nov-22
Jaune	CERT-IST/AL-2022.014	Risque d'attaques visant **F5 BIG-IP** (CVE-2022-41622)	22-nov-22
Jaune	CERT-IST/AL-2022.015	Attaques en cours visant les équipements fonctionnant sur **FortiOS** (CVE-2022-42475)	13-déc-22
Jaune	CERT-IST/AL-2022.016	Attaques visant **Citrix Application Delivery Controller (ADC) et Citrix Gateway** (CVE-2022-27518)	14-déc-22

3.2 Les malwares Infostealer dominent l'actualité 2022

3.2.1 En bref

L'actualité de 2022 a montré plusieurs fois que certaines attaques dans les entreprises se déroulent sans exploiter de vulnérabilité :

- L'attaquant achète sur le site web d'un IAB (Initial Access Broker) des données d'authentification volées
- Puis, il rentre dans l'entreprise en utilisant ces données. Suivant les cas (et le niveau de protection) il va rentrer dans l'entreprise (vol d'un compte VPN) ou simplement dans un service Cloud externalisé (par exemple un espace GitLab ou GitHub privé).

Ces attaques fonctionnent bien parce que les accès à distance se sont généralisés (d'une part avec le télétravail et d'autre part avec le développement du Cloud et de la dé-périmétrisation) et que des attaques contre le MFA ont été mises au point (cf. § 3.8.1). Elles génèrent une demande croissante sur le marché des IAB qui est alimenté grâce à des malwares appelés des Infostealers.

Un Info-Stealer est un logiciel malveillant qui a pour but de voler les données d'authentifications présentes sur le poste de la victime (mot de passe sauvegardés, cookie de session), les crypto-monnaies, ainsi que quelques données techniques annexes. Les plus célèbres des Infostealers sont **Racoon** et **RedLine**.

Au cours de l'année 2022, une augmentation massive des attaques au moyen d'Infostealers a été observée.

Nota : **L'autre malware marquant de l'année, après l'Infostealer, c'est le Wiper** que l'on a vu de façon incessante dans des cyber-attaques de la Russie contre l'Ukraine (cf. § 3.4.1).

3.2.2 La chaine d'infection : du Navigateur Web jusqu'au Bot-Shops

Voici une séquence type de ce que l'on peut observer dans une infection par un Infostealer :

- La victime télécharge un logiciel "cracké" : ces logiciels contiennent presque toujours des malwares, et c'est souvent un Infostealer.
- L'Infostealer vole les comptes et mots de passe que l'utilisateur a stocké dans son navigateur web. Si ce dernier a activé la synchronisation de ses données web entre navigateurs, on peut même parfois retrouver sur le poste personnel de l'utilisateur les données de ses comptes professionnels.
- Les comptes volés sont envoyés par le malware au pirate, puis mis en vente sur un site marchand que les cybercriminels appellent un **Bot-Shop** ou **Log-Shop**. Le plus célèbre est Genesis. Ces "boutiques" vendent l'ensemble complet des données collectées sur la machine infectée. Ce lot de données est appelé un « Log ». Il contient les identifiants, les cookies, mais aussi les caractéristiques techniques de la machine (résolution d'écran, CPU, RAM). Cette panoplie d'informations permet à l'attaquant de se faire passer pour l'ordinateur de la victime et ainsi de contourner des protections anti-fraude (ce sont des outils qui détectent les bots et les faux clics).

3.2.3 Comment se protéger ?

Nous n'avons pas vu d'étude spécifique qui propose des solutions à ces attaques par Infostealer, mais les pistes suivantes sont à examiner :

- Sensibiliser les utilisateurs aux dangers des logiciels téléchargés sur Internet (dans un contexte professionnel ou personnel). Au-delà des logiciels piratés (qui sont illégaux) il faut que les utilisateurs soient prudents lorsqu'ils téléchargent des logiciels, car certains sites proposent des versions piégées des logiciels originaux gratuits. Il faut donc toujours chercher le site officiel (par exemple en consultant la fiche Wikipédia) plutôt que de télécharger le 1er site proposé par une recherche Google.
- Eviter de sauver les logins et mots de passe dans le navigateur web car beaucoup de logiciels malveillants savent voler ces mots de passe. Il vaut mieux utiliser un coffre-fort à mots de passe (par exemple KeePass) qui sont beaucoup moins exposés à ce type d'attaque.
- Ne jamais synchroniser ses comptes professionnels entre plusieurs ordinateurs, ne jamais utiliser les mots de passes de ses comptes d'entreprise pour d'autres comptes ou pour des sites n'appartenant pas à l'entreprise.
- Etudier la possibilité de surveiller si des comptes relatifs à l'entreprise sont mis en vente sur des market-places d'IAB.
- Lorsqu'une infection par Infostealer est détectée, déterminer les comptes compromis et faire changer les mots de passe.

3.3 Une année de stabilisation pour les ransomwares ?

3.3.1 En bref

Nous reproduisons ci-dessous la Une de notre bulletin mensuel de décembre 2022 qui donne les tendances que nous avons observées. Globalement, au cours de l'année 2022 :

- Il a été observé une baisse du nombre d'attaques de ransomware en début d'année (1ere semestre) et les attaques de type chantage aux données volées ont pris une part croissante.
- Mais les attaques de ransomware sont revenues en force à partir de septembre 2022.

