EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RAPPORT DE L'ENISA CONCERNANT LE PAYSAGE DES MENACES DANS LE CADRE DES ATTAQUES DE LA CHAÎNE D'APPROVISIONNEMENT

JUILLET 2021

À PROPOS DE L'ENISA

L'Agence européenne pour la cybersécurité (ENISA) est l'agence de l'Union européenne qui vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis informatiques de demain. Par le partage des connaissances, le renforcement des capacités et des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations sur l'ENISA et ses travaux, consultez le site suivant: www.enisa.europa.eu.

CONTACT

Pour contacter les auteurs, veuillez utiliser l'adresse etl@enisa.europa.eu.
Pour les demandes de renseignements des médias concernant le présent document, veuillez utiliser l'adresse press@enisa.europa.eu.

ÉDITEURS

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agence de l'Union européenne pour la cybersécurité
Sebastian Garcia, Veronica Valeros – Université technique tchèque de Prague

REMERCIEMENTS

Nous tenons à remercier les membres et les observateurs du groupe de travail ad hoc de l'ENISA sur le paysage des cybermenaces pour leurs précieux retours et commentaires dans le cadre de la validation de ce rapport. Nous tenons également à remercier Volker Distelrath (Siemens) et Konstantinos Moulinos (ENISA) pour leurs commentaires.

MENTION LÉGALE

DÉCLARATION CONCERNANT LES DROITS D'AUTEUR

ISBN: 978-92-9204-509-8 – DOI: 10.2824/168593

TABLE DES MATIERES

RÉSUMÉ

Les attaques de la chaîne d'approvisionnement constituent un problème de sécurité depuis de nombreuses années, mais la communauté semble être confrontée à un nombre plus important d'attaques plus organisées depuis le début de l'année 2020. Il se peut que, en raison de la protection plus solide mise en place par les organisations en matière de sécurité, les agresseurs se soient tournés avec succès vers les fournisseurs. Ils ont eu d'importantes répercussions notamment sur les temps d'arrêt des systèmes, les pertes monétaires et les atteintes à la réputation. L'importance des chaînes d'approvisionnement est attribuée au fait que les attaques réussies peuvent toucher un grand nombre de clients qui font appel au fournisseur touché. Par conséquent, les effets en cascade d'une seule attaque peuvent avoir un impact largement répandu.

Le présent rapport vise à cartographier et à étudier les attaques de la chaîne d'approvisionnement qui ont été découvertes entre janvier 2020 et début juillet 2021. Sur la base des tendances et des modèles observés, les attaques de la chaîne d'approvisionnement ont augmenté en nombre et en sophistication en 2020 et cette tendance se poursuit en 2021, ce qui représente un risque croissant pour les organisations. Selon les estimations, il y aura quatre fois plus d'attaques dans la chaîne d'approvisionnement en 2021 qu'en 2020. La moitié des attaques étant attribuées à des acteurs de la menace persistante avancée (Advanced Persistence Threat, ou APT), leur complexité et leurs ressources dépassent largement les attaques non ciblées les plus courantes et, par conséquent, il est de plus en plus nécessaire de mettre en place de nouvelles méthodes de protection intégrant les fournisseurs afin de garantir la sécurité des organisations.

Le présent rapport présente le paysage des menaces de l'Agence concernant les attaques liées à la chaîne d'approvisionnement, produit avec le soutien du groupe de travail ad hoc sur le paysage des cybermenaces[1].

Les principaux aspects du rapport sont les suivants:

