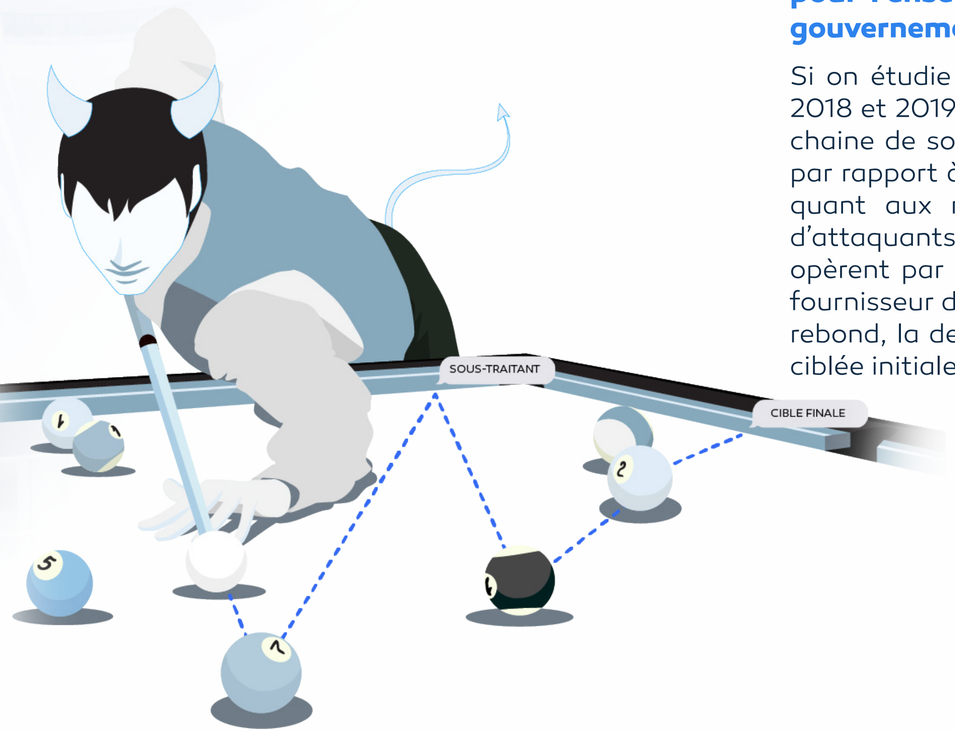
ALSID ACADEMY

Épisode 9

# SUPPLY CHAIN : LA PORTE DÉROBÉE VERS VOTRE AD




**Les cybermenaces liées à la chaine de sous-traitance représentent un nouveau risque majeur pour l'ensemble des organisations commerciales ou gouvernementales.**

Si on étudie les modèles d'attaque utilisés sur les années 2018 et 2019, il s'avère que les cyber-attaques exploitant la chaine de sous-traitance ont doublé pendant l'année 2019 par rapport à l'année 2018. Il s'agit d'une évolution majeure quant aux modes opérationnels des différents groupes d'attaquants : au lieu de viser directement la cible, les hackers opèrent par rebond en infectant sur la première bande un fournisseur direct ou indirect de la cible convoitée - puis, via rebond, la deuxième bande est infectée, à savoir la victime ciblée initialement.

# QUELLES CATÉGORIES D'ATTAQUE SUR LA CHAINE DE SOUS-TRAITANCE ?

## Nous pouvons segmenter les attaques exploitant la chaine de sous-traitance en trois catégories majeures :

1. Attaque programmée classique utilisant le vecteur du sous-traitant comme première étape de la compromission : nous pouvons citer comme exemple l'attaque réalisée sur la société Target via un rebond depuis le système d'information d'un sous-traitant « Fazio Mechanical Services » primo-infecté par un phishing déclenchant l'installation d'un Trojan. Ce sous-traitant opérant des actions de surveillance et de correction sur les systèmes de Target, l'infection s'est rapidement répandue
2. Attaque ciblée via injection de code malveillant : L'attaque ShadowHammer visant les clients de la société ASUS est bon exemple de ce type d'attaque. Les attaquants ont tout d'abord réussi à injecter du code malicieux dans l'utilitaire « ASUS Live Update » - la mise à jour de cet utilitaire depuis les machines des clients ASUS installant par la même occasion une backdoor sur des dizaines de milliers de PCs. Concernant ce type d'attaque, le code est ciblé, l'action est minutieuse
3. Attaque générique via injection de code malveillant : Il s'agit ici d'implémenter un code malicieux mais sans cibler une victime précise, l'objectif étant plus quantitatif que qualitatif. Dans ce cadre, une infection à grande échelle est visée même si la valeur de la cible n'est pas avérée. Nous pouvons citer en exemple l'attaque réalisée sur PrismWeb qui est une plateforme de e-commerce largement utilisée aux USA. Par rebond, les clients de PrismWeb furent infectés via l'usage de codes JavaScript modifiés par les attaquants