Une du bulletin mensuel Cert-IST de décembre 2022 (publié en janvier 2023):

En ce début d'année 2023, beaucoup d'articles sont publiés à propos de l'évolution future des ransomwares. Sans faire de prédiction, voici quelques tendances que nous avons vues au cours de notre activité :

- 2022 a été une année de stabilisation, alors que 2021 avait été l'année de l'explosion du nombre d'attaques connues. D'après le journaliste Valérie Reiss-Marchive (LeMagIT), qui est intervenu lors de notre Forum 2022 en décembre (cf. notre article plus loin dans ce bulletin), il y a eu en France en 2022 un nombre d'attaques équivalent à ce qui avait été vu en 2021 (cf. l'article de LeMagIT).
- Il y a eu beaucoup d'établissements de santé attaqués. Cependant il n'est pas certain que ce secteur d'activité soit plus ciblé que les autres et l'explication est peut-être que l'on porte plus d'attention à ces attaques.
- En début d'année 2022, les « vrais » ransomware étaient plutôt en baisse et on a observé à leurs places des attaques de type vol de données (et chantage à leur publication). On appelle souvent ces incidents des « data-leak extorsions »). Les vrais ransomwares sont revenus en force par la suite, en particulier à partir de septembre 2022.
- Il faudrait trouver un autre terme que « ransomware », parce que maintenant ce terme est utilisé aussi bien pour les vrais ransomwares que pour les « data-leak extorsions ». Le terme ransomware a tendance à être utilisé pour toutes les intrusions cybercriminelles amenant à un chantage.
- Un nombre croissant d'états utilisent des attaques de ransomware. (cf. TheRecord.media) Certaines fois, c'est pour dissimuler une action de sabotage (on fait croire que c'est un ransomware, mais le but est de bloquer les machines et il n'y a pas de négociation de rançon). Cela a été vu en 2022 par exemple dans des attaques russes contre l'Ukraine ou dans des attaques de l'Iran contre Israël. D'autres fois, il s'agit d'attaques visant à capter des devises, en particulier pour des pays soumis à embargo. La Corée du Nord pratique ces attaques depuis plusieurs années, et l'Iran semble le faire aussi depuis 2021.

Nota : Voici quelques articles sur ce sujet, en plus que ceux cités ci-dessus : TheRecord.media 2, Trend Micro, EMSI soft, BlackFog.

3.3.2 *Les effets inattendus de la guerre RU-UA et le leak de CONTI*

Une partie significative des groupes cybercriminels sont basés en Russie et dans les pays satellites. Il est donc possible que la baisse des attaques de ransomware au 1er semestre soit liée à la guerre de la Russie contre l'Ukraine et soit due à la suspension des activités de certains cybercriminels. Ce n'est qu'une hypothèse, mais il semble qu'il y ait eu plusieurs arrestations de cybercriminels lorsqu'ils ont quitté la zone d'influence de la Russie du fait de la guerre. Ce serait le cas de l'auteur du malware Zeus et également de celui du malware Racoon.

Le groupe de ransomware CONTI s'est disloqué au début de la guerre parce que certains membres étaient pro-Russe alors que d'autres étaient pro-Ukrainien. Une quantité importante de données internes ont été rendues publique à cette occasion en particulier des informations inédites sur la structure de ce groupe cybercriminel. CONTI était l'un des plus importants groupes de ransomware. La fuite de donnée montre qu'il faisait travailler une équipe de 80 à 100 personnes et avait une structure d'entreprise, avec son service RH, des équipes chargées de l'infrastructure et un budget conséquent pour l'achat de services (par exemple pour avoir des renseignements financiers sur les entreprises attaquées) ou de logiciels (par exemple pour acheter le logiciel offensif Cobalt Strike).

3.3.3 *La lutte contre les groupes de ransomware se densifie*

Les groupes de ransomware sont restés très actifs en 2022. Mais la lutte contre ces groupes s'est également poursuivie. On peut noter par exemple en 2022 les arrestations des groupes cybercriminels REvil et Lapsus$ et la neutralisation du groupe HIVE (début 2023).

A partir de mai 2021 (et l'incident Colonial Pipe aux Etats-Unis), les gouvernements ont intensifié leur lutte contre les ransomwares. C'était l'un des phénomènes marquants que nous avions identifié dans notre bilan 2021. Il est clair que ce mouvement se poursuit en 2022.

3.4 La guerre RU-UA redéfinit le rôle du cyber dans un conflit

3.4.1 En bref

La guerre de la Russie contre l'Ukraine est le premier conflit armé dans lequel le cyber prend une place entière, puisque la Russie maitrise parfaitement cette arme et a déjà réalisé, depuis 2015, plusieurs cyber-attaques d'ampleur contre l'Ukraine.

On ne connait très probablement qu'une partie des attaques qui ont été réalisées par la Russie ou par l'Ukraine, mais on peut en retenir les points suivants :

- Il n'y a pas eu de cyber-Armageddon (i.e. de chaos déclenché par des attaques cyber tout azimut). Le cyber semble donc plutôt une arme de reconnaissance et de déstabilisation plutôt qu'une arme de destruction.
- Les attaques russes connues sont surtout des cas de Wipers (logiciels d'effacement de données visant à mettre hors service des ordinateurs). En dehors des Wipers, l'attaque la plus marquante est celle des modems du satellite KA-SAT (modems utilisés par l'armé ukrainienne pour accéder à Internet). Nous en parlons au § 3.8.2.
- En plus des attaques étatiques, il y a eu une mobilisation importante de mouvements Hacktivistes qui ont réalisé des attaques pro-Ukrainienne ou pro-Russes. Ces attaques ont été encouragées par les Etats (qui ont publié des listes de cibles à viser). Ces attaques ont eu un effet limité (même si elles ont eu des résultats réels) et ont plus contribué à créer du désordre qu'à donner un avantage significatif. Il a aussi été fait appel aux civils pour des actions défensives comme par exemple pour signaler les passages de drones.
- Les sociétés américaines Microsoft et Amazon ont eu un rôle défensif important en migrant et en hébergeant dans le Cloud les données des administrations Ukrainiennes. Ce déplacement des données amène des interrogations sur la souveraineté puisque l'on considère généralement que le maîtrise des données (et de leur hébergement) est un point clé de souveraineté.
- Le « Hunt-forward » pratiqué par les américains (des actions défensives par anticipation, voir ci-dessous) est une approche qui n'avait pas été documentée jusque-là et qui sera sans doute reprise par d'autres.