- Une **taxinomie** pour classer les attaques liées à la chaîne d'approvisionnement afin de mieux les analyser de manière systématique et de comprendre la manière dont elles surviennent.
- **24 attaques de la chaîne d'approvisionnement** ont été signalées entre janvier 2020 et début juillet 2021 et ont été étudiées dans le présent rapport.
- Environ **50 % des attaques ont été attribuées à des groupes APT connus** de la communauté de la sécurité.
- Environ **42 % des attaques analysées** n'ont **pas encore été attribuées à un groupe particulier**.
- Environ **62 % des attaques contre des clients** ont profité de leur **confiance dans leur fournisseur**.
- Dans **62 % des cas**, **les logiciels malveillants ont été la technique d'attaque** utilisée.
- Lors de l'examen des actifs ciblés, dans **66 % des incidents**, les pirates se sont **concentrés sur le code des fournisseurs** afin de compromettre davantage les clients ciblés.
- Environ **58 % des attaques de la chaîne d'approvisionnement visaient** à obtenir l'accès aux **données** (principalement les données relatives aux clients, y compris les données à caractère personnel et la propriété intellectuelle) et environ **16 %** à accéder à des **personnes**.
- **Toutes les attaques ne sont pas à considérer comme des attaques de la chaîne d'approvisionnement**, mais, en raison de leur nature, bon nombre d'entre elles sont des vecteurs potentiels de nouvelles attaques de la chaîne d'approvisionnement à l'avenir.
- **Les organisations doivent mettre à jour leur méthodologie de cybersécurité en tenant compte des attaques liées à la chaîne d'approvisionnement** et associer tous leurs fournisseurs à leur protection et à leur vérification de sécurité.

[1] Voir https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

1. INTRODUCTION

Les attaques de la chaîne d'approvisionnement constituent un problème de sécurité depuis de nombreuses années, mais la communauté semble être confrontée à un nombre plus important d'attaques plus organisées depuis 2020. Il se peut que, en raison de la protection plus solide mise en place par les organisations en matière de sécurité, les agresseurs se soient tournés vers les fournisseurs et soient parvenus à avoir un impact significatif notamment sur les temps d'arrêt des systèmes, les pertes monétaires et les atteintes à la réputation. Le présent rapport vise à cartographier et à étudier les attaques de la chaîne d'approvisionnement qui ont été découvertes entre janvier 2020 et début juillet 2021.

L'attaque de SolarWinds[2] a mis en lumière les effets dévastateurs et les répercussions des attaques de la chaîne d'approvisionnement. SolarWinds est considéré comme l'une des plus grandes attaques de la chaîne d'approvisionnement de ces dernières années, compte tenu en particulier des entités touchées qui comprenaient des organisations gouvernementales et de grandes entreprises. Elle a fait l'objet d'une grande attention médiatique et a débouché sur des initiatives politiques dans le monde entier[3]. Plus récemment, en juillet 2021, l'attaque de Kaseya[4] a souligné la nécessité d'accorder une attention accrue et particulière aux attaques de la chaîne d'approvisionnement qui touchent des prestataires de services gérés. Malheureusement, ces deux exemples ne sont pas des cas isolés et le nombre d'attaques de la chaîne d'approvisionnement n'a cessé d'augmenter au cours de l'année écoulée. Cette tendance souligne en outre la nécessité pour les décideurs politiques et la communauté de la sécurité de concevoir et d'introduire de nouvelles mesures de protection pour faire face à d'éventuelles attaques de la chaîne d'approvisionnement à l'avenir et en atténuer les effets.

Au moyen d'une enquête et d'une analyse minutieuses, le présent rapport répertorie les attaques de la chaîne d'approvisionnement sur la base des incidents recensés entre janvier 2020 et début juillet 2021. Chaque incident a été décomposé en ses principaux éléments, tels que les techniques d'attaque ainsi que les actifs des fournisseurs et des clients touchés par les pirates. L'introduction d'une taxinomie pour les attaques de la chaîne d'approvisionnement facilitera leur classification et pourrait constituer le point de départ d'une approche plus structurée dans l'analyse de ces attaques et la mise en place de contrôles de sécurité spécifiques visant à les atténuer. La taxinomie proposée permet également de classer, de comparer et d'examiner ces attaques sur une base commune. Les similitudes entre la taxinomie proposée et d'autres cadres bien connus sont évoquées.

Le présent rapport analyse également les similitudes entre le cycle de vie des attaques liées à la chaîne d'approvisionnement et celui des attaques plus connues de menaces persistantes avancées (APT). Un résumé des incidents les plus importants de la chaîne d'approvisionnement depuis 2020 figure en annexe, chacun d'entre eux ayant été décomposé conformément à la taxinomie susmentionnée.

