Cert IST

Industrie Services Tertiaire

Bilan Cert-IST des failles et attaques de 2021

Publié en Février 2022

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 présentons dans un premier temps une rétrospective de l'actualité de 2021 (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 2022.

> ➢ **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 2021

2.1 Le Top 8 pour 2021

Parmi l'ensemble de l'actualité que nous présentons dans ce chapitre, voici notre classement des événements qui, pour nous, sont les plus marquants pour l'année 2021 :

- Attaques **ProxyLogon et ProxyShell** dans Microsoft Exchange,
- Vulnérabilité Apache **Log4J**,
- Vulnérabilités **PrintNightmare**,
- Retour des attaques **NTLM Relay** (PetitPotam),
- Attaque de REvil contre **Kaseya**
- Attaque **Pegasus** et vulnérabilités **Zéro-Clic** visant Apple (ForcedEntry)
- Attaques **Codecov.io** visant les environnements CI-CD
- La montée en puissance de la recherche de vulnérabilités dans **Microsoft Azure**

A propos de ce 8ème événement, nous reproduisons ci-dessous la Une de notre bulletin mensuel de septembre 2021 qui développe cet aspect.

Une du bulletin mensuel Cert-IST de septembre 2021:

En un mois (du 30 août au 29 septembre 2021), nous avons publié 3 messages d'information pour des problèmes touchant le Cloud Azure de Microsoft : **INFO-2021.023** sur Azure Cosmos, **INFO-2021.026** sur OMI et **INFO-2021.027** sur l'attaque en force brute des mots de passe Azure. A chaque fois, il s'agit de chercheurs qui ont prévenu Microsoft suite à leurs travaux sur Azure. Et ces annonces vont sans doute inciter d'autres chercheurs à se pencher également sur ce sujet. **Il faut donc s'attendre à une multiplication des vulnérabilités découvertes dans Azure (et Microsoft 365).**

L'incident SolarWinds fin 2020 avait montré que les attaquants étatiques (en l'occurrence probablement la Russie) étaient déjà sur ces sujets, avec des attaques visant l'authentification Azure et Microsoft 365 (attaques Golden SAML). Le fait que des entreprises de sécurité publient sur ces sujets et donc plutôt bénéfique, puisque cela va permettre de mettre en évidence (et de corriger) des problèmes qui sont peut-être déjà des 0days connus de certains états.

Ces publications récentes montrent enfin que la recherche de vulnérabilités dans le Cloud est en train de changer, pour s'intéresser à des choses plus techniques que ce que l'on connaissait déjà. En effet, jusqu'à présent on parlait plutôt de problèmes de mauvaises configurations des infrastructures, avec par exemple des Buckets AWS mal protégés, que n'importe qui pouvait venir consulter. Maintenant les chercheurs s'intéressent aussi aux protocoles sous-jacents et à la façon dont les mécanismes de sécurité sont implémentés. On a donc franchi une étape dans le niveau de maturité de la recherche des vulnérabilités des solutions Cloud.

2.2 Les événements marquants de 2021

Le tableau ci-dessous récapitule des événements marquants de 2021, 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 2021	**Démantèlement Emotet, Arrestation Netwalker** : Les opérations de lutte contre le cybercrime débutent dès janvier et vont se poursuivre tout au long de l'année 2021 : • Contre les ransomware : Netwalker (janvier), Egregor (février), Clop (juin), REvil (octobre). Certains groupes vont d'ailleurs stopper d'eux-mêmes leurs activités : DarkSide (mai), Avaddon (juin) et Blackmatter (novembre). • Contre certains mass-malware : Emotet (janvier et avril) • Contre des infrastructures : Shutdown de DoubleVPN (juin), Darkweb Operation Dark HunTor (octobre) Bien sûr, c'est un jeu sans fin : Trickbot revient en février, Emotet en novembre. Et quand un ransomware stoppe son activité, il renait souvent sous une autre forme : En 2021 REvil laisse place à DarkSide puis BlackMatter puis BlackCat (ALPHV).

Janvier 2021	**Sudo Baron Samedit :** Une vulnérabilité découverte par Qualys dans la commande « sudo » sur Linux et Unix permet à un utilisateur d'obtenir les privilèges « root ». C'est une simple élévation de privilèges, mais la faille est triviale à exploiter (avec un programme d'exploitation) et touche un très grand nombre de distributions Linux, mais aussi Solaris, AIX et macOS.
Janvier 2021	**SonicWall** commence une année difficile : attaques 0-day contre le produit VPN **SMA** en janvier et février puis **Email Security** en avril puis à nouveau **SMA et SRA** en juin**.** Nous avons publié les messages **INFO-2021.003** , **INFO-2021.010** et **INFO-2021.017** pour ces actualités. **Zyxel** (un autre constructeur de VPN) annoncera aussi en janvier puis en juin des failles critiques dans ses produits.
Février 2021	**La station d'eau de la ville d'Osmard (Floride**) est piratée, et le niveau de fluorine augmenté à un niveau dangereux. L'enquête montre que l'ordinateur d'un employé a été piraté, ce qui a donné accès à la station d'eau (grâce au TeamViewer présent sur l'ordinateur). La catastrophe a été évitée car l'opérateur en charge de la station a vu le niveau de fluorine anormal.
Février 2021	**Confusion de dépendances.** Un chercheur décrit une technique d'attaque qui tire parti de la façon dont les outils de génération de code (ou d'installation de packages) vont chercher leurs dépendances (les librairies ou les packages liés). Le problème est à nouveau illustré en juin car un chercheur pirate accidentellement le site Microsoft du jeu Halo. Nous abordons ce problème de dépendances au paragraphe 3.6.1 qui traite de la Supply-chain logicielle
Février 2021	**France : Des attaques Russes (Sandworm) visant Centreon.** L'ANSSI publie un rapport pour des attaques (de 2017 à 2020) visant de vieilles versions du logiciel de supervision Centreon. Il s'agit probablement d'attaques du groupe Sandworm. *(Nous avons publié le message **INFO-2021.006** pour cet événement).*
Mars 2021	**Accellion FTA :** Des cybercriminels utilisent des 0-day dans le logiciel FTA de Accellion pour voler des documents et faire du chantage à des clients utilisant FTA. Parmi les victimes, il y a Singapore-Telecom. (en févier) puis Qualys et Shell (en mars).
Mars 2021 Top Actu	**Attaque ProxyLogon visant Exchange**. Cette attaque a été utilisée ponctuellement en janvier par le groupe Hafnium, puis massivement à partir de mars par différents types d'attaquants. Nous détaillons cette actualité au paragraphe 3.1.
Mars 2021	**France : Incendie du data-center OVH** à Strasbourg. Il s'agit d'un accident, probablement d'origine électrique.
Mars 2021	**France : Le laboratoire Pierre Fabre** est touché par un **ransomware**. C'est une victime parmi des centaines qui ont été touchées en France en 2021. Parmi elles, on peut citer aussi **Manutan**, (attaqué en février) dont le partage d'expérience sur cette crise a été très apprécié. A l'international, on se rappelle aussi du ransomware ayant touché **Accenture** en août. L'ampleur de l'incident a été apparemment beaucoup moins grande que ce qu'a prétendu le groupe LockBit (à l'origine de l'attaque). Nous mentionnons aussi plus loin dans ce tableau les attaques **Colonial Pipe** (mai), **Kaseya** (juin)

Avril 2021	**Attaque contre un centre nucléaire à Natanz en Iran.** On a évoqué la possibilité que ce soit une cyber-attaque, mais à notre connaissance les faits ne sont pas clairement établis.
Avril 2021 Top Actu	**Attaque Codecov.io « Bash Uploader » :** Un pirate modifie le script « Bash Uploader » dans l'environnement Cloud de la société Codecov.io, et pendant 2 mois (février et mars) récupère des données à propos des logiciels développés en mode CI/CD par des tiers (par exemple Rapid7 et IBM). Nous parlons de cette actualité au paragraphe 3.6.2 qui traite de la Supply-chain logicielle
Avril 2021 Top Actu	**Attaques NTLM relay :** Déjà connues des spécialistes, les attaques NTLM Relay ont fait un retour remarqué cette année : - en avril avec l'attaque **RemotePotato0** - en juillet avec l'attaque **PetitPotam** - et janvier 2022 avec l'attaque **ShadowCoerce** **PetitPotam** est considérée comme l'attaque la plus dangereuse parce qu'elle peut être combinée avec l'attaque ESC8 présentée en juin dans l'étude Certified Pre-Owned: Abusing ADCS. Elle permet à un attaquant sans compte (mais déjà sur le réseau interne de l'entreprise) de prendre le contrôle de la PKI Microsoft (ADCS). *(Nous avons publié le message INFO-2021.018 à propos de cette attaque)*
Avril 2021	**21Nails** : Il s'agit d'une série de 21 vulnérabilités dans Exim (serveur de messagerie sous Linux/Unix) découverte par Qualys. Nous avons émis l'alerte jaune **CERT-IST/AL-2021.007** pour la plus grave (CVE-2020-28018) mais il n'y a pas eu d'attaques massives observées par la suite**.**
Avril 2021	**Vulnérabilité BadAlloc dans les RTOS** (Real-Time OS) : Microsoft publie une série de 25 vulnérabilités après une étude des OS temps réel utilisés par exemple dans l'automobile ou dans les équipements médicaux. L'OS le plus cité par la presse est QNX de Blackberry.
Mai 2021	**Colonial Pipeline** est touché par une attaque de ransomware du groupe DarkSide. Suite à cette attaque la Maison Blanche déclare la lutte contre les ransomwares comme une priorité nationale. Le sujet est aussi abordé lors du sommet du G7 en juin 2021.
Mai 2021	**Vulnérabilité WiFi FragAttack.** Un chercheur publie une série de 12 vulnérabilités dans les fonctions de fragmentation et d'agrégation (d'où le nom FR-AG) des trames Wifi. *(Nous avons publié le message INFO-2021.012 à propos de cette actualité)*
Mai 2021	**Vulnérabilités dans Nagios**. Depuis l'attaque SolarWinds Orion en 2020, les logiciels de supervisions sont regardés attentivement par les chercheurs. - En mai skylightcyber.com publie un premier rapport sur 13 vulnérabilités dans Nagios ainsi qu'un outil d'attaque publié **SoyGun**. - En octobre Synacktiv.com publie 5 vulnérabilités - En novembre grimm-co.com publie 11 vulnérabilités.
Juin 2021	**Le piégeage des téléphones ANOM par le FBI et la police australienne** permet l'arrestation de criminels. Ces téléphones sécurisés étaient vendus aux criminels sur un marché parallèle. Cette opération rappelle l'infiltration en 2020 sur les téléphones **EncroChat** par les polices en France et aux Pays-Bas.
Juin 2021	**ALPACA** : une nouvelle technique d'attaque TLS. Il s'agit d'un travail universitaire et l'attaque semble pour le moment difficile à réaliser. Elle met en évidence en particulier le danger des certificats TLS jokers (de type *.my-company.com). *(Nous avons publié le message INFO-2021.015 à propos de cette actualité)*