3.4.2 Le « Hunt-Forward »

Une du bulletin Cert-IST de mai 2022

Au début de la guerre de la Russie contre l'Ukraine, les cyber-attaques étatiques russes ont semblé plutôt moins importantes que l'on pouvait redouter (cf. la Une de notre bulletin de Février). *[…]* Si l'effet de ces opérations a été assez limité (pour ce qui est publiquement connu) c'est peut-être du fait des opérations de « Hunt Forward » que les Etats-Unis ont annoncées avoir menées. Ces opérations consistent à anticiper d'éventuelles crises cyber en envoyant des experts pour analyser la situation de terrain. On imagine qu'ils recherchent des traces de compromissions (découvertes d'agent dormants) ou donnent des recommandations pour renforcer la sécurité ou faciliter la reprise après une attaque (sauvegardes, PRA, etc.). Les Etats Unis ont indiqué avoir mené 9 opérations de « Hunt Forward » en Ukraine et mentionnent en particulier une opération de 2 mois débutée fin 2021. Ce type d'opérations existerait depuis 4 ans et 28 missions dans 16 pays auraient été réalisées.

Nota : Le principe d'anticiper l'arrivée d'une attaque que l'on voit ici avec le Hunt-Forward s'illustre aussi probablement (ce n'est qu'une hypothèse) avec la découverte du malware PIPEDREAM puisque selon la rumeur, les Etats-Unis seraient allés voler ce malware chez l'attaquant plutôt que d'attendre qu'il soit trouvé au cours d'une attaque réelle (cf. § 3.5.2).

3.5 La menace SCADA augmente avec le malware PIPEDREAM

3.5.1 En bref

L'un des événements marquants de l'année 2022 est pour nous la découverte du toolkit d'attaque PIPEDREAM. Il s'agit d'un malware spécialisé dans l'attaque d'installations industrielles. Sa découverte est aussi importante que la découverte de Stuxnet en 2010 car il montre que désormais les attaques sont conçues pour contourner les défenses actuelles (le cloisonnement en zones) des réseaux industriels.

PIPEDREAM est probablement un outil russe. La Russie est l'acteur le plus présent dans le domaine des attaques de systèmes industriels. On peut imaginer bien sûr que d'autres pays étudient aussi ce type d'attaques. La Chine, les Etats-Unis et les autres pays avancés dans le domaine cyber, développent sans doute aussi ces compétences, mais cela est beaucoup plus discret.

Un autre événement marquant de l'année est **la publication en juin, par la société Forescout, d'une étude baptisée OT:ICEFALL.** Cette étude a identifié 56 vulnérabilités qui impactent une dizaine de constructeurs (comme Honeywell, Siemens ou Yokogawa). Il s'agit pour la plupart de vulnérabilités « by design » et cela montre les faiblesses de sécurité que l'on trouve encore pour les systèmes industriels (Forescout compare la sécurisation des systèmes industriels à l'ascension de l'Everest et le nom « Icefall » fait référence à l'une des premières étapes de cette l'ascension). La dernière partie de l'étude montre comment utiliser ces vulnérabilités dans des scénarios d'attaques (attaque d'un pipeline de transport gazier, attaque de turbines éoliennes et attaque d'une chaine de fabrication). Contrairement au très sophistiqué PIPEDREAM, OT:ICEFALL montre que dans certains cas mettre au point une attaque industrielle n'est pas forcément très compliqué.

Nota : Le Cert-IST a émis le message **INFO-2022.013** pour avertir notre communauté à propos de cette actualité OT:ICEFALL.

3.5.2 *Le toolkit PIPEDREAM / Incontroller*

Une du bulletin mensuel Cert-IST d'avril 2022 :

Mi-avril, la CISA américaine ainsi que les sociétés Dragos et Mandiant, ont publié la description d'un nouveau malware (ou plutôt d'une boite à outils composée de plusieurs malwares) conçu pour attaquer les systèmes industriels (ICS). Il a été baptisé **PIPEDREAM** (par Dragos) et **INCONTROLLER** (par Mandiant). Ce malware est considéré comme un nouveau « grand » malware ICS à placer dans la lignée de Stuxnet (2010), Industroyer (2016) et TRITON (2017). Il fait suite aussi à l'annonce quelques jours plus tôt d'une tentative d'attaque Industroyer2 en Ukraine. **Ces 2 événements montrent que la menace d'attaques visant les systèmes industriels croit de façon inquiétante.**

Les origines de PIPEDREAM sont mystérieuses. Dragos a dit que ce malware lui a été donné par une source de confiance et qu'il n'a pas été utilisé dans des attaques réelles. La rumeur dit que PIPEDREAM aurait été volé par les services secrets américains dans les instituts de recherche Russe (peut-être le TsNIIKhM qui est accusé d'avoir mis au point TRITON). Avec la montée en sophistication des attaques contre les systèmes industriels, et du fait des impacts potentiellement catastrophiques de ce type d'attaques, on peut en effet imaginer qu'une approche offensive ait été choisie, consistant à aller chercher le malware chez l'attaquant plutôt que d'attendre qu'il soit trouvé au cours d'une attaque.

Le fait de révéler publiquement ce malware permet de :

- forcer l'attaquant à changer son malware (et donc le retarder),
- prévenir les victimes potentielles et les inciter à se protéger.

Pour aider les victimes à se protéger, le SANS a publié un webcast qui détaille les capacités offensives du malware et propose une démarche globale pour la sécurité : PIPEDREAM and Countering ICS Malware (compte SANS gratuit nécessaire).