Le cœur du rapport est une analyse de tous les incidents de la chaîne d'approvisionnement signalés afin d'identifier leurs principales caractéristiques et techniques. L'analyse entend répondre aux questions suivantes: quelles sont les techniques les plus couramment utilisées dans les attaques de la chaîne d'approvisionnement, quels sont les principaux actifs des clients touchés par les pirates, et quelle est la relation entre les attaques et les actifs visés?

Avec l'attention croissante portée aux attaques de la chaîne d'approvisionnement, de nombreux autres incidents de sécurité ont également été mis en évidence comme étant liés à la chaîne d'approvisionnement, à savoir qu'ils étaient considérés comme des attaques de la chaîne d'approvisionnement. Nous évoquons donc ce qui constitue une attaque liée à la chaîne d'approvisionnement et la raison pour laquelle de nombreuses attaques ne sont pas vraiment des attaques de la chaîne d'approvisionnement, en citant certains cas à titre d'exemple. Il est important de

[2] Russian SolarWinds hackers launch email attack on government agencies, The Guardian. https://www.theguardian.com/technology/2021/may/28/russian-solarwinds-hackers-launch-assault-government-agencies. Accessed on 08/07/2021.
[3] Voir https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html
[4] Ransomware Attack Affecting Likely Thousands of Targets Drags On, WSJ, https://www.wsj.com/articles/ransomware-group-behind-meat-supply-attack-threatens-hundreds-of-new-targets-11625285071. Consulté le 09/07/2021.

comprendre le paysage des menaces liées aux attaques de la chaîne d'approvisionnement, étant donné qu'une classification erronée des incidents pourrait conduire à une analyse des tendances et à des conclusions erronées.

Le rapport comprend également une série de recommandations destinées aux décideurs politiques et aux organisations, en particulier les fournisseurs, dont l'adoption est susceptible d'accroître la sécurité globale contre les attaques de la chaîne d'approvisionnement.

Le rapport est structuré de la manière suivante:

- **Le chapitre 1** présente brièvement le thème de la chaîne d'approvisionnement et le paysage des menaces de l'ENISA consacré à ce sujet.
- **Le chapitre 2** examine ce qui constitue une attaque de la chaîne d'approvisionnement et introduit une taxinomie structurée pour classer les incidents pertinents qui se rapportent également à des cadres bien établis de renseignement sur les cybermenaces.
- **Le chapitre 3** donne une vue d'ensemble du cycle de vie d'une attaque typique de la chaîne d'approvisionnement.
- **Le chapitre 4** détaille les principales attaques de la chaîne d'approvisionnement qui ont eu lieu à la fin de 2020 et au début de 2021.
- **Le chapitre 5** donne un calendrier des incidents concernés et fournit une analyse approfondie de ces incidents.
- **Le chapitre 6** traite de la question de la classification erronée d'incidents comme des attaques de la chaîne d'approvisionnement.
- **Le chapitre 7** présente des recommandations de haut niveau ainsi que des recommandations techniques visant à améliorer la sécurité de la chaîne d'approvisionnement et à atténuer les conséquences des attaques de la chaîne d'approvisionnement.
- **L'annexe A** résume 24 incidents de la chaîne d'approvisionnement recensés et analysés dans le présent rapport.

2. QU'EST-CE QU'UNE ATTAQUE DE LA CHAINE D'APPROVISIONNEMENT?

La chaîne d'approvisionnement **désigne l'écosystème des processus, des personnes, des organisations et des distributeurs participant à la création et à la fourniture d'une solution ou d'un produit final**[5]. Dans le domaine de la cybersécurité, la chaîne d'approvisionnement comprend un large éventail de ressources (matériel et logiciel), de stockage (en nuage ou local), de mécanismes de distribution (applications web, magasins en ligne) et de logiciels de gestion.