Juin 2021	**Décès de John McAfee** dans une prison espagnole. Personnage sulfureux et fantasque à l'origine du célèbre antivirus, il s'est apparemment suicidé dans la prison où il était détenu.
Juin 2021 Top Actu	**PrintNightmare :** La saga autour des failles dans le Print Spooler de Microsoft débute en juin par la publication (accidentelle ?) d'un PoC pour une vulnérabilité supposée corrigée en juin par Microsoft. Elle durera une bonne partie de l'été, avec la publication d'un patch urgent au bout d'une semaine, aussitôt contourné, puis la publication de nouveaux correctifs … entrainant des problèmes d'impression !
Juin 2021 Top Actu	**Attaque Kaseya :** Suite à une faille dans la solution VSA de la société Kaseya, le groupe REvil parvient à rentrer chez des MSP et à infecter les clients de ces MSP. Près de 1500 entreprises sont finalement infectées. Le groupe REvil demande 70 millions de dollars, mais finalement une clé de déchiffrement sera donnée le 23 juillet à Kaseya par une source gardée secrète. L'incident avait débuté le 2 juillet. *(Nous avons publié le message INFO-2021.020 à propos de cette actualité)*
Juillet 2021 Top Actu	**Pegasus** : un consortium de journalistes révèle que les usages abusifs du logiciel d'espionnage de la société NSO (conçu pour lutter contre le terrorisme) sont bien plus larges que ce qui était déjà connu. Les Nations Unis demandent un moratoire sur la vente de ce type de logiciel (en août). Le gouvernement Israélien interdit par la suite l'exportation de Pegasus vers 65 pays (en novembre).
Juillet 2021	**Vulnérabilité SeriousSAM** dans Windows. C'est l'une des vulnérabilités Windows qui agitera l'actualité de juillet (avec PrintNightmare et PetitPotam), et sans doute la moins grave : une vulnérabilité dans la Base de Registres Windows permet des attaques sur la SAM (Security Account Manager).
Août 2021	**Fuite de données chez T-Mobile :** les données volées concernent 50 millions de clients de l'opérateur télécom. C'est la 4eme fuite de données connue chez T-mobile après août 2018, novembre 2019, et mars 2020. Une 5eme sera ensuite annoncée en décembre 2021.
Août 2021	**Linux a 30 ans** cette année. Et apparemment **le mot de passe informatique fête ses 60 ans.**
Septembre 2021	**Vulnérabilités BrakTooth dans le Bluetooth.** Une série de 16 vulnérabilités est publiée par des chercheurs universitaires. Et en novembre un programme de démonstration est rendu disponible. Ce n'est pas un événement exceptionnel, puisque des vulnérabilités Bluetooth sont découvertes chaque année.
Septembre 2021	**Les produits de Zoho ManagEngine** font l'objet d'une série d'attaques de cyber-espionnage (possiblement chinoises) qui ciblent successivement les produits **ADSelfService Plus** (révélées en septembre) puis **ServiceDesk Plus** (révélées en décembre), puis **Desktop Central** (décembre également).
Septembre 2021	**Vulnérabilités Apple Zero-clic FORCEDENTRY** : Apple publie un correctif pour la plus célèbre des vulnérabilités Zéro-clic (utilisée depuis mi-2020 par Pegasus).
Septembre 2021 Top Actu	**Vulnérabilité OMIGOD** (à prononcer « Oh My God! ») **dans Microsoft Azure** : Des chercheurs de Wiz.io découvrent une vulnérabilité critique dans le composant OMI (Open Management Infrastructure) qui est installé automatiquement par Microsoft dans certaines VM Linux déployées dans Azure.

Octobre 2021	**Attaque LightBasin contre 13 opérateurs télécom**. CrowdStrike publie un rapport sur cette attaque et montre le niveau de sophistication que peut atteindre une attaque conçue spécifiquement pour un domaine d'activité particulier. Les opérateurs télécom sont une cible fréquente des attaques de cyber-espionnage. Pour 2021, on peut citer par exemple : Operation Diànxùn (mars), Deadringer (août), Operation GhostShell (octobre)
Octobre 2021	**Cyberattack 64411 en Iran**. En octobre, une attaque mystérieuse (non expliquée) paralyse des pompes de stations-services en affichant le message « Cyberattack 64411 ». 64411 est le numéro de téléphone du guide suprême iranien Ali Khamenei. Ce numéro avait déjà été affiché lors d'une attaque début juillet ayant paralysé le service ferroviaire.
Novembre 2021	**Meris DDOS botnet.** Un nouveau botnet (découvert en juin) bat des records et se fait une place à côté des traditionnels botnets de la famille Mirai.
Novembre 2021	**Lancement de la base KEV de la CISA :** KEV est l'acronyme de Known Exploited Vulnerabilities. C'est une base qui référence les vulnérabilités déjà exploitées et que les agences fédérales américaines doivent obligatoirement prendre en compte (en appliquant les correctifs). KEV est présenté par la CISA comme un complément de la base NVD.
Décembre 2021 Top Actu	**Log4j** : La vulnérabilité **Log4Shell** (CVE-2021-44228) dans la librairie Apache Log4j a entrainé un travail acharné au sein des entreprises pour identifier les installations vulnérables et les protéger.
Décembre 2021	**iLOBleed un rootkit visant HP iLO** découvert par une société iranienne. Le rootkit est très sophistiqué et l'analyse de la société iranienne remarquable.

3 Analyse des phénomènes les plus marquants de 2021

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

- **Exchange ProxyLogon** : l'attaque majeure de l'année 2021
- **Ransomware** : les attaques continuent
- Les autres **chantages visant les entreprises**
- **Crypto-monnaies** : les attaques visant les plates-formes et les actifs se multiplient
- Les attaques via la **Supply-Chain**
- **Codes sources : une nouvelle cible** d'attaques
- Multiplication du **nombre de vulnérabilités**
- **Log4j** : que faut-il en retenir ?
- **Géopolitique** et attaques étatiques

3.1 Exchange ProxyLogon : l'attaque majeure de l'année 2021

3.1.1 En bref

Les attaques ProxyLogon (en mars 2021) et ProxyShell (août 2021) contre les serveurs Exchange "On-Premise" sont, de notre point de vue, les attaques les plus marquantes de l'année 2021. Elles ont été utilisées comme points d'entrée dans des intrusions par des acteurs étatiques (attaques APT) aussi bien que par des cybercriminels (attaques de ransomware).

En 2020 le vecteur d'intrusion le plus courant avait été les vulnérabilités des VPN et Appliances (BIG IP, Citrix, Palo Alto Networks, Pulse Secure). En 2021 ce sont les vulnérabilités Exchange. Et pour 2022, ce sera peut-être les attaques au moyen des vulnérabilités Log4j ?

3.1.2 Zoom sur ProxyLogon et ProxyShell

Microsoft Exchange (On-premise) a été la cible en 2021 de 2 séries d'attaques :

- **ProxyLogon** en mars 2021 pour laquelle nous avons fait une **alerte rouge** **CERT-IST/AL-2021.003**. Il est très rare que le Cert-IST utilise ce niveau d'alerte (les précédents cas étaient en 2017 avec WannaCry et NotPetya). L'encart ci-dessous explique plus en détail cette crise.
- **ProxyShell** en août 2021 pour laquelle nous avons fait une alerte orange **CERT-IST/AL-2021.010**

Du fait de ces attaques, un grand nombre de serveurs Exchange qui n'avaient pas été patchés immédiatement après la publication des correctifs Microsoft ont été compromis, et cela tout au long de l'année 2021.