3.6 Les attaques de la Supply-Chain visent aussi les activités externalisées

L'attaque via la chaine des fournisseurs (la Supply-chain) était l'un des faits majeurs que nous identifions l'an dernier dans notre bilan sur l'année 2021. En 2022 ce sujet reste une préoccupation forte. Pour rappel nous avions décomposé ce sujet en 3 domaines :

- *Attaque via un MSP (Managed Services Provider) : Un infogérant ayant un accès au réseau de l'entreprise, subit une attaque et son accès privilégié est ensuite utilisé par l'attaquant pour rentrer dans l'entreprise visée.*
- *Attaque via un autre fournisseur ou partenaire (autre qu'un MSP).*
- *Attaque via un logiciel ou un matériel envoyé par un fournisseur officiel. Ce logiciel aura préalablement été piégé à l'insu du fournisseur.*

• Les attaques visant les logiciels se poursuivent

En 2022, les attaques les plus observées ont concerné des cas de librairies piégées (par exemple **NPM**, **PyPi** ou **Ruby**). Il s'agit de la dernière catégorie ci-dessus.

Nous avons également relevé une attaque visant Travis.CI, ce qui montre que l'attaque des environnements de développement (ici le CI/CD) reste un domaine qui monte en puissance (c'était un des faits majeurs que nous avions noté en 2021).

• Des attaques visant les activités externalisées apparaissent

L'attaque la plus intéressante est celle groupe cybercriminel LAPSUS$ contre OKTA en janvier 2022 (rendue publique en mars) : pour voler les identifiants OKTA, LAPSUS$ s'est attaqué à une société chargée par OKTA du support technique des clients OKTA. Cette société (Sitel) avait donc accès aux outils permettant de réinitialiser des accès OKTA. Il s'agit d'un cas particulier des attaques de la Supply-Chain via un fournisseur (2eme catégorie dans notre classement ci-dessus), mais qui pourrait constituer une catégorie à part entière : les attaques sur les processus métiers qui ont été externalisés (les BPO : Business Process Outsourcing).

Nota : Nous avons publié le message **INFO-2022.004** à propos de cette attaque contre OKTA.

3.7 La montée des Hackers-for-hire et des produits offensifs pour les états

• L'affaire Pegasus se poursuit

Lors de l'été 2021, l'affaire Pegasus, avait mis en évidence les usages abusifs de l'outil Pegasus vendu par la société NSO. Il permet d'espionner les téléphones portables de personnes jugées dangereuses ; conçu pour lutter contre le terrorisme, il a aussi été utilisé par certains états pour surveiller des journalistes et des opposants. Ce « marché sale » des outils de surveillance est connu depuis 2015 au moins, mais 2021 a montré que les abus étaient plus larges que ce qui était connu.

En 2022 la prise de conscience du phénomène s'est poursuivie avec par exemple en Europe la mise en évidence de l'utilisation de Pegasus en Espagne (avril 2022) ou d'un logiciel équivalent (Predator) en Grèce. Le Parlement Européen a lancé en mars 2022 la commission PEGA pour enquêter sur ce phénomène des usages abusifs. Aux Etats-Unis, la Chambre des Représentants a organisé fin juillet 2022 une audition publique sur le sujet au cours de laquelle Google, Microsoft et CitizenLab.ca ont présenté leurs témoignages.

Pegasus n'est pas le seul logiciel de cette catégorie. On connait aussi **Candiru** (de la société Israélienne éponyme), **Predator** (de la société **Cytrox** basée en Macédoine) ou **Hermit** (des sociétés italiennes RCS Lab et Tykelab). Il est probable qu'il en existe d'autres.

• Hackers for hire

Il y a visiblement une demande de la part des Etats pour disposer d'outils offensifs. Google a indiqué en 2022 avoir recensé plus de 30 sociétés sur le marché de la vente aux États de 0-day et d'outils offensifs de Cybersécurité. Google a plus récemment cité dans cette catégorie la société espagnole **Variston** qui propose un outil d'attaques baptisé **Heliconia**.

Il y a aussi une tendance à faire appel à des sociétés de « Hacking for Hire » (piratage à la demande) pour prendre en charge l'approche et l'attaque de cibles. Fin 2021 Facebook a publié un rapport identifiant sept sociétés qui proposent, à des degrés divers, ces services. Six de ces sociétés sont nommées dans le rapport : Cobwebs, Cognyte, Black Cube, Bluehawk, BellTroX et Cytrox.

• Un marché qui s'adresse progressivement aux entreprises

Les outils et services développés pour les Etats se diffusent aussi progressivement vers un public plus large. Le « Hacking for hire » proposé aux entreprises est d'un niveau de sophistication très variable. Il peut s'agir d'attaques de Spear-phishing ordinaires, comme exposées dans un article Reuter de juin 2022 décrivant le service proposé par des sociétés Indiennes et qui vise principalement des cabinets d'avocats. Il peut s'agir également d'attaques plus sophistiquées, aux moyens de failles 0-day, comme décrit dans le rapport KNOTWEED de Microsoft en juillet 2022 à propos de la société Autrichienne **DSIRF**. Cette dernière indique dans ses publicités qu'elle propose des services "avancés" de collecte et d'analyse d'informations, destinés aux entreprises internationales.

Groupes Cyber-mercenaires recensés par le Cert-IST dans le cadre du service « Veille sur les attaques et IOC »

- **Bahamut** (CERT-IST/ATK-2017-068) : Organisation mercenaire réalisant du cyber-espionnage au Moyen Orient et en Asie du sud.
- **Dark Basin** (CERT-IST/ATK-2020.066) : Groupe de hackers mercenaires ayant visé des milliers d'individus dans le monde. Citizen Lab attribue les activités de Dark Basin à des employés d'une société indienne nommée **BellTroX InfoTech Service.**
- **DeathStalker** (CERT-IST/ATK-2020.090) : Groupe de hackers mercenaires visant les secteurs financiers et juridiques.
- **CostaRicto** (CERT-IST/ATK-2020.126) : Campagne de cyber-espionnage menée par un groupe de hackers mercenaires proposant des attaques de type APT.
- **Void Balaur** (CERT-IST/ATK-2021.131) : Groupe de cybermercenaires russophones vendant des boîtes mail et autres données privées (aussi connu sous le nom de **Rockethack**).
- **KNOTWEED** (CERT-IST/ATK-2022.082) : Groupe de "hacking-as-a-service" de la société autrichienne **DSIRF.**

3.8 Les autres phénomènes observés

3.8.1 Attaques sur les MFA

Avec la généralisation du MFA, les attaquants sont obligés de mettre au point de nouvelles techniques d'attaques. En 2022 deux nouvelles techniques ont été observées :

- Le MFA fatigue
- Le pass the cookie

Nous détaillons ces attaques dans l'encart ci-dessous. Bien sûr, ce n'est pas parce que des attaques existent qu'il faut abandonner le MFA.