## D’un point de vue de l’attaquant, l’usage de la chaine de sous-traitance permet deux avantages importants :

1. L’attaquant pourra utiliser la réputation du sous-traitant et s’appuyer sur son image pour espérer obtenir le plus d’accès possibles via rebond. Nous pouvons conclure que plus la réputation du sous-traitant est « bonne », plus il représente une cible privilégiée comme pivot d’attaque
2. L’attaquant pourra exploiter les mécanismes de distribution techniques du sous-traitant pour diffuser au plus grand nombre ses outils d’intrusion (malware, code malicieux, etc.) de manière silencieuse – par exemple l’attaquant pourra utiliser un outil de gestion des patchs infogéré par le sous-traitant afin de déployer son code à grande échelle

**Face à la multiplication des attaques par rebond exploitant la chaine de sous-traitance, dans le monde entier, les gouvernements mettent alors en œuvre un plan de défense adapté à cette nouvelle menace.**

# UNE PRISE DE CONSCIENCE DES ORGANISATIONS GOUVERNEMENTALES

**Ce nouveau type d'attaque se multipliant de manière exponentielle, la plupart des organisations gouvernementales en charge de la cybersécurité nationale ont créé des contenus spécifiques pour aider leurs organisations vitales respectives.**

Aux USA, le US Department of Homeland Security (DHS) a créé un groupe de travail nommé « Information and Communications Technology (ICT) Supply Chain Risk Management Task Force (SCRM) » dont l'objectif est d'étudier les mécanismes d'attaque via la chaine de sous-traitance et de fournir un recueil éclairé de bonnes pratiques pour les fournisseurs de services. De plus, les entreprises américaines peuvent utiliser ce canevas afin d'évaluer le niveau de fiabilité de leurs différents sous-traitants. Une description des différents travaux est consultable ici.

En France, l'ANSSI travaille depuis quelques mois sur ce sujet et a créé un document décrivant les constats de l'agence pendant ses investigations : **« SUPPLY CHAIN ATTACKS - THREATS TARGETING SERVICE PROVIDERS AND DESIGN OFFICES »** consultable ici. De plus, l'ANSSI propose la mise en œuvre d'un plan d'assurance sécurité (PAS) lors du choix d'un prestataire de sous-traitance. Enfin, un document de référence décrit les différentes démarches à implémenter, il est consultable ici.

Toujours aux USA, le 15 Mai 2019, la Maison Blanche produit un décret stipulant une liste de sous-traitants interdits dans les activités considérées comme d'importance vitale pour le pays. Le Secrétariat au Commerce est responsable de sélectionner ou d'éliminer les différents fournisseurs, notamment étrangers et jugés non conformes aux règles de sécurité édictées. La société Huawei se retrouve alors sur la liste des fournisseurs bannis.

# ILLUSTRATION PAR L'EXEMPLE : RETOUR SUR L'ATTAQUE VISANT UNE GRANDE SOCIÉTÉ DE DISTRIBUTION AMÉRICAINE

## Les éléments présentés dans ce chapitre sont basés sur des faits réels et issus de la collection d'informations de plusieurs études post-mortem

### Séquence de l'attaque et mode opératoire.

- **Phase de reconnaissance :** Les attaquants réalisent des recherches sur Google pour comprendre comment la cible travaille avec ses sous-traitants et afin de recueillir l'identité des sous-traitants. Un sous-traitant responsable du système de climatisation est ciblé.
- **Septembre :** Les attaquants compromettent le sous-traitant via un email contenant un malware. Le malware utilisé serait un dérivé du code Citadel permettant de capturer les mots de passe utilisés sur la machine. Le malware recueille alors un mot de passe permettant de se connecter au portail d'accès des sous-traitants.
- **15 novembre :** Les attaquants infectent le réseau de la cible et testent le mouvement latéral sur les terminaux de paiement. Les attaquants continuent la phase de reconnaissance interne en utilisant des outils relativement basiques : ils comprennent qu'ils peuvent utiliser Active Directory pour réaliser un mouvement latéral et une escalade de grande ampleur.
- **27 novembre :** Les attaquants commencent à collecter des informations sur les cartes de paiement via les malwares installés sur les terminaux de paiement. De plus, les attaquants trouvent un contrôleur de domaine Active Directory non patché et mal configuré permettant d'industrialiser l'infection des terminaux de paiement.
- **30 novembre :** La quasi-totalité des terminaux de paiement sont infectés. Les attaquants utilisent les outils de gestion de patch de la cible elle-même, à savoir SCCM, pour disséminer leur malware à grande échelle. Le malware déployé possède du code personnalisé indétectable par les anti-virus utilisés chez la cible.
- **2 décembre :** Les données collectées sont récupérées depuis la mémoire des machines, ensuite stockées dans un DLL puis transférées sur un partage réseau créé pour l'occasion en utilisant les ports 139, 443 et 80. Les données sont ensuite exfiltrées via FTP. Via des outils de surveillance réseau, le SOC basé en Inde détecte des mouvements suspects, une alerte est remontée mais aucune action n'est prise, les équipes pensent à un faux positif.
- **12 décembre :** Les données volées sont alors en vente sur le Black Market. Le département de la Justice Américaine est notifié de la brèche. La cible déclenche un plan de remédiation mais la plupart des données sont déjà exfiltrées.
- **15 décembre :** En trois jours, la cible a nettoyé la quasi-totalité de ses machines, mais le mal est fait.