Extrait du bulletin mensuel Cert-IST à propos de ProxyLogon :

Le 02/03/2021, Microsoft a publié des correctifs « hors bande » (en dehors des correctifs mensuels) pour 7 vulnérabilités critiques affectant le serveur Exchange. Deux de ces vulnérabilités (CVE-2021-26855 et CVE-2021-27065) ont été utilisées dans des attaques ponctuelles début janvier 2021 (attaques par le groupe Hafnium, décrites par Microsoft et Volexity), puis à une échelle plus large vers le 27 février, et c'est sans doute cela qui a décidé Microsoft à publier les correctifs.

A partir du 03/03/2021 les attaques ont encore augmenté en nombre, et comme aucun programme d'exploitation n'a été diffusé sur Internet avant le 11/03/2021, on peut supposer que les programmes d'attaques se sont transmis dans des cercles fermés. Rien de ce qui suit n'a été confirmé mais il est possible qu'il y ait eu 2 fuites successives à propos de ces attaques :

- Le découvreur officiel des 2 vulnérabilités (la société Taiwanaise DEVCORE) s'est peut-être fait voler sa découverte fin décembre 2020 par le groupe Hafnium qui l'a utilisé début janvier (ou alors Hafnium et DEVCORE ont découvert ces vulnérabilités de façon indépendante),
- Un des participants du programme Microsoft MAPP s'est peut-être fait voler le PoC que Microsoft a publié dans MAPP mi-février 2021. Cela pourrait expliquer la vague d'attaques qui a commencé le 27 février.

Pour cette crise Exchange le Cert-IST a publié le 03/03/2021 :

- L'avis de sécurité **CERT-IST/AV-2021.0339** pour décrire les vulnérabilités et les correctifs disponibles,
- La fiche attaque **CERT-IST/ATK-2021.029** pour décrire le groupe **HAFNIUM,**
- L'alerte **CERT-IST/AL-2021.003** (au niveau jaune).

Le 04/03/2021 un blog a été créé dans le HdC (Hub de Crise) pour suivre l'évolution de cette menace (11 articles postés dans ce blog durant le mot de mars). Le même jour, nous avons fait passer l'alerte au niveau rouge lorsque nous avons constaté l'augmentation rapide des attaques visant Exchange.

3.1.3 Les autres attaques de 2021

Le tableau ci-dessous détaille les 16 alertes émises par le Cert-IST en 2021.

Alerte	Référence	Description	Date
Jaune	CERT-IST/AL-2021.001	Risque d'attaques **Sudo** contre les systèmes Linux/Unix (CVE-2021-3156)	31-janv.-21
Orange	CERT-IST/AL-2021.002	Attaques en cours contre **VMware vCenter** Server (CVE-2021-21972)	25-févr.-21
Rouge	CERT-IST/AL-2021.003	Attaques en cours contre **Microsoft Exchange Server (ProxyLogon)**	03-mars-21
Jaune	CERT-IST/AL-2021.004	Risque d'attaques visant **SAP** Solution Manager	11-mars-21
Jaune	CERT-IST/AL-2021.005	Risque d'attaques visant **F5 BIG-IP** (CVE-2021-22986)	22-mars-21
Orange	CERT-IST/AL-2021.006	Attaques en cours visant **Pulse Connect Secure** (CVE-2021-22893)	21-avr.-21
Jaune	CERT-IST/AL-2021.007	Risque d'attaques visant **Exim sur Linux/Unix** (CVE-2020-28018)	19-mai-21
Jaune	CERT-IST/AL-2021.008	Attaques en cours visant **VMware vCenter** Server (CVE-2021-21985)	03-juin-21
Orange	CERT-IST/AL-2021.009	Attaques visant le Spouleur d'impression de Microsoft Windows (**PrintNightmare**)	01-juil.-21
Orange	CERT-IST/AL-2021.010	Attaques visant **Microsoft Exchange Server (ProxyShell)**	13-août-21
Jaune	CERT-IST/AL-2021.011	Attaques en cours visant **Atlassian Confluence** (CVE-2021-26084)	02-sept.-21
Jaune	CERT-IST/AL-2021.012	Attaques en cours visant **VMware vCenter** Server (CVE-2021-22005)	27-sept.-21
Jaune	CERT-IST/AL-2021.013	Risque d'attaques visant les **serveurs web Apache** (CVE-2021-41773)	06-oct.-21
Jaune	CERT-IST/AL-2021.014	Attaques visant **ManageEngine ADSelfService Plus** (CVE-2021-40539)	05-nov.-21
Jaune	CERT-IST/AL-2021.015	Attaques visant les **serveurs GitLab** (CVE-2021-22205)	05-nov.-21
Orange	CERT-IST/AL-2021.016	Attaques visant Apache **Log4j** (CVE-2021-44228)	10-déc.-21

3.2 Ransomware : les attaques continuent

3.2.1 En bref :

Très répandues depuis septembre 2019, les attaques de ransomware visant les entreprises (et les collectivités territoriales) se sont poursuivies en 2020 puis en 2021 à un rythme toujours croissant. Les 2 principaux phénomènes de l'année 2021 sont :

- Les états contre-attaquent et déploient des efforts sans précédents pour stopper les attaques les plus massives : démantèlements d'infrastructures, saisies de crypto-monnaies et arrestations. Les Etats-Unis ont été particulièrement actifs sur ces sujets suite aux attaques Colonial-Pipe (mai 2021) et Kaseya (juillet 2021), mais l'effort est international.
- Les assurances baissent leurs couvertures en cas de sinistres et augmentent leurs prix.

3.2.2 Etes-vous prêts en cas d'attaque de ransomware ?

Si elle est victime d'une attaque de ransomware, l'entreprise devra gérer une crise avec de multiples aspects :

- Quel est le périmètre compromis, et comment l'isoler ?
- Quels moyens informatiques utiliser pendant la crise ?
- Depuis quand les attaquants sont sur le réseau ?
- Les plans de backups et de reprises sont-ils adaptés pour ce type de crise
- Qui prévenir ? Comment communiquer : en interne, en externe, avec les attaquants ?
- Quelles aides extérieures pourra-t-on solliciter : Assurance, prestataires, autres ?
- Faut-il payer la rançon ?
- Etc.

Certaines de ces questions ne pourront être résolues qu'au cours de la crise, parce qu'elles sont trop dépendantes de la crise elle-même. Mais d'autres peuvent être anticipées et, préparer un plan de réponse pour ce type d'attaques est une action largement souhaitable.

De multiples guides ont été publiés sur ce sujet, en particulier par des organismes gouvernementaux :

- Canada : https://cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099
- France : https://www.ssi.gouv.fr/entreprise/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/ et https://www.ssi.gouv.fr/administration/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/
- Nouvelle-Zélande : https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/
- Royaume-Uni : https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- USA : https://www.cisa.gov/stopransomware

3.3 Les autres chantages visant les entreprises

Les attaques par ransomwares ne sont pas les seuls types de chantages cyber auxquels les entreprises sont confrontées. Globalement il y a une augmentation de ces chantages.

3.3.1 Chantage à la divulgation de données (Data Leak) :

Le pirate vole des données mais ne cherche pas à bloquer les ordinateurs de la victime (comme ferait un ransomware). Eventuellement, le pirate n'est même pas rentré sur les réseaux internes de l'entreprise visée et a volé les données sur un système exposé sur Internet ou chez un partenaire de la victime. Ces attaques ont augmenté en 2021 et le phénomène va sans doute s'amplifier en 2022. Par exemple Qualys a été visé en mars 2021 suite à l'attaque Accellion FTA.

3.3.2 Chantage aux attaques DDOS (Ransom DDOS) :

Le pirate menace de bloquer l'accès Internet si une rançon n'est pas payée, et fait une démonstration de sa force de frappe en réalisant une première attaque de courte durée. Ce type d'attaques qui existait déjà dans les années 2010 pour les sites de paris en ligne, a fait un retour en septembre 2019 en visant cette fois n'importe quel type d'entreprise. Depuis, le phénomène reste discret mais continue à toucher régulièrement de nouvelles victimes. Ces « Ransom-DDOS » (aussi appelées R-DDOS) apparaissent désormais dans une rubrique dédiée dans les rapports trimestriels des éditeurs de solutions de protection anti-DDOS.

3.3.3 Bientôt des attaques informationnelles ?

Une nouvelle catégorie de menaces devraient être prises en considération dans le futur par les entreprises : les attaques informationnelles (la diffusion de fausses informations au travers des réseaux sociaux, ou même des attaques cyber visant à porter atteinte à l'image de l'entreprise). Pour le moment ces attaques sont plutôt du domaine des états et concernent moins les entreprises. Mais on sait que les attaques étatiques ont souvent servi d'exemples pour d'autres attaques lancées ensuite à plus large échelle ; par exemple les attaques APT ont été d'abord des techniques militaires, puis ont été utilisées plus largement avec des visées économiques, pour finir par être utilisées aussi par les cybercriminels.

3.4 Crypto-monnaies : les attaques visant les plates-formes et les actifs se multiplient

Les attaques sur les crypto-monnaies, les problèmes de sécurité des plates-formes d'échange, et les attaques des protocoles spécifiques à la finance décentralisée (DeFI) ont été plus que jamais traités dans les médias IT cette année. En l'occurrence, **2021 est une année record quant aux vols et aux détournements de cryptomonnaies**, qu'ils soient menés via des escroqueries ou des attaques informatiques. Au total, les montants dérobés sont estimés autour des 14 milliards de dollars, à savoir presque le double de l'année précédente.