Article Cert-IST publié dans le bulletin mensuel de septembre 2022

Les attaques visant le MFA

Alors que l'utilisation du MFA (Multi-Factors Authentification) se généralise pour renforcer la sécurité des accès, les attaquants progressent aussi dans ce domaine et mettent au point des attaques contre certains de ces systèmes MFA. Durant l'été 2022, deux attaques de ce type ont été médiatisées :

- Des utilisateurs **OKTA** ont été visés par une large campagne de phishing (via des SMS les invitant à se connecter sur leur compte OKTA) qui a touché des sites comme **Twilio**, Cloudflare, Klaviyo MailChimp et Doordash. Nous avons consacré un article à ce sujet.
- Un employé **Uber** a été visé par une attaque appelée « MFA fatigue » : son téléphone a été inondé de messages de notification MFA et il a fini par accepter l'un d'eux, ce qui a autorisé l'accès pour le pirate.

Nous avons publié en 2018 un article sur les attaques de « SIM swap » qui visaient à cette époque le MFA par SMS. Voici aujourd'hui une synthèse plus globale des techniques d'attaques connues contre les systèmes MFA.

Les différentes techniques de MFA :

Voici les 4 techniques de MFA actuellement utilisées.

1 : **MFA par SMS** : Un code secret est envoyé par SMS sur le téléphone de l'utilisateur au moment de sa connexion.
2 : **MFA via une application « Authentificator »** : Un code secret est généré toutes les 30 secondes par une application installée sur le téléphone de l'utilisateur. Ces applications (comme par exemple Google Authenticator, Authy, Duo ou Microsoft Authenticator) utilisent un algorithme T-OTP pour générer ce code secret.
3 : **MFA par « Push notification »** : Une fenêtre popup apparait sur le téléphone de l'utilisateur au moment où celui-ci se connecte sur le site. Il doit confirmer via cette popup qu'il autorise cet accès.
4 : **MFA via une clé FIDO2** : Un algorithme cryptographique est utilisé pour réaliser l'authentification en suivant le protocole FIDO2. Ce type d'algorithme est implémenté par exemple par les clés hardware Ubikey.

Quelle que soit la technique MFA utilisée, pour éviter de redemander à chaque connexion une authentification complète, un mécanisme de **cookie d'authentification** est souvent mis en place : si l'utilisateur dispose déjà d'un cookie valide (non expiré), alors sa nouvelle connexion est acceptée sans aucune autre authentification (et il n'y a donc pas de MFA) : c'est la fonction « se souvenir de moi » qui est présente sur de très nombreux sites.

Les attaques connues

Voici les attaques connues.

- **SIM swap** (vise le mécanisme 1) : L'attaquant se fait passer pour la victime auprès de l'opérateur téléphonique de cette dernière et demande une nouvelle carte SIM. Avec cette SIM, il reçoit désormais les SMS envoyés par le système MFA. L'attaque est plutôt complexe (il faut convaincre l'opérateur) et utilisée pour des cibles de valeurs, par exemple pour voler le portefeuille de crypto-monnaie de la victime.
- **Phishing MFA** (vise les mécanismes 1 et 2) : L'attaquant attire la victime sur un faux site qui va relayer vers le vrai site, les données échangées lors de la connexion, y compris le code MFA. Il s'agit d'une attaque MiTM (Man in The Middle). Elle fonctionne pour les MFA de type SMS ou Authenticator. Il existe des outils pour implémenter cette attaque (comme par exemple le service payant EvilProxy, ou le projet open-source evilgophish).
- **Vol de cookie d'authentification** (vise les mécanismes 1, 2, 3 et 4) : Si un malware (de type Infostealer) a infecté le poste de la victime, alors il peut voler les cookies d'authentification et si ceux-ci ne sont pas expirés, se connecter sans authentification (et donc sans MFA). Ce type d'attaque semble gagner en popularité depuis le début de l'année 2022, probablement du fait de services illégaux de type BotShop comme Genesis (dont nous parlions dans notre article de mai 2022) qui vendent les données volées par les Infostealers.
- **MFA fatigue** (vise le mécanisme 3) : Il s'agit de la technique d'attaque la plus récemment documentée et que nous décrivons en début d'article pour l'attaque subie par Uber. Il est probable qu'elle deviendra rapidement obsolète grâce à l'amélioration des popups « Push notification » (par exemple il suffirait d'inclure une fonction « Mute », activée par l'utilisateur, qui bloquerait ces popups pour une durée donnée, par exemple une demi-heure).

Conclusion

Même s'ils sont attaqués, les mécanismes de MFA sont un progrès important pour la sécurité de l'authentification et il faut poursuivre les efforts pour les déployer. Pour les pirates, ils sont devenus un point de passage obligé lorsqu'ils attaquent des cibles bien défendues. Il est donc logique de voir des tentatives de contournement et les attaques contre les MFA.

Pour plus d'information

- MFA Fatigue (et solutions possibles) :
  https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/
  https://www.securityweek.com/high-profile-hacks-show-effectiveness-mfa-fatigue-attacks

- Techniques de MFA :
  https://jumpcloud.com/blog/push-notification-mfa

3.8.2 Attaques visant les satellites ?

L'attaque par les Russes du satellite KA-SAT (exploité par ViaSat) est un des événements cyber marquants de la guerre contre l'Ukraine. Il ne s'agit pas d'une attaque visant le satellite lui-même, mais du service rendu (la communication Internet par satellite). Néanmoins cet événement s'inscrit dans une tendance plus générale qui est que les satellites sont depuis ces dernières années devenus des cibles d'attaques :

- En 2018 la France a annoncé vouloir défendre ses satellites contre des attaques par des satellites d'autres pays. Depuis septembre 2019 la France dispose d'un Commandement de l'Espace et fin 2019 les Etats-Unis ont créé l'USSF (la US Space Force, 6eme branche de l'armée américaine)
- Depuis de nombreuses années, des tests de tir de missiles contre des satellites sont réalisés. Le plus récent est un tir Russe en novembre 2021.