Il existe quatre éléments clés dans une chaîne d'approvisionnement:

- *Fournisseur*: entité qui fournit un produit ou un service à une autre entité.
- *Actifs du fournisseur*: éléments de valeur utilisés par le fournisseur pour concevoir le produit ou le service.
- *Client*: entité qui consomme le produit ou le service proposé par le fournisseur.
- *Actifs du client*: éléments de valeur appartenant à la cible.

Une entité peut être une personne physique, un groupe de personnes ou une organisation. Les actifs peuvent être des personnes, des logiciels, des documents, des finances, du matériel informatique ou autres.

Une attaque de la chaîne d'approvisionnement est une combinaison d'au moins deux attaques. La première attaque cible un fournisseur, qui est ensuite utilisé pour attaquer la cible afin d'accéder à ses actifs. L'objectif peut être le client final ou un autre fournisseur. Par conséquent, pour qu'une attaque soit qualifiée d'attaque de la chaîne d'approvisionnement, il faut que les cibles soient à la fois le fournisseur et le client.

2.1. TAXINOMIE DES ATTAQUES DE LA CHAINE D'APPROVISIONNEMENT

Le présent rapport propose une taxinomie pour caractériser les attaques de la chaîne d'approvisionnement et structurer leur analyse ultérieure. Cette taxinomie tient compte des quatre éléments clés d'une chaîne d'approvisionnement, ainsi que des techniques utilisées par les pirates. La taxinomie peut aider les organisations à comprendre les différentes parties d'une attaque liée à la chaîne d'approvisionnement, en les comparant à d'autres cyberattaques similaires et, plus important encore, à identifier les incidents comme étant des attaques de la chaîne d'approvisionnement.

La taxinomie devrait servir de modèle de référence dans lequel, en cas de nouvelle attaque potentielle de la chaîne d'approvisionnement, la communauté pourrait tenter d'effectuer une analyse en identifiant et en cartographiant chacun des quatre éléments de taxinomie distincts. Si aucun client ou aucun fournisseur n'est attaqué, il ne s'agit probablement pas d'une attaque de la chaîne d'approvisionnement[6].

La taxinomie, telle que présentée dans le tableau 1, comporte une section pour le fournisseur et une section pour le client. Pour le fournisseur, la première partie se nomme «Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement» et identifie **la manière** dont le fournisseur a été attaqué. La deuxième partie concernant le fournisseur se nomme «Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement» et identifie **la cible** de l'attaque contre le fournisseur.

[5] Beamon, B. M. (1998). Supply chain design and analysis: Models and methods. International journal of production economics, 55(3), 281-294.
[6] Pour plus d'exemples, voir la section «Toutes les attaques ne sont pas forcément des attaques de la chaîne d'approvisionnement».

Pour le client, la première partie se nomme «Techniques d'attaque utilisées pour compromettre le client» et identifie **la manière** dont le client a été attaqué. La deuxième partie concernant le client se nomme «Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement» et identifie **la cible** de l'attaque contre le client.

Pour chacun de ces quatre éléments distinctifs de la taxinomie, nous avons défini les éléments qui caractérisent au mieux une attaque de la chaîne d'approvisionnement. En sélectionnant les éléments correspondants, il est possible de mieux comprendre les aspects connus et inconnus d'une attaque. La taxinomie est conceptuellement différente de la base de connaissances MITRE ATT&CK® et ne vise pas à remplacer cette dernière mais à la compléter. Les techniques d'attaque définies dans la taxinomie proposée et illustrées dans le tableau 1 sont parfois liées aux techniques d'attaque pertinentes identifiées dans le cadre MITRE ATT&CK®, et sont indiquées en conséquence par l'identifiant MITRE ATT&CK® entre crochets, par exemple [T1189]. Les sous-sections suivantes précisent chacune des quatre parties de la taxinomie et comment identifier ses éléments.