**Ce qu'il faut retenir.**

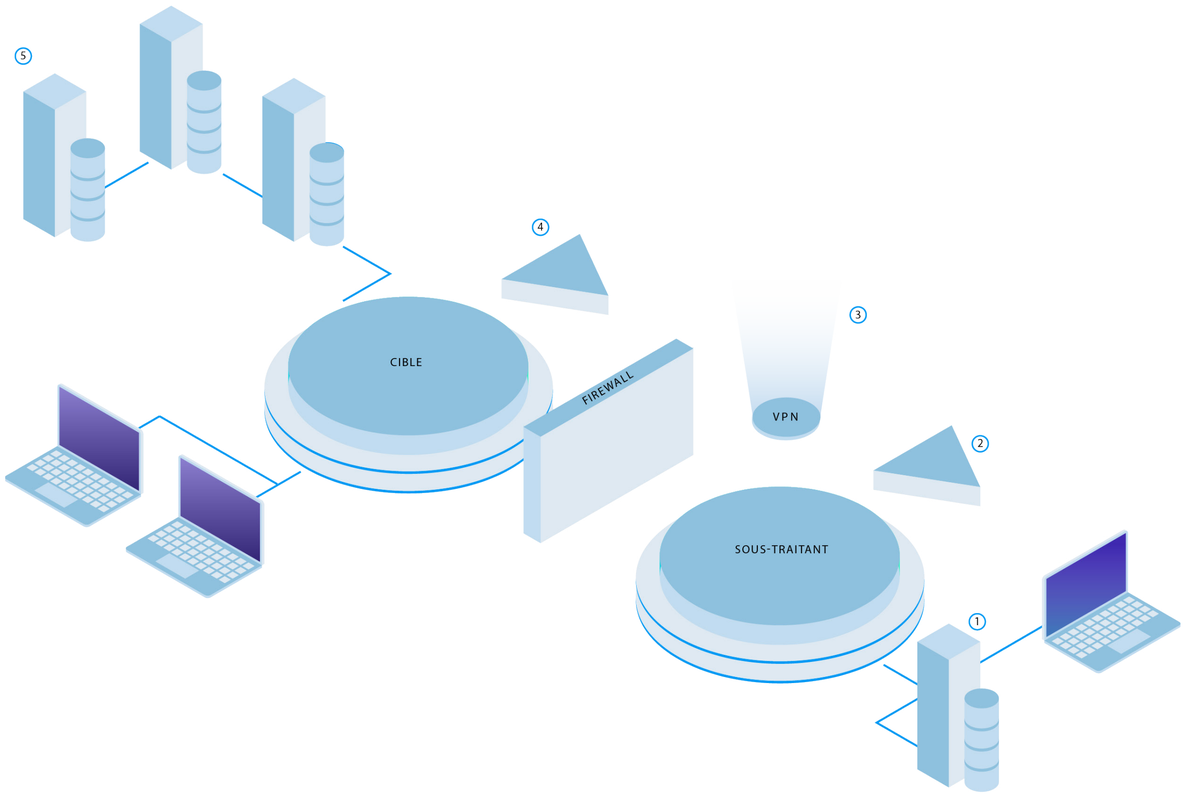
1. De simples recherches Google ont permis de se renseigner sur l'environnement IT de la cible – la phase de reconnaissance fut d'une facilité déconcertante.
2. Le maillon le plus faible n'était pas chez la cible mais chez le sous-traitant. Un sous-traitant dédié à la maintenance des climatisations a permis d'infiltrer le réseau de la cible.
3. Les attaquants ont utilisé Active Directory pour réaliser le mouvement latéral et l'escalade de privilèges afin de réaliser une attaque rapide et de grande ampleur.
4. Les équipes internes ont détecté des mouvements de données suspicieux, mais n'ont pas pris conscience qu'il s'agissait d'une attaque, ils ont pensé à un faux positif.
5. En dehors de la phase de reconnaissance, la phase d'attaque elle-même n'a duré que 4 mois.