Le détournement de crypto-devises peut prendre des formes différentes, selon que l'attaquant vise l'utilisateur final, une société d'investissement, une plate-forme d'échange, ou même directement l'implémentation d'un protocole. On notera au passage que les protocoles / les plates-formes DeFI sont aussi un moyen de blanchiment de fonds, domaine sur lequel il reste toutefois difficile d'avoir des chiffres précis.

3.4.1 Attaques visant les plates-formes d'échange et les protocoles DeFI

Ce sont les événements les plus médiatiques, bien qu'ils ne représentent pas forcément l'essentiel des sommes dérobées (2,2 milliards de dollars en 2021 selon ChainAnalysis). Les protocoles DeFI ayant enregistré le plus d'attaques sont dans l'ordre Ethereum, Binance, Polygon et Avalanche. Ces attaques exploitent souvent le fait que les plates-formes en ligne (cf. les incidents chez Grim Finance, AscendEX, Vulcan Forged, BitMart, Badger, …) n'implémentent pas correctement un contrat intelligent (smart contract en anglais. *Un smart contract est un protocole informatique souvent implémenté grâce à une block chain qui facilite, vérifie et exécute la négociation ou l'exécution d'un contrat*).

En 2021, le plus gros vol a été subi en août par la plate-forme PolyNetwork pour un montant de 600 millions de dollars. Dans ce cas précis, 99% des sommes volées ont été restituées peu après par le hacker, qui voulait surtout dénoncer une vulnérabilité dans un smart contract gérant l'échange de liquidité d'une blockchain à une autre.

Mais il arrive aussi souvent que les vols sur les plates-formes d'échange soient réalisés via une intrusion plus classique. Par exemple, en novembre 2021, un développeur de la plate-forme bZx a été victime d'un e-mail de spear-phishing avec une pièce jointe Word piégée, ce qui a conduit au vol d'un portefeuille de crypto-monnaie et à la perte de 55 millions de dollars pour la société.

Le secteur des plates-formes d'échange / DeFI est finalement sujet aux mêmes problèmes que celui des banques. Il est extrêmement ciblé du fait des opportunités de gains pour les attaquants. Mais les nouvelles technologies qu'elles mettent en œuvre, notamment les codes implémentant les contrats intelligents, devront impérativement faire l'objet d'une attention et d'un investissement tout particulier en termes de sécurité (sécurité du code, cryptographie, protection des données, sensibilisation du personnel …).

3.4.2 Les arnaques

Les arnaques (scams) de toutes sortes auraient représenté un peu plus de la moitié des détournements de crypto-monnaies en 2021 (7,8 milliards de dollars). Parmi ces arnaques celles qui ont le vent en poupe sont surnommées « rug pull », littéralement « tirer le tapis sous les pieds » : Profitant de la crédulité de certains primo-investisseurs, des personnes mal intentionnées posent les jalons d'un projet

de crypto-monnaie bidon, mais suffisamment crédible de prime abord, afin de réunir un « pool » d'investisseurs. Ces projets sont souvent soutenus par une grosse campagne de marketing autour d'influenceurs sur les réseaux sociaux. La peur de passer à côté d'un investissement prometteur attire de plus en plus de personnes, fait monter le prix initial du jeton, générant encore plus d'attente. Une fois suffisamment de fonds rassemblés, les escrocs ferment ou laissent la plate-forme à l'abandon, et disparaissent avec les liquidités. Le cas le plus connu de cette arnaque en 2021 est celui de Thodex, une plate-forme turque d'échange de crypto-monnaie dont le président et fondateur a disparu au mois d'avril après avoir siphonné 2 milliards de dollars.

A court terme, et en l'absence de régulation, seule une sensibilisation massive des utilisateurs pourrait aider à la diminution de ces chiffres. A plus long terme, l'industrie devra peut-être prendre des mesures plus drastiques pour empêcher les jetons associés à des projets potentiellement frauduleux ou dangereux d'être cotés sur les principales bourses (audits systématiques, pentests, …).

3.4.3 Le vol pur et simple auprès des utilisateurs

Beaucoup d'attaques visent plus simplement l'utilisateur final / le petit porteur dans le but de lui dérober son portefeuille de crypto-monnaie, ou de lui faire réaliser des transferts de fonds à son insu. Ces attaques sont menées au moyen de malwares peu sophistiqués, générant pourtant des millions de dollars, et que l'on peut catégoriser comme suit :

- **Les stealers** (exemple : Redline, Cryptbot) : Ces malwares dérobent les portefeuilles de crypto-monnaies eux-mêmes. Ils récupèrent d'un côté les adresses qu'ils trouvent dans le presse-papiers. De l'autre, ils parcourent le système à la recherche des mots de passe associés, ou installent un module de capture des saisies clavier (keylogger) pour récupérer ces mots de passe plus directement.
- **Les clippers** (exemple : Hackboss, MyKings) : Ces malwares remplacent les adresses de portefeuilles de crypto-monnaies qu'ils trouvent dans le presse-papiers par l'adresse d'un portefeuille appartenant au pirate. Les adresses étant de longues suites aléatoires de chiffres et de lettres, la victime peut ne pas s'en rendre compte au moment de transférer des fonds.

3.4.4 Le cryptojacking, toujours une valeur sûre

Le cryptojacking désigne l'attaque qui consiste à utiliser la puissance de calcul d'un système compromis, pour miner des crypto-monnaies (généralement du Monero XMR) et ce, à l'insu du propriétaire de la machine. Il semble difficile d'évaluer les montants générés par cette menace, mais ils représenteraient selon ChainAnalysis les ¾ des montants générés en crypto-monnaie par des malwares, hors ransomware.

Vers 2018, on avait pu constater que le cryptojacking quittait peu à peu le poste de travail de l'utilisateur lambda pour s'orienter vers les serveurs, et donc vers les entreprises. Début 2021, Cisco estimait même dans un rapport que 69% de ses clients avaient été touchés par du cryptojacking en 2020. En 2021, le cryptojacking semble générer toujours plus de profits en compromettant des serveurs au moyen de vulnérabilités connues dans des applicatifs comme Microsoft Exchange (ProxyLogon, ProxyShell), Oracle WebLogic, Atlassian Confluence, ElasticSearch, Docker, … La menace s'industrialise de plus en plus sous la forme de botnets de plusieurs milliers de machines compromises, scannant continuellement Internet à la recherche de nouvelles cibles vulnérables. Les plus actifs d'entre eux en 2021 sont notamment TeamTNT, LemonDuck, Z0Miner, Kinsing, Sysrv, Freakout, Glupteba.

3.5 Les Attaques via la Supply-Chain

3.5.1 Plusieurs types d'attaques

Depuis l'attaque SolarWinds Orion révélée fin 2020, les attaques au travers des fournisseurs (les Supply-chain attacks) sont devenues une préoccupation pour beaucoup d'entreprises.

Il s'agit d'un problème complexe qui regroupe plusieurs catégories d'attaques. Il n'existe pas de définition de ce qui rentre dans le cadre des « Supply chain attacks » (voir notre § 3.5.3 ci-dessous), mais les principales catégories à considérer sont les suivantes :

- 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

Nota : il existe d'autres catégories qui peuvent être rattachées ou non (suivant les points de vue) à ces 3 catégories. Par exemple « l'attaque via un service Cloud » qui peut être considérée comme un cas particulier d'une attaque via un MSP, ou comme une catégorie à part entière.

La catégorie des attaques via un logiciel ou un matériel est celle qui est la plus discutée dans la communauté sécurité. Certains considèrent même qu'il s'agit des seules vraies « Supply-chain attacks », ce qui est un peu réducteur. Nous approfondissons cette catégorie plus loin (au paragraphe 3.6).

3.5.2 Des solutions d'atténuation existent déjà

Voici 2 exemples de mesures permettant de limiter les attaques via les fournisseurs :

- Solution organisationnelle : identifier ses fournisseurs clés, les informer de ses préoccupations par rapport au risque d'une attaque de type « Supply-chain » et leur demander de mettre en place des mesures pour diminuer le risque et l'impact.

  Il s'agit ici d'une approche classique déjà appliquée par beaucoup d'entreprises dans le domaine de la sécurité informatique et qui donne lieu par exemple à l'ajout de clauses contractuelles spécifiques.

- Solution technique : Limiter les accès informatiques accordés aux fournisseurs de type MSP (par exemple pour la télémaintenance), les gérer strictement et les surveiller.

  Ce type de mesure est déjà appliqué largement et s'accompagne souvent d'équipements spécifiques (comme par exemple les « jump host ») facilitant le contrôle des accès externes.

3.5.3 Y a-t-il une définition de « Supply-chain Attack » ?

• Selon le modèle Mitre Att&ck

Dans la matrice Att&ck, Mitre définit 2 techniques distinctes :

- **T1195 - Supply Chain Compromise.**
  Cette technique inclut toutes les attaques visant à piéger un logiciel ou un matériel avant qu'il ne soit réceptionné par la victime. L'interception d'un colis pendant le transport fait partie de cette technique
- **T1199 - Trusted Relationship**
  Cette technique inclut toutes les attaques qui utilisent (à son insu) un accès autorisé accordé à un fournisseur

Du fait de cette distinction, le projet Att&ck semble clairement considérer que seules les attaques T1195 (la 3eme catégorie dans notre analyse du § 3.5.1) sont des attaques via la Supply-chain.