Tableau 1: Taxinomie proposée pour les attaques de la chaîne d'approvisionnement. Elle se compose de quatre parties: (i) techniques d'attaque utilisées contre le fournisseur, (ii) actifs du fournisseur ciblés, (iii) techniques d'attaque utilisées contre le client, (iii) actifs du client ciblés.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Infection par logiciel malveillant	Logiciels préexistants	Relation de confiance [T1199]	Données
Ingénierie sociale	Bibliothèques logicielles	Compromission «drive-by» [T1189]	Données à caractère personnel
Attaque par force brute	Code	Hameçonnage [T1566]	Propriété intellectuelle
Exploitation d'une vulnérabilité de logiciel	Configurations	Infection par logiciel malveillant	Logiciel
Exploitation d'une vulnérabilité de la configuration	Données	Attaque ou modification physique	Processus
Renseignement de sources ouvertes (OSINT)	Processus	Contrefaçon	Bande passante
	Matériel		Finances
	Personnes		Personnes
	Fournisseur		

Une taxinomie des incidents de cybersécurité de l'UE[7] est utilisée aux fins des actions concertées de réaction aux incidents et de partage d'informations à l'échelle de l'Union. Étant donné que la taxinomie est conceptuellement différente et ne permet pas une analyse détaillée des incidents de la chaîne d'approvisionnement, nous recommandons l'utilisation complémentaire des deux taxinomies.

[7] Cybersecurity incident taxonomy, Publications du NIS Cooperation Group, juillet 2018. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group. Consulté le 28/07/2021.

2.2. TECHNIQUES D'ATTAQUE UTILISEES POUR COMPROMETTRE UNE CHAINE D'APPROVISIONNEMENT

Les techniques d'attaque font référence à «la manière» dont l'attaque a eu lieu, et non à «ce qui a été utilisé» pour attaquer. Par exemple, cette catégorie distingue les situations dans lesquelles le fournisseur a été attaqué à l'aide d'un mot de passe trouvé en ligne (OSINT) ou lorsque son mot de passe a été forcé (attaque par force brute). Toutefois, pour la taxinomie, il n'est pas pertinent de savoir si le mot de passe trouvé en ligne a été divulgué, s'il s'agit d'un mot de passe par défaut ou s'il a été vendu sur un marché noir. Les catégories de techniques d'attaque ci-dessous couvrent les techniques les plus couramment utilisées dans les attaques de la chaîne d'approvisionnement analysées dans le présent rapport. Il est évident que plusieurs techniques peuvent avoir été utilisées dans une attaque donnée et que, dans plusieurs cas, les entités peuvent ne pas avoir connaissance de la manière dont les pirates ont eu accès à leur infrastructure, ou que ces informations n'ont pas été divulguées ou dûment signalées.

Tableau 2: Techniques d'attaque utilisées pour compromettre le fournisseur de la chaîne. Chaque technique permet de déterminer comment l'attaque s'est produite, et non ce qui a été attaqué. Plusieurs techniques peuvent être utilisées dans le cadre d'une même attaque.

TECHNIQUES D'ATTAQUE UTILISÉES POUR COMPROMETTRE UNE CHAÎNE D'APPROVISIONNEMENT	
Infection par logiciel malveillant	par exemple, logiciels espions utilisés pour voler les identifiants des employés.
Ingénierie sociale	par exemple, hameçonnage, fausses applications, typosquattage, fausse identité du Wi-Fi, duperie du fournisseur.
Attaque par force brute	par exemple, piratage d'un mot de passe SSH, piratage d'un login web.
Exploitation d'une vulnérabilité de logiciel	par exemple, injection SQL ou exploitation du débordement de la mémoire tampon dans une application.
Exploitation d'une vulnérabilité de la configuration	par exemple, exploitation d'un problème de configuration.
Attaque ou modification physique	par exemple, modification du matériel, intrusion physique.
Renseignement de sources ouvertes (OSINT)	par exemple, recherche en ligne d'identifiants, de clés API, de noms d'utilisateur.
Contrefaçon	par exemple, imitation d'USB à des fins malveillantes.