Dans ce contexte, les attaques cyber contre les satellites est un sujet de plus en plus envisagé. On peut noter d'ailleurs que depuis 2020, l'US Air-Force a mis en place concours annuel appelé « Hack A Sat » pour explorer ce domaine.

3.8.3 BruteRatel et les nouveaux outils offensifs

Il y a 2 ans, nous avons indiqué que Cobalt Strike (un outil commercial vendu pour réaliser des exercices d'attaques) était devenu l'outil le plus utilisé dans des attaques réelles, très souvent dans des cas de ransomwares, mais aussi quelque fois dans des attaques étatiques (par exemple l'attaque SolarWinds).

En 2022 un outil similaire a commencé à faire parler de lui : **Brute Ratel C4**

Cet outil a déjà été vu dans des attaques réelles (voir par exemple l'analyse publiée en juillet 2022 par Palo Alto Networks) et plusieurs analystes estiment que ce phénomène va s'amplifier.

D'autres outils similaires ont été cités (mais à un degré moindre) :

- **Sliver** : outil open-source de la société Bishop Fox, disponible sur GitHub et décrit par Microsoft en août 2022
- **Havoc** : outil open-source disponible sur GitHub
- **Manjusaka** et **Ninja** : outils open-source disponibles sur GitHub et cités par Kaspersky
- **Nightawk** : outil commercial de la société MDSec

Le projet C2 Matrix a identifié plus de 100 projets proposant des outils offensifs.

3.8.4 *Windows : Bring Your Own Vulnerable Driver*

Le **BYOVD** (Bring Your Own Vulnerable Driver) est une technique d'attaques dont on a beaucoup parlé en 2022. Elle permet à un attaquant ayant déjà obtenu les privilèges SYSTEM sur une machine Windows, d'exécuter du code dans le noyau Windows.

L'accès au noyau (le « kernel mode ») est protégé, et seuls les codes signés (avec une signature approuvée par Microsoft) sont autorisés à s'exécuter dans le noyau. Pour contourner cette protection la technique du BYOVD procède ainsi :

- Elle installe un driver authentique (par exemple un driver développé par Dell ou par Avast) qui est signé, mais pour lequel il existe une vulnérabilité connue.
- Elle exploite ensuite cette vulnérabilité pour forcer ce driver à exécuter des actions malveillantes.

L'attaque BYOVD a été vue plusieurs fois en 2022, ce qui en fait désormais une technique classique.

Pour lutter contre le BYOVD, Microsoft a établi une liste des drivers vulnérables connus, et dispose d'une fonction qui bloque l'installation de ces drivers. Malheureusement ce mécanisme n'était pas correctement implémenté pour Windows 10 et Windows Server ce qui a amplifié les discussions sur le BYOVD.

3.8.5 *Moins d'Exploits publiés avant les attaques*

Pour une vulnérabilité, l'évolution classique de la menace suit les étapes suivantes :

1	Attaques ciblées ou limitées (ex. 0-days)
2	Exploit privé annoncé (ex. vidéo)
3	PoC (Proof Of Concept) public
4	Rapports techniques
5	**Exploit public**
6	Attaques isolées
7	Utilisation de la vulnérabilité par un malware
8	Attaques massives

Toutes les étapes ne sont pas forcément présentes, mais l'étape 5 (publication d'un exploit sur Internet) est utilisée par beaucoup comme un indicateur de la nécessité de patcher la vulnérabilité rapidement (parce que des attaques vont se multiplier et toucher un plus grand nombre de victimes que les attaques 0-day initiales).

Cet indicateur est en train de changer et il n'est pas rare désormais de voir les cas d'attaques se multiplier sans qu'un programme d'exploitation ait été rendu public. Nous avons constaté cela par exemple :

- Pour la vulnérabilité **ProxyNotShell** dans Microsoft Exchange (alerte **CERT-IST/AL-2022.011** du 30/09/2022) où le programme d'exploitation n'a été publié que 2 mois plus tard (le 30/11/2022).

- Pour la vulnérabilité CVE-2022-24086 dans **Adobe Commerce (anciennement Magento Commerce)**. Cette vulnérabilité a été corrigée par Oracle en février 2022 (sans avoir été exploitée en 0-day) et à notre connaissance il n'y a toujours pas de programme d'exploitation public. Par contre on sait qu'il y a eu une montée progressive des attaques à partir de septembre 2022 et cela nous a amené à publier l'alerte **CERT-IST/AL-2022.013** le 16/11/2022. Il est probable qu'un programme d'exploitation privé (non rendu public) a circulé dans le milieu cybercriminels.

Il est important de prendre conscience de cette évolution car si ce constat se confirme il faudra ajuster les processus de déclenchement d'alerte et de priorisation des correctifs de sécurité.