• Selon l'Enisa

L'ENISA a publié en juillet 2021 un rapport (Threat Landscape for Supply Chain Attacks) qui analyse 24 attaques de la Supply-chain. Ces attaques sont très variées, et sont plus larges que la définition de Mitre Att&ck. Dans la taxonomie qu'elle propose l'ENISA considère qu'il y a attaque via la Supply-chain dès qu'une attaque enchaine 2 étapes : une première attaque vise le fournisseur ; puis une seconde exploite l'avantage acquis coté fournisseur pour atteindre la victime finale (qui est un client du fournisseur et qui est le but visé par l'attaque globale).

3.5.4 Une attaque difficile aussi pour les attaquants

Lors de la conférence de sécurité BruCon en septembre 2021, Joe Slowik a présenté un point de vue original en se posant la question : est-ce qu'il est difficile de réaliser une attaque via la supply ?

Dans le cas où l'attaquant n'a pas de cible précise, attaquer via la Supply-chain ne pose pas de difficulté particulière : ce peut être un moyen efficace de toucher un grand nombre de victimes en altérant un seul composant (par exemple une librairie logicielle populaire).

Mais si l'attaquant vise une cible particulière (une victime ou un secteur d'activité), alors mettre au point une attaque via la Supply-chain devient beaucoup plus complexe car il faut contrôler 2 paramètres :

- la largeur de la diffusion de l'attaque : l'attaquant prend-t-il le risque d'une distribution sans limite qui va forcément être détectée par au moins une victime, ou veut-il contrôler la distribution ?
- le niveau de contrôle que l'on garde sur la cible finale : L'attaquant peut-il établir un canal direct de communication avec la cible finale, ou doit-il continuer à passer par le fournisseur pour exercer ce contrôle ? L'attaquant choisit-il un code d'attaque autonome (de type ver) ou piloté ?

Globalement, hormis dans le cas d'une attaque sans cible précise, réaliser une attaque via la Supply-Chain est une tâche complexe et qui n'a d'intérêt pour l'attaquant que si une attaque classique (sans passer par un fournisseur) est trop difficile.

3.6 Codes sources : une nouvelle cible d'attaques

En 2021, on a beaucoup parlé d'attaques via la Supply-chain pour des attaques qui ont visé les environnements de développement et les logiciels développés. Dans ce cas le « Supplier » est le développeur du code source et la victime finale est la société qui utilise le code développé. Nous traitons dans ce paragraphe dédié ce cas particulier d'attaques via la Supply-chain.

3.6.1 Les attaques visant les codes sources

Les attaques visant les codes sources sont un phénomène encore assez discret mais qui a pris de l'importance en 2021 et qui risque de s'amplifier. Il prend 2 formes :

- Le vol de code source,
- L'insertion de code malveillant.

Le vol du code source a été observé dans plusieurs incidents de sécurité. Microsoft et MimeCast ont par exemple indiqué que, lorsqu'ils avaient été touchés en 2020 par l'attaque SolarWinds, l'une des actions des attaquants (supposés Russes) avait été d'accéder au code sources de certains de leurs produits. Nous avons aussi connaissance d'au moins un autre cas non public d'incident similaire (en dehors du contexte SolarWind).

Il s'agit d'une tendance faible (peu discutée) mais à prendre en compte sérieusement, et que l'on peut résumer ainsi : certains pirates sont intéressés à voler le code source des produits, probablement pour y chercher des vulnérabilités, ou peut-être pour évaluer la possibilité d'y insérer du code malveillant.

L'insertion de code malveillant est un phénomène répandu et qui s'est amplifié en 2021 avec des attaques telles que :

- La compromission directe de librairies Open-source (par exemple au moyen d'accès mal protégés ou volés). Ces attaques existent depuis plusieurs années et touchent surtout les espaces de partages de code (Package Repositories) tel que NPM (JavaScript), Maven Central (Java), NuGet Gallery (.Net), RubyGems (Ruby), PyPI (Python) etc…
- Les attaques par **« Dependency Confusion »** (découvertes en février 2021) qui tirent parti des règles de recherche sur les dépendances lors de la génération du logiciel, et utilisent ces règles (souvent mal connues) pour que des librairies malveillantes soient utilisées en priorité à la place de librairies légitimes.

Jusqu'à présent, les attaques de ce type ont surtout été utilisées pour des malversations plutôt banales comme installer un crypto-miner ou voler des identifiants Discord. Mais on a vu aussi des cas où l'attaque cherchait à voler des clés d'accès Amazon AWS. Il est aussi théoriquement possible d'utiliser ces attaques pour déposer une backdoor au sein des entreprises qui utilisent une des librairies open-source piégées.

Techniques d'attaques utilisant la supply-chain logicielle

Extrait d'un article du bulletin mensuel Cert-IST de décembre 2021, et basé sur un rapport du NIST et un rapport de Sonatype.

Liste des techniques citées par le NIST :

- Piégeage via le mécanisme de mise à jour,
- Usurpation de la signature électronique des binaires,
- Compromission de code open-source.

Pour la compromission de code open-source, Sonatype cite les techniques suivantes :

- Attaque par « Dependency Confusion »,
- Typosquatting,
- Injection de code malveillant.

Pour l'injection de code malveillant, Sonatype cite les techniques suivantes :

- Vol d'un compte développeur,
- Publication d'un fork piégé du projet légitime,
- Envoi de contributions piégées,
- Compromission du poste de travail d'un développeur.

3.6.2 Attention aux attaques DevOps et CI/CD

L'évolution des technologies a apporté ces dernières années des avancées significatives dans le monde du développement logiciel avec le DevOps (unification des activités de développement et d'exploitation des applicatifs) et le CI/CD (Continous Integration – Continous Delivery).

Ces approches ont amené des progrès indéniables. Mais en 2021 nous avons noté que **les problèmes de sécurité DevOps et CI/CD deviennent le sujet de nombreuses présentations de conférences**. Cela montre que ces technologies ont atteint une maturité qui amène certains à en chercher les faiblesses. Voici des exemples des avertissements faits par ces chercheurs :

- Attention aux instances fantômes : avec le CI/CD les environnements sont très dynamiques et des instances Docker sont automatiquement lancées après chaque génération applicative réussie. Mais il n'est pas rare que suite à des dysfonctionnements certaines instances Docker ne soient pas correctement terminées et continuent leur vie en fantôme. D'où des préoccupations telles que : Savez-vous exactement quelles instance Docker sont en cours ? Sont-elles toutes légitimes ? Savez-vous identifier une instance pirate qui aurait été ajoutée au milieu des instances légitimes ?
- Attention aux droits accordés aux développeurs : Si le développeur peut changer les règles de génération de l'applicatif alors il peut aussi prendre la main sur l'environnement de production. La séparation des rôles et la revue des changements par des pairs sont des notions de sécurité importantes pour se protéger contre ces attaques internes. Il faut les transposer dans le monde DevOps.
- Savez-vous qui a modifié ce code source ? En cas d'incident de sécurité il sera nécessaire d'investiguer pour identifier à quel moment l'intrusion s'est produite. Pour ce faire, il est sans doute nécessaire de signer numériquement les changements (les commits) sur les codes sources.

Un autre événement marquant de l'année 2021 est **l'attaque Codecov.io**. Codecov.io est une société qui propose des outils d'intégration continue pour la phase de test (déclenchée entre les phases Build et Release du cycle DevOps). Fin janvier 2021 une attaque visant Codecod.io a permis à un pirate de modifier un des outils de Codecov.io (le Bash Uploader), et pendant 2 mois (avant la découverte début avril 2021 de l'attaque) une version modifiée de cet outil a été exécutée par tous les clients de Codecov.io qui utilisaient cet outil. Cela a permis à l'attaquant d'obtenir un accès illégal aux espaces de développement des clients de Codecov.io. Par exemple IBM et Rapid7 ont indiqué avoir été affectés. On se trouve ici dans une attaque en cascade de la Supply-chain :

- L'attaque initiale visait Codecov.io.
- Elle a permis d'attaquer les clients de Codecov.io (par exemple IBM ou Rapid7)
- Et éventuellement de piéger les codes développés par ces clients pour toucher ensuite les clients de ces clients…

3.6.3 Sécuriser les environnements de développement : un chantier de longue haleine

Les attaques visant le code source et la Supply-chain logicielle mettent en évidence la nécessité de renforcer la sécurité des environnements de développement. Cela est d'autant plus vrai que l'on est passé au cours des dernières années d'un modèle traditionnel segmenté (avec une frontière forte entre développement, livraison, et exploitation) à un modèle continu (DevOps) beaucoup plus dynamique et même souvent connecté directement à des services Cloud (SaaS) sur Internet.

Le problème est complexe et a de multiples dimensions :

- Comment gérer les vulnérabilités dans les librairies (les dépendances) utilisées par le projet ?
- Les outils CD/CI utilisés induisent-il des problèmes de sécurité ?
- Comment concilier une approche continue de type DevOps avec un besoin sécurité de séparation de rôles ?

Il est clair qu'il s'agit d'un chantier de longue haleine. Mais les attaques observées en 2021 montrent qu'il est souhaitable d'entamer dès maintenant les réflexions sur ce sujet.