2.3. ACTIFS DES FOURNISSEURS CIBLES PAR UNE ATTAQUE DE LA CHAINE D'APPROVISIONNEMENT

Les actifs du fournisseur visés par les agresseurs font référence à la «cible» de l'attaque contre le fournisseur, ayant permis de monter d'autres attaques par la suite. Le ou les actifs visés ont généralement un lien direct avec la cible finale, et il est généralement possible de comprendre les intentions finales du pirate en analysant la liste des actifs visés. Dans certains cas, en raison d'un manque d'informations divulguées ou signalées par le fournisseur, il n'est pas

possible de disposer d'informations sur les actifs ciblés. Cela peut également être le cas lorsque les fournisseurs ne disposent pas des connaissances ou de l'expertise nécessaires pour déterminer quels actifs ont été compromis par les pirates.

Tableau 3: Actifs du fournisseur visés par les pirates. Chaque élément identifie la cible attaquée chez le fournisseur. Plusieurs techniques susceptibles d'affecter plusieurs actifs peuvent être utilisées dans le cadre d'une même attaque.

ACTIFS DES FOURNISSEURS CIBLÉS PAR UNE ATTAQUE DE LA CHAÎNE D'APPROVISIONNEMENT	
Logiciels préexistants	par exemple, logiciels utilisés par le fournisseur, serveurs web, applications, bases de données, systèmes de contrôle, applications cloud, micrologiciels. Ne comprend pas les bibliothèques logicielles.
Bibliothèques logicielles	par exemple, bibliothèques tierces, progiciels installés à partir de tiers tels que NPM, ruby, etc.
Code	par exemple, code source ou logiciel produit par le fournisseur.
Configurations	par exemple mots de passe, clés API, règles pare-feu, URL.
Données	par exemple, informations sur le fournisseur, valeurs obtenues à partir de capteurs, certificats, données à caractère personnel des clients ou des fournisseurs eux-mêmes, autres données à caractère personnel.
Processus	par exemple, mises à jour, procédures de sauvegarde ou de validation, procédures de signature des certificats.
Matériel	par exemple, matériel produit par le fournisseur, puces, soupapes, USB.
Personnes	par exemple, personnes ciblées ayant accès aux données, aux infrastructures ou à d'autres personnes.

2.4. TECHNIQUES D'ATTAQUE UTILISEES POUR COMPROMETTRE UN CLIENT

Cet élément de la taxinomie fait référence aux techniques d'attaque utilisées pour compromettre le client par l'intermédiaire de son fournisseur. Dans cet élément de la taxinomie, nous identifions «la manière» dont le client a été attaqué et non «ce qui a été utilisé» pour l'attaque. Il s'agit d'une technique et non d'un type spécifique d'attaque. Par exemple, si le client met à jour son logiciel auprès du fournisseur et reçoit un type de logiciel malveillant, l'attaque appartient à la fois au type «relation de confiance» et «infection par logiciel malveillant». Il est évident que plusieurs techniques peuvent être appliquées dans plusieurs cas. Il se peut que les clients n'aient pas toujours connaissance de la technique utilisée par les pirates pour accéder à leurs actifs par l'intermédiaire de leurs fournisseurs, mais qu'ils aient les moyens d'identifier que la technique utilisée ne se trouvait pas dans leur périmètre.

Tableau 4: Techniques d'attaque utilisées pour compromettre le client. Chaque technique permet de déterminer comment l'attaque s'est produite, et non ce qui a été attaqué. Plusieurs techniques peuvent être utilisées dans le cadre d'une même attaque.

TECHNIQUES D'ATTAQUE UTILISÉES POUR COMPROMETTRE UN CLIENT	
Relation de confiance [T1199]	par exemple, confiance dans un certificat, confiance dans une mise à jour automatique, confiance dans une sauvegarde automatique.
Compromission «drive-by» [T1189]	par exemple, scripts malveillants sur un site web visant à infecter les utilisateurs avec des logiciels malveillants.
Hameçonnage [T1566]	par exemple, faux messages du fournisseur, fausses notifications de mise à jour.
Infection par logiciel malveillant	par exemple, cheval de Troie d'accès à distance (RAT), porte dérobée, rançongiciel.
Attaque ou modification physique	par exemple, modification du matériel, intrusion physique.
Contrefaçon	par exemple, création d'un faux USB, modification d'une carte mère, fausse identité du personnel du fournisseur.