4 Productions du Cert-IST en 2022

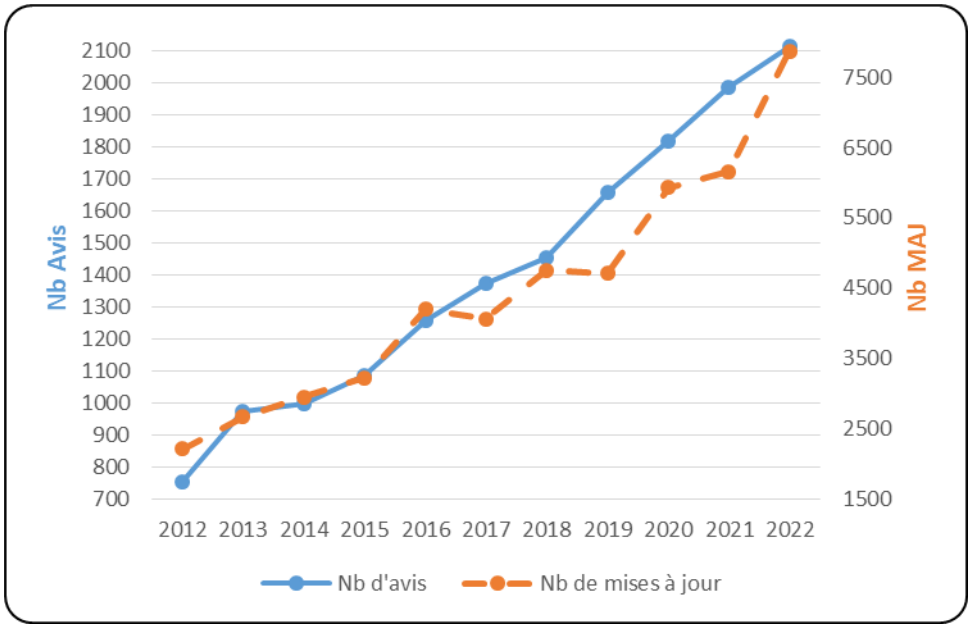
4.1 Veille sur les vulnérabilités et les menaces

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 entre CERTs, etc.) afin d'être informé des nouvelles vulnérabilités. Ces informations sont analysées quotidiennement pour fournir à nos adhérents des informations triées, qualifiées et priorisées.

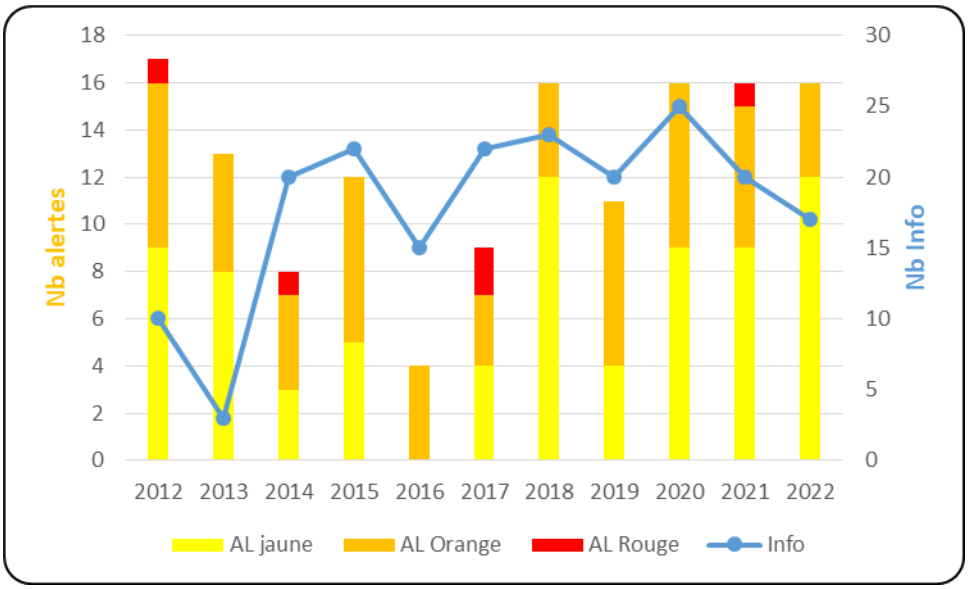
Le Cert-IST émet ainsi plusieurs types de publications :

- **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, Exploit-Kit, Ransomware), ainsi que les attaques de cyber-espionnages (attaques APT) et les ransomware les plus importants.

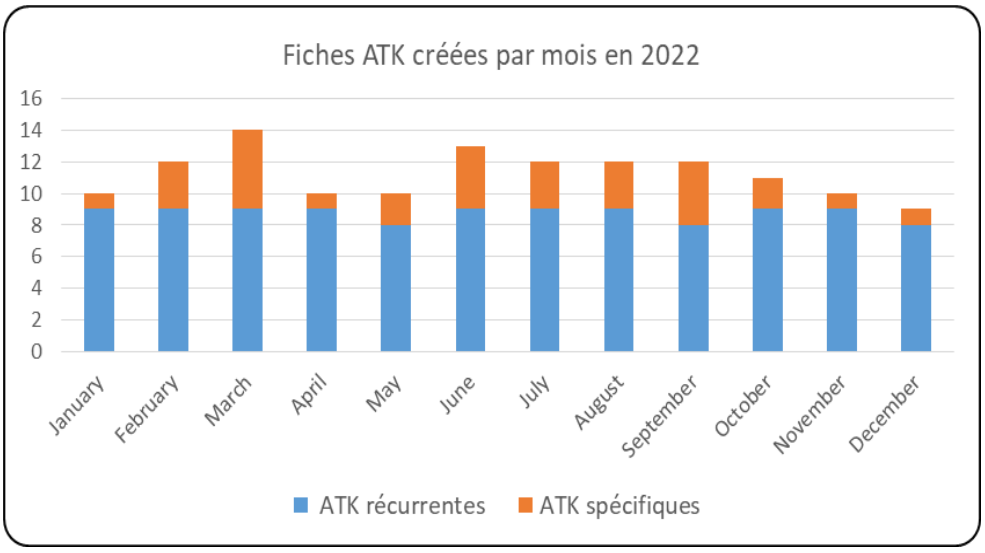
Les graphiques ci-dessous montrent la production du Cert-IST au cours des dernières années.