3.7 Multiplication du nombre de vulnérabilités

3.7.1 Stratégie de patch et gestion des urgences

Face à l'augmentation du nombre de vulnérabilités découvertes et donc du nombre de correctifs publiés par les constructeurs, les entreprises sont confrontées à une tâche de plus en plus ardue pour déployer ces correctifs. La plupart des entreprises différencient pour cela 2 processus:

- d'une part le déploiement régulier des correctifs (durant les phases de maintenance programmées),
- d'autre part la gestion des correctifs urgents.

L'augmentation du nombre de vulnérabilités influe surtout (en charge de travail) :

- Sur l'opération de triage qui permet en amont de ces 2 processus de définir quels sont les correctifs urgents.
- Et sur le déploiement de ces correctifs urgents. A l'opposé, l'ajout de correctifs dans la catégorie « correctif régulier » n'a qu'un impact faible puisque ce processus regroupe un ensemble (généralement large) de correctifs.

Le principe général pour définir l'urgence est assez bien établi : une faille est urgente si elle est grave et qu'un programme d'exploit existe. Mais l'évaluation de la gravité est trop souvent influencée par le volume de discussions autour d'une faille.

• <u>Attention à l'emballement médiatique</u>

En 2021, il y a eu plusieurs failles médiatisées (comme PrintNightmare ou SeriousSAM) qui correspondaient à des attaques de type élévation de privilèges : un attaquant ayant déjà obtenu un accès dans l'entreprise peut au moyen de cette faille acquérir des privilèges élevés. Le fait qu'il s'agisse d'une attaque interne (l'attaquant doit avoir déjà un accès dans l'entreprise) diminue le risque d'attaque. L'emballement qu'il y a eu sur ces failles est, il nous semble, plus dû à l'intérêt des chercheurs pour le problème soulevé (avec une succession de correctifs et de contournement des correctifs) que d'une évaluation du risque réel induit.

Pour limiter ces effets d'emballement il est important de définir à l'avance les règles d'urgences qui serviront pour analyser les situations de crise ; par exemple, statuer sur le fait qu'une vulnérabilité de type élévation de privilèges peut (ou non), déclencher un déploiement d'urgence.

• <u>Les constructeurs doivent produire des logiciels plus fiables</u>

Le nombre de correctifs de sécurité publiés chaque année augmente sans cesse. Si l'on ne peut pas se plaindre du fait que des vulnérabilités soient corrigées, on peut par contre parfois s'interroger sur la qualité (la fiabilité) des codes. On sait aussi que lorsqu'une vulnérabilité est corrigée, des chercheurs vont s'intéresser au problème soulevé : soit pour trouver comment contourner la correction, soit pour trouver un problème similaire ailleurs. Il est donc indispensable de redoubler de vigilance lors de la correction d'une vulnérabilité.

Comme la qualité du code est un problème étudié depuis longtemps et qu'il ne semble pas y avoir eu d'amélioration significative sur cet aspect, certaines personnes pensent désormais que seule une obligation légale pourrait faire avancer le sujet.

3.7.2 2021 : Annus Horribilis pour Microsoft ?

Microsoft a été beaucoup mis à l'épreuve en 2021 avec en particulier:

- Les attaques ExchangeProxyLogon (mars 2021) et ProxyShell (août 2021). La vague d'attaques ProxyLogon vue en mars pourrait être due aux détails diffusés par Microsoft vers ses partenaires dans le cadre du programme MAPP.
- PrintNighmare (juillet 2021), avec beaucoup de rebondissements (attente de correctifs, puis correctifs incomplets) et des dysfonctionnements provoqués par les correctifs diffusés par Microsoft.
- PetitPotam et les attaques par Relais NTML. Ce type d'attaques était déjà connu et montre les faiblesses de l'authentification NTLM dans le monde Windows ; il a beaucoup été discuté cette année avec la faille PetitPotam. NTLM est considéré comme obsolète par Microsoft, mais il a encore une empreinte forte dans l'environnement Windows (difficile de s'en passer). Et son successeur (Kerberos) est également connu pour ses faiblesses (attaques Golden Tickets et DCSync).
- OMIGOD : une vulnérabilité critique dans un composant open-source développé par Microsoft (OMI : Open Management Infrastructure) qui est installé automatiquement par Microsoft dans certaines VM Linux déployées dans Azure.

On peut aussi citer aussi d'autres vulnérabilités Microsoft médiatisées cette année, par exemple **SeriousSAM** (une élévation de privilèges via la base de registres Windows). Mais il s'agit d'une vulnérabilité classique qui prise seule n'a pas de caractère particulier.

Enfin, pour le suivi des vulnérabilités (à notre grand regret) Microsoft a changé en 2021, ses bulletins de sécurité qui désormais ne contiennent (le plus souvent) plus aucune description sauf une note CVSS. Après l'abandon des célèbres Microsoft Security Bulletin en 2017 (MS17-023 est de mémoire le dernier et le niveau de détail qui était fourni par ces bulletins a toujours été considéré comme exemplaire), les bulletins Microsoft s'appauvrissent donc encore….

3.8 Log4j : que faut-il en retenir ?

La vulnérabilité Log4j (annoncée en décembre 2021) a entrainé un travail acharné au sein des entreprises afin d'identifier les installations vulnérables et les protéger. Elle constitue l'une des vulnérabilités les plus marquantes de l'année. Après une vague massive d'attaques tous azimuts en décembre (que l'on qualifie classiquement de « Spray and Pray » : arroser au hasard et prier pour que l'attaque marche à quelques endroits), des attaques plus sélectives (visant des applications particulières) vont probablement se poursuivre pendant toute l'année 2022. Ce dossier n'est donc pas clos et l'application des correctifs sur tous les systèmes vulnérables doit être poursuivie.

L'aspect le plus marquant de cette vulnérabilité est qu'elle impacte un grand nombre d'applications et qu'identifier ces applications est un travail complexe. Il serait donc souhaitable de disposer **d'une cartographie logicielle** dans l'entreprise, qui indique pour chaque application quelles sont les composants externes (les librairies) utilisés. Ce principe correspond à la notion de **SBOM (Software Bill of Materials)** que les Etats Unis promeuvent activement :

- Le SBOM est par exemple considéré par la CISA comme un moyen pour lutter contre le phénomène des VBOS (Vulnerability Below the OS : des vulnérabilités dans des composants de bas niveau comme l'UEFI, cf cette présentation à la conférence RSA 2021) ;
- C'est aussi un moyen de remédier plus rapidement aux attaques via la Supply-chain logicielle ;
- Enfin, le SBOM est cité dans un Executive Order en mai 2021 signé par le président des Etats Unis comme un moyen pour améliorer la sécurité. Ce n'est bien sûr pas la seule recommandation de cette publication, puisse qu'on y retrouve aussi des concepts tels que le Zero trust, les EDR, etc.

Bien sûr, ce travail de cartographie est colossal s'il est réalisé à l'échelle d'une entreprise. On sait déjà qu'il est difficile d'identifier toutes les machines et les applications qui sont utilisées dans une organisation (du fait du Shadow-IT et de l'existant). Construire un SBOM est un challenge supplémentaire ! Néanmoins, à la lumière de la crise Log4j et du phénomène de Software Supply-Chain attack, le SBOM semble un chantier indispensable pour les prochaines années. Une première étape peut-être de demander un SBOM pour les nouveaux systèmes mis en production.

3.9 Géopolitique et attaques étatiques

Notre analyse des rapports d'attaques, des alertes gouvernementales, et des indicateurs de compromission rendus publics en 2021 ne montrent pas un changement radical quant aux pays les plus rapportés comme source d'attaque. Sans surprise, c'est la Chine, la Corée du Nord, l'Iran, et la Russie qui font l'objet de l'essentiel des attributions. Par ailleurs, si on oppose souvent par habitude le cybercrime (à but financier) et le cyber-espionnage (traditionnellement associé à l'Etat-nation), on doit aujourd'hui composer avec des menaces étatiques combinant largement ces deux aspects.

Les attaques de 2021 sont également très teintées par la pandémie de Covid-19. En effet, la majorité des pays cyber-offensifs ont soit tenté d'espionner leurs homologues quant à la gestion de cette crise (développement de vaccins, traitements, taux d'infections, …), ou ont simplement utilisé la Covid-19 comme thème dans des campagnes d'hameçonnage. De fait, au-delà des gouvernements, les secteurs pharmaceutiques et médicaux ont été particulièrement ciblés cette année.

3.9.1 La Chine

Acteur le plus actif si l'on s'en réfère au nombre d'attaques rapportées, la Chine a été citée de très nombreuses fois comme source de la menace dans les rapports de CTI ou les conférences en 2021. Sa progression et sa présence sur la scène cyber, y compris sur l'aspect défensif, sont impressionnantes. Fait anecdotique, mais révélateur de cette progression : en 2021, il est devenu indispensable que nous traitions certains rapports d'attaques rédigés en chinois alors que ce n'était que rarement le cas auparavant.