2.5. ACTIFS DES CLIENTS CIBLES PAR UNE ATTAQUE DE LA CHAINE D'APPROVISIONNEMENT

Les actifs des clients sont la cible principale et finale des agresseurs et, généralement, la raison d'être d'une attaque de la chaîne d'approvisionnement. Ces actifs peuvent varier en fonction du secteur industriel et du type de service offert. Cet élément particulier de la taxinomie vise à faciliter la compréhension de l'impact de l'attaque et à permettre des comparaisons concernant les objectifs des pirates. Certains actifs peuvent avoir été directement visés par les pirates, tandis que d'autres peuvent avoir été affectés par inadvertance. Plus d'un client est généralement touché par des attaques typiques de la chaîne d'approvisionnement. Il est possible que le client n'ait pas connaissance de la cible du pirate (par exemple lorsque l'attaque a échoué ou a été rapidement détectée).

Tableau 5: Actifs du client visés par les pirates. Chaque élément identifie la cible attaquée chez le client. Plusieurs techniques peuvent être utilisées dans le cadre d'une même attaque. Il s'agit généralement de la cible finale de l'attaque.

ACTIFS DES CLIENTS CIBLÉS PAR UNE ATTAQUE DE LA CHAÎNE D'APPROVISIONNEMENT	
Données	par exemple, données de paiement, flux vidéo, documents, courriels, plans de vol, données relatives aux ventes et données financières, propriété intellectuelle.
Données à caractère personnel	par exemple, données relatives aux clients, registres des employés, identifiants.
Logiciel	par exemple, accès au code source du produit client, modification du logiciel du client.

Processus	par exemple, documentation des processus internes de fonctionnement et des configurations, insertion de nouveaux processus malveillants, documents de schématique.
Bande passante	par exemple, utilisation de la bande passante pour le déni de service distribué (DDoS), envoi de SPAM ou infection d'autres personnes à grande échelle.
Finances	par exemple, vol de cryptomonnaies, piratage de comptes bancaires, virements monétaires.
Personnes	par exemple, personnes ciblées en raison de leur position ou de leurs connaissances.

2.6. COMMENT UTILISER LA TAXINOMIE

Voici un exemple de la manière dont l'application de la taxinomie à un cas réel peut aider à identifier ses caractéristiques particulières et à faciliter la compréhension des caractéristiques de l'attaque.

Codecov est une société qui propose des logiciels de couverture de codes et d'outils de test. La société fournit des outils à d'autres sociétés telles qu'IBM et Hewlett Packard Enterprise. En avril 2021, Codecov a indiqué que des pirates avaient obtenu une partie de ses identifiants valides à partir d'une image Docker[8] en raison d'une erreur de création de ces images Docker. Une fois que les auteurs des attaques ont obtenu ces identifiants, ils les ont utilisés pour compromettre un «chargement de script bash» utilisé par les clients de Codecov[9]. Lorsque les clients ont téléchargé et exécuté ce script, les pirates ont été en mesure d'extraire des données des clients de Codecov, y compris des informations sensibles qui leur permettraient d'accéder aux ressources des clients[10]. Plusieurs clients de Codecov ont indiqué que les pirates avaient pu accéder à leur code source en utilisant des informations volées provenant de cette attaque sur Codecov[11]. L'attaque n'a pas été attribuée à des pirates spécifiques. La figure 1 (ci-dessous) décrit les étapes de cette attaque.

Sur la base de ces informations, nous pouvons identifier les quatre éléments de la taxinomie proposée. L'attaque contre le fournisseur correspond à la manière dont les pirates ont eu accès au fournisseur et, dans ce cas, il s'est agi d'une attaque de type «exploitation d'une vulnérabilité de la configuration». Grâce à cette attaque, les pirates ont ciblé l'actif «code» du fournisseur. Une fois les éléments concernant le fournisseur identifiés dans la taxinomie, nous pouvons passer à la manière dont le client a été attaqué. Dans l'affaire Codecov, il s'agit d'une «relation de confiance» avec le fournisseur qui n'a pas été garantie ni vérifiée. Il a été indiqué que l'actif final visé par le client était le code source, donc l'actif «logiciel».