**Conclusions pour votre organisation.**

1. Il faut régulièrement réaliser des vérifications sur les moteurs de recherche publics pour évaluer son exposition en termes d'informations IT confidentielles.
2. Il faut mettre en œuvre un plan d'évaluation de vos sous-traitants, dès le démarrage du contrat et sur la durée de celui-ci – il faut compléter ce plan d'évaluation avec des audits réguliers.
3. Active Directory représente un vecteur de dissémination systématique dans plus de 80% des attaques réalisées par un individu mal intentionné ou par un malware automatisé. Il s'agit de s'assurer de la bonne configuration Active Directory au sein de vos organisations afin de contrôler ce risque systémique.
4. Il faut considérer l'ensemble des signaux faibles collectés et former vos équipes SOC en continu sur les nouveaux modèles d'attaque.
5. Selon l'expérience de l'attaquant, les intrusions ciblées peuvent être extrêmement courtes et intenses, quelques mois ou même semaines. Il s'agit de s'assurer en amont que vous possédez bien l'ensemble de l'arsenal de dissuasion, de détection et de réponse.

# QUELS SONT LES POINTS DE CONTRÔLE LES PLUS IMPORTANTS DANS LA CHAINE DE SOUS-TRAITANCE ?

**Le schéma suivant représente une vue simplifiée de la chaine de sous-traitance avec les points de contrôle principaux que vous devez implémenter à minima au sein de votre système d'information étendu :**




- **Point de contrôle numéro 1 :** vous devez accompagner votre sous-traitant en vérifiant comment il stocke les informations nécessaires à la connexion sur votre propre système d'information. En complément, il est nécessaire de contrôler le mode d'accès à cette information.
- **Point de contrôle numéro 2 :** vous devez exiger un audit de la conformité Active Directory de votre sous-traitant, comme nous l'avons évoqué plus haut dans ce document, plus de 80% des attaques utilisent le mouvement latéral et l'élévation de privilèges via une compromission Active Directory.

- **Point de contrôle numéro 3 :** vous devez implémenter une authentification par méthode multiple (MFA) sur le point d'entrée vers votre système d'information – une authentification par simple mot de passe ne suffit pas. De plus il est nécessaire de tracer l'ensemble des informations de connexion via un SIEM par exemple.
- **Point de contrôle numéro 4 :** vous devez mettre en œuvre un plan de surveillance et de remédiation de votre configuration Active Directory. Si malheureusement votre sous-traitant se fait infecter et que la compromission rebondit sur votre propre système d'information, l'infection massive utilisera les faiblesses de configuration et les vulnérabilités de votre Active Directory.
- **Point de contrôle numéro 5 :** vous devez vérifier que votre processus de sauvegarde fonctionne convenablement et que vous êtes capable de restaurer vos données les plus importantes, cela concerne les sauvegardes de votre annuaire Active Directory, les sauvegardes de vos fichiers et de vos bases de données. La vérification de la bonne sauvegarde des emails peut être un plus lors d'un plan de restauration s'ils contiennent des informations stratégiques pour votre activité.

# CONCLUSION

Il est avéré que le niveau de fiabilité d'une chaine de sous-traitance regroupant un ensemble d'organisations est mesuré via son maillon le plus faible. Il convient de mettre en œuvre les mesures nécessaires pour évaluer le niveau de sécurité de l'ensemble des sous-traitants ayant accès à votre système d'information. De plus les modes de connexion et d'accès peuvent grandement varier, via un VPN, avec un PC géré par l'organisation ou non, en utilisant des protocoles divers, etc. Le choix des outils et des protocoles peut s'avérer stratégique pour diminuer le risque global.

Il est donc extrêmement important d'inclure votre chaine de sous-traitance dans vos contrôles de conformité réguliers et d'associer l'ensemble des parties prenantes dans votre stratégie de sécurité. Vous devez considérer vos sous-traitants comme une extension de votre système d'information et devez les traiter comme tels afin de ne pas augmenter mécaniquement votre risque global.

**Comme toujours, il convient de bien évaluer le risque et de mettre en œuvre les mesures adéquates pour se protéger convenablement et finalement résister aux attaques - pour ce, vous pourrez trouver quelques idées supplémentaires sur le site** www.alsid.com