Au-delà de l'aspect purement offensif (l'acteur chinois le plus mentionné dans les rapports OSINT en 2021 est le méta-groupe APT41/Winnti lié au Ministry of State Security), on notera cette progression de la Chine dans l'indépendance qu'elle a acquise vis-à-vis du reste du monde :

- Depuis plusieurs années la Chine a créé son propre catalogue des vulnérabilités (CNVD équivalente à la base NVD des USA).
- En 2018 la Chine a interdit à ses citoyens de participer aux concours internationaux de failles 0-day du type de Pwn2Own et a créé un équivalent chinois : la Tianfu Cup.
- Cette année la Chine a rendu obligatoire pour ses citoyens de déclarer les vulnérabilités 0-day qu'ils découvrent au gouvernement chinois et l'interdiction de les communiquer à d'autres que le constructeur affecté. Cela donne aussi un avantage certain en termes d'attaques au gouvernement Chinois.

3.9.2 La Corée du Nord

Remarquée en 2020 pour ses campagnes surnommées « Dream job », la Corée du Nord est restée active en termes d'ingénierie sociale et de cyber-espionnage en 2021. Ces opérations combinant e-mails piégés et sollicitations via les réseaux sociaux, visent souvent les employés de sociétés technologiques via de prétendues offres d'emploi. En 2021, certaines de ces attaques ont précisément visé des chercheurs en sécurité via de faux profils sur Twitter et Linked-In.

Mais la menace nord-coréenne (la communauté cyber la découpe en deux grands groupes : Lazarus et Kimsuky) est surtout caractéristique du fait des restrictions économiques visant le pays et de sa politique autarcique. 2021 montre encore que le gouvernement du pays multiplie les offensives visant à récupérer des liquidités, au moyen d'attaques ciblées par ransomware, d'extorsions diverses, et de plus

en plus, de vol de crypto-monnaies. Le pays aurait généré 400 millions de dollars en 2021 en seulement 7 attaques réussies contre des plates-formes centralisées d'échange de crypto-devises et des sociétés d'investissement. Cela n'inclut pas le très grand nombre de campagnes que nous avons observées et qui piègent directement le petit porteur, au moyen de fausses applications de crypto-trading. L'ONU a d'ailleurs récemment déclaré dans un rapport que l'argent du cybercrime (près de 2 milliards de dollars par an) était investi dans le développement de l'armement nucléaire et autres technologies militaires de la Corée du Nord.

3.9.3 L'Iran

Connus pour leurs attaques d'ingénierie sociale via les smartphones ou les réseaux sociaux, ainsi que leurs campagnes de phishing visant les universités du monde entier, les acteurs iraniens ont définitivement repris un tournant offensif en 2021. Microsoft note par exemple une nette augmentation des attaques en force brute (scan et exploitation de vulnérabilités de VPN ou de serveurs Exchange, spraying de mots de passe sur Office365), dans le but de déployer des ransomwares ou des malwares destructeurs (cf. les groupes/opérations PAY2KEY, AGRIUS, Black Shadow, N3TW0RM, MosesStaff). Entre espionnage politique, déstabilisation (en Israel surtout), et génération de profits financiers, les groupes / modes opératoires iraniens foisonnent. On peut raisonnablement supposer que les attaques à but lucratif (i.e. Les ransomwares) servent notamment à financer des opérations de cyber-espionnage plus conséquentes (comme cette campagne menée à l'encontre du secteur des télécoms).

Côté cyberdéfensif, nous avons pu constater que le niveau de technicité de certains rapports de sociétés iraniennes spécialisées en cybersécurité (en particulier l'analyse to rootkit iLOBleed visant le mécanisme iLO sur serveur HP) est remarquable, suggérant des investissements croissants sur ce secteur d'activité.

3.9.4 Israel

Pour 2021, l'événement le plus marquant est **l'affaire Pegasus** (logiciel espion en théorie vendu pour lutter contre le terrorisme mais utilisé en fait très largement pour viser des personnes de la société civile et des opposants). Pegasus était connu depuis 2015 avec des usages abusifs dans certains pays (Emirat Arabe Unis, Mexique, Maroc, etc.). Les révélations de l'été 2021 montrent que ces abus sont bien plus larges que ce qui était connu jusque-là.

3.9.5 La Russie

La Russie est un pays très avancé depuis plusieurs années dans les attaques contre les infrastructures critiques (notamment mises en pratique en Ukraine) et dans la manipulation (attaques informationnelles et collusions supposées avec des acteurs cybercriminels russes).

2021 restera une année un peu particulière pendant laquelle beaucoup de rapports ont été publiés pour analyser en détails et tirer des leçons de l'attaque type supply chain menée un peu partout dans le monde via le logiciel Orion de Solarwinds. En effet, les USA ont officiellement attribué l'attaque SolarWinds aux services de renseignement russes, dans le cadre d'une série de sanctions contre le pays annoncée le 15/04/2021.

Un des éléments étonnant pour la seconde moitié de 2021 et que l'on a vu plusieurs cas d'attaques de ransomware visant la Russie, ce qui jusque-là était considéré comme interdit et dangereux pour les groupes de hackers russes.

3.9.6 Les Etats Unis

Il n'y a pas eu en 2021 d'action offensive médiatisée attribuée aux Etats-Unis. On imagine bien qu'il doit y en avoir, mais elles sont restées secrètes jusqu'à présent. L'effort le plus remarquable est sur le plan défensif avec d'une part une **lutte très active contre les groupes de ransomware** et d'autre part des efforts exemplaires pour renforcer la sécurité des infrastructures avec par exemple **le lancement du catalogue KEV** (Known Exploited Vulnerabilities) qui liste les vulnérabilités exploitées que doivent obligatoirement corriger les agences gouvernementales américaines. Le FBI mais aussi le département de la justice communiquent de plus en plus souvent publiquement avec par exemple des alertes sur les menaces en cours, des attributions publiques, et des mises en accusations de hackers chinois, russes ou iraniens.

3.9.7 Et la France ?

La France reste toujours très discrète sur le plan offensif (pas d'attaque connue publiquement depuis Babar et Animal Farm révélés en 2015). On peut noter par contre pour 2021 la création de la L2I (Lutte Informatique d'Influence, qui complète la LID de 2018 et LIO de 2019) et la création de CERT sectoriels: Santé, Maritime, Aviation, Espace, et de CERT régionaux.

4 Productions du Cert-IST en 2021

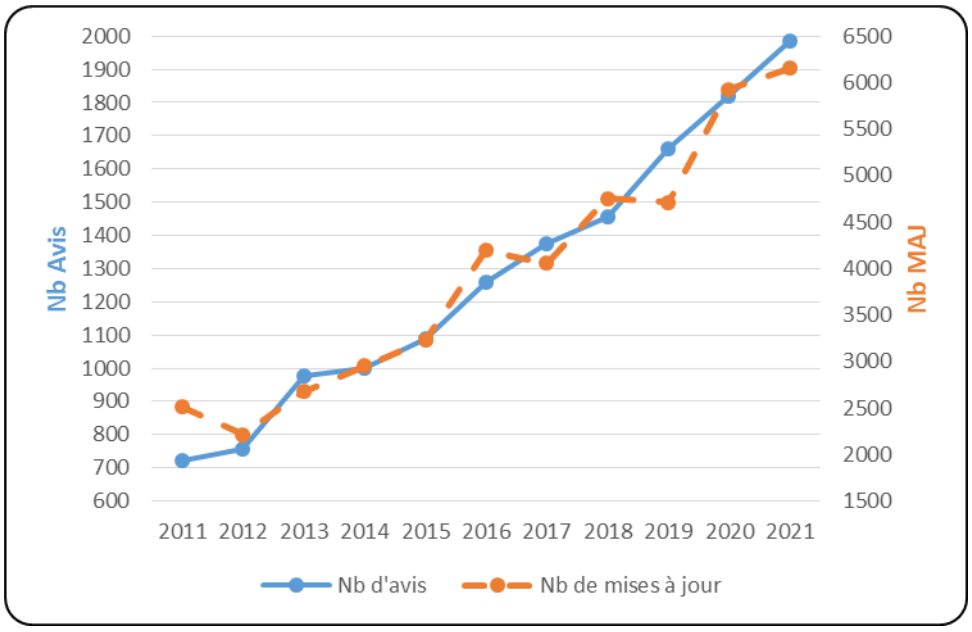
4.1 Veille sur les vulnérabilités et les menaces

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.

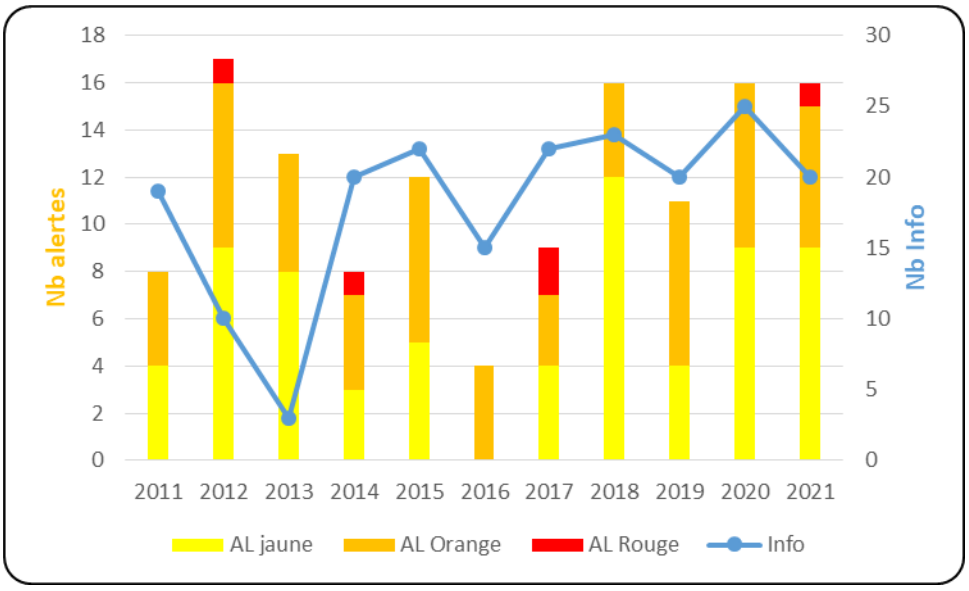
Le Cert-IST émet ainsi plusieurs types de publications :

- **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'attaque 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)** à travers une base de données MISP. Elles répertorient les attaques majeures, qu'il s'agisse de menaces récurrentes (MalSpam, Exploit-Kit, Ransomware), ou de cas de cyber-espionnages (attaques APT).