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



Nombre d'alertes publiées par an



Nombre de fiches attaques publiées par mois

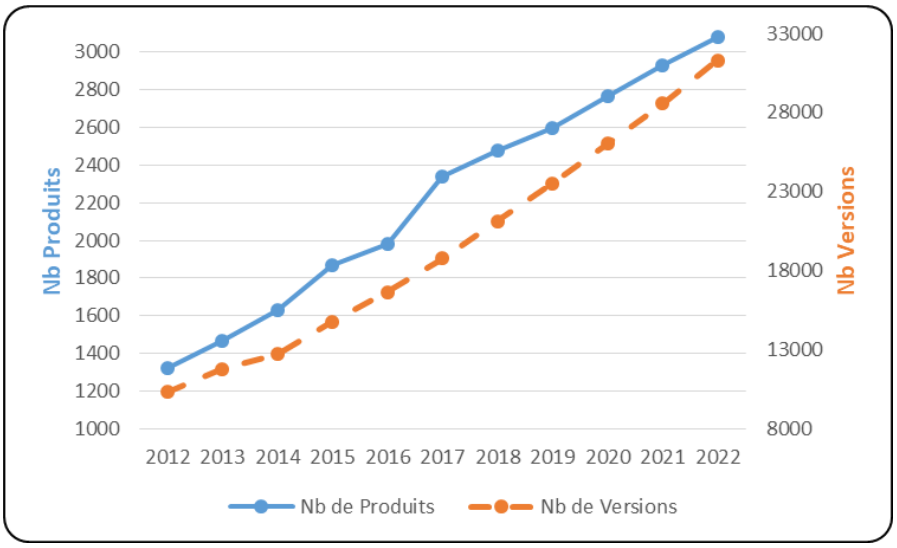
Ainsi, en 2022, le Cert-IST a publié :

- **2 115** avis de sécurité (dont **120** avis SCADA), **7 875** mises à jour mineures et **170** mises à jour majeures.
  Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), avec en 2022 une augmentation de **6%** par rapport à 2021. 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.
- **16** alertes et **17** 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). D'année en année,

l'activité dans cette catégorie est très fluctuante, mais depuis 2018 le nombre d'alerte par an s'est stabilisé (exception faite de 2019).

- **135** fiches attaques ont été publiées en 2022, avec dans la base de données MISP **3 765** évènements enrichis par l'équipe Cert-IST, et **855 717** marqueurs (IOC) ajoutés. Au total il y a **6,2 millions** de marqueurs dans la base MISP Cert-IST.

Concernant les produits et les versions suivis par le Cert-IST, fin 2022 le Cert-IST suivait **3 080** produits et **31 281** versions de produits. Le graphique suivant montre l'évolution du nombre des produits et des versions qui sont suivis par le Cert-IST.



4.2 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.

5 Conclusions

Les attaques visant l'identité sont de plus en plus fréquentes.

Depuis 2020 (et l'attaque SolarWinds) on sait que les attaquants avancés cherchent les faiblesses des systèmes d'authentification avec des attaques SAML, OAuth ou PKI.

On a vu en 2022 que les cybercriminels visent les comptes utilisateurs, en les volant grâce aux malware Infostealer (comme Racoon ou RedLine, cf. § 3.2) et en contournant l'authentification MFA par de nouvelles techniques (cf. § 3.8.1).

Ces deux phénomènes montrent que certains attaquants préfèrent se faire passer pour des vrais utilisateurs, plutôt que d'exploiter des vulnérabilités pour entrer sans compte valide. Et c'est ce que l'on constate lors des analyses post-attaques. Bien sûr la recherche de vulnérabilités existe toujours (voir ci-dessous) mais **le vol des mots de passe (ou d'autres données d'authentification comme les cookies, etc) est un des phénomènes marquants de l'année.**

Avec la montée en puissance des solutions Zero-Trust Architecture (ZTA), l'attaque de l'identité est un risque critique : si l'on parvient à tromper le ZTA sur son identité, la protection s'effondre.

L'attaque des équipements exposés sur Internet continuent d'augmenter.

Dans les années 2010, les attaques visaient majoritairement le poste de travail de l'utilisateur en exploitant les vulnérabilités des logiciels installés sur ce poste (Flash, Java, PDF).

Dans les années 2015, les attaques visaient l'utilisateur, en incitant celui-ci à ouvrir un document piégé (avec le retour des attaques par macros) ou à donner ses mots de passe (avec des attaques de phishing).

Depuis 2019, les attaques se font aussi de plus en plus souvent en exploitant les vulnérabilités découvertes dans les équipements exposés sur Internet (attaques de VPN ou d'appliances exposées). Ce phénomène se confirme en 2022. D'ailleurs, il est probable que si l'on cumule les intrusions au moyen de mots de passe volés (1er phénomène identifié ci-dessus) avec les intrusions grâce à des vulnérabilités sur les équipements exposés, on dépasse le nombre d'intrusion réalisée par infection directe d'un poste de travail au moyen d'un mail ou d'un site web piégé.

Les chantiers de fond demeurent.

L'actualité de 2022 montre que pour les entreprises les domaines suivants restent une priorité :

- Se préparer à une éventuelle attaque de ransomware, ou à un chantage aux données volées. Cela peut-être par exemple au moyen d'exercices de crises, ou d'études sur la résilience en cas de cyber-attaque.
- Prendre en compte les attaques via la Supply-chain, en particulier en travaillant sur ces sujets avec ses fournisseurs (lorsqu'on est donneur d'ordres) et en analysant la sécurité de ses environnements de développement logiciels (voir sur ce sujet notre bilan de l'an dernier)
- Poursuivre la sécurisation des systèmes industriels (SCADA, OT, etc).

La veille sur les menaces et les attaques reste un atout important pour structurer sa cyber-sécurité

L'année 2022 a été riche en actualité dont la plus importante est sans aucun doute la guerre Russie/Ukraine. Sur le plan cyber, cela influencera probablement de façon notable la défense, en particulier sur des aspects de résilience en cas d'attaque.

Plus généralement, la multiplication des attaques et du nombre de vulnérabilité, ainsi que l'évolution rapide des technologies rend indispensable une veille permanente sur les menaces.

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