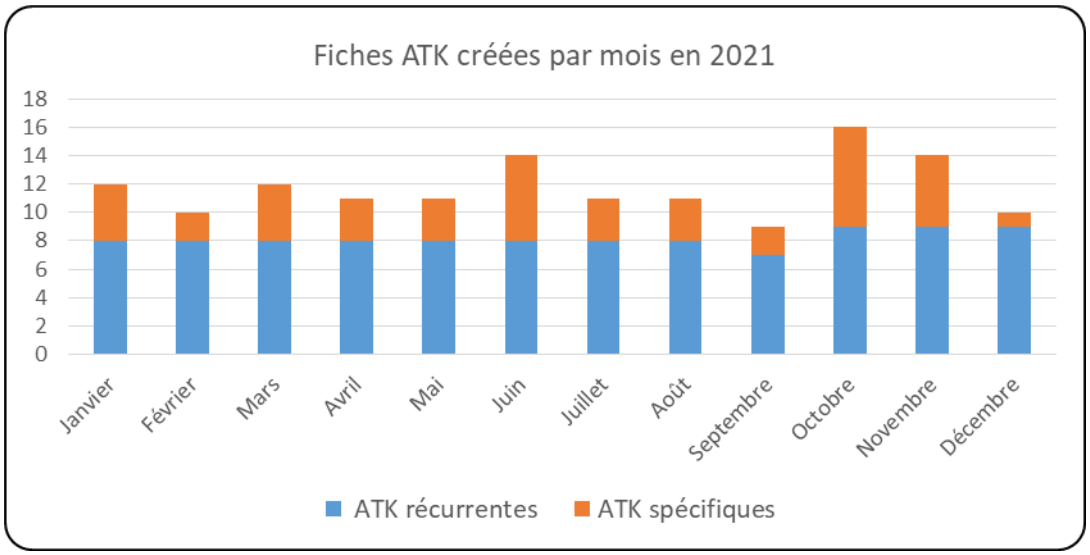
Les graphiques ci-dessous montrent la production du Cert-IST au cours des dernières années.



Nombre d'avis de sécurité publiés par an



Nombre d'alertes publiées par an



Nombre de fiches attaques publiées par mois

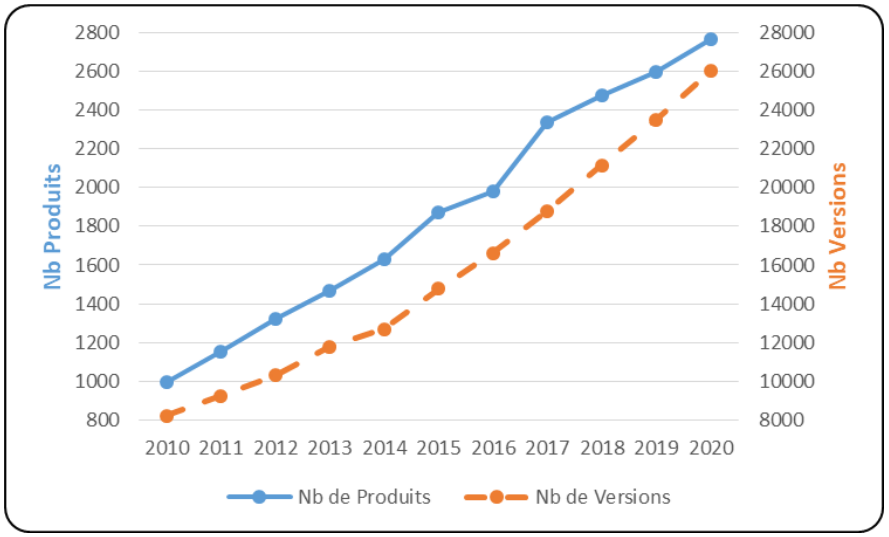
Ainsi, en 2020, le Cert-IST a publié :

- **1 987** avis de sécurité (dont **79** avis SCADA), **5 982** mises à jour mineures et **173** mises à jour majeures.
  Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), avec en 2021 une augmentation de **9%** par rapport à 2020. 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 **20** messages Info. Cette année nous avons émis une alerte rouge pour les attaques Echange ProxyLogon. Les précédentes alertes rouges ont été émises en 2017 (WannaCry et

NotPetya). D'année en année, l'activité dans cette catégorie est très fluctuante et on ne note pas de tendance sur l'évolution globale. Une tendance à la stabilité semble s'installer depuis 2018.

- **140** fiches attaques ont été publiées en 2021, avec dans la base de données MISP **3 453** évènements qui ont été enrichis, et **793 185** marqueurs (IOC) ajoutés (au total il y a **5,5 millions** de marqueurs dans la base).

Concernant les produits et les versions suivis par le Cert-IST, fin 2021 le Cert-IST suivait **2 930** produits et **28 561** 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 contre Exchange (ProxyLogon en mars et ProxyShell en août) sont un des événements majeurs de 2021. Elles confirment deux tendances déjà amorcées les années précédentes :

- les pirates utilisent tous les moyens à leur disposition pour rentrer dans les entreprises. Alors que pendant longtemps les vecteurs privilégiés étaient l'utilisateur (avec des attaques au moyen de mails piégés) et son mot de passe (attaque des mots de passe faibles ou vol au moyen d'un phishing), depuis 2 ans les attaques visant les serveurs se multiplient.
- Les cybercriminels sont autant présents dans ce type d'attaques que les cyber-espions. Le temps où les attaques par infiltration (APT) étaient réservées à ces derniers est maintenant terminé.

Plus généralement, la frontière entre acteurs étatiques et cybercriminels devient plus floue du point de vue des défenseurs :

- Ils utilisent les mêmes outils, par exemple PowerShell et Cobalt-Strike. Les attaquants étatiques disposent bien sûr d'outils spécifiques plus avancés, mais pour toutes les actions ordinaires ils utilisent les mêmes outils que les cybercriminels.
- Certains états (la Corée du Nord et peut-être l'Iran) adoptent parfois un comportement de cybercriminel et mènent des attaques dans le but de générer des revenus financiers.

L'attaque par un ransomware est cette année encore la menace la plus présente et aucune entreprise n'est à l'abri de se trouver attaquée. Si cela n'a pas déjà été fait, il parait souhaitable de se préparer à cette éventualité et d'étudier les différents aspects de ce type de crise (cf. notre § 3.2.2).

De même la sécurité des postes de télétravail est un autre sujet urgent s'il n'a pas déjà été traité. Dans ce domaine il n'y a probablement que deux solutions sûres (en termes de sécurité) : le traditionnel accès full-VPN (par opposition au split-VPN) qui envoie tout le trafic vers l'entreprise, ou une solution de type ZeroTrust qui prend en charge nativement la problématique des utilisateurs nomades.

En 2021 nous avons vu une évolution des attaques visant le Cloud et en particulier Azure et Microsoft 365. Les vulnérabilités dans Azure Cosmos, OMI (vulnérabilité OMIGOD) ou les attaques en force brute des mots de passe Azure, montrent que la recherche de vulnérabilités dans le Cloud est en train de changer, pour s'intéresser à des choses plus techniques que ce que l'on connaissait déjà. On peut s'attendre à que ces vulnérabilités Azure prennent de l'importance dans le futur.

Les attaques via la Supply-chain continuent d'être une préoccupation croissante. Le sujet est complexe parce qu'il recouvre plusieurs catégories d'attaques qu'il faudrait peut-être mieux traiter séparément (cf. notre paragraphe 3.5.1). Il existe déjà des éléments de réponse, plutôt méthodologiques (identifier ses fournisseurs, sensibiliser les parties prenantes, etc.) ou du domaine de la bonne pratique (limiter les accès des tiers). La protection contre les attaques de la Supply-Chain est sans doute un chantier de fond qu'il faut démarrer maintenant.

Enfin, la protection des environnements de développement constitue une nouvelle préoccupation. Ils sont une cible : pour voler le code source, accéder aux données associées ou même pour réaliser une attaque vers un tiers (attaque via la Supply-chain logicielle). L'évolution des méthodes de développement avec l'intégration continue (le CI/CD), le DevOps et le recours à des outils en mode Cloud (Saas) accentuent l'exposition des environnements de développement aux cyber-attaques. La sécurisation de ces environnements est une action de longue durée, mais il est important de prendre conscience dès maintenant de ce problème et de démarrer des actions sur le sujet.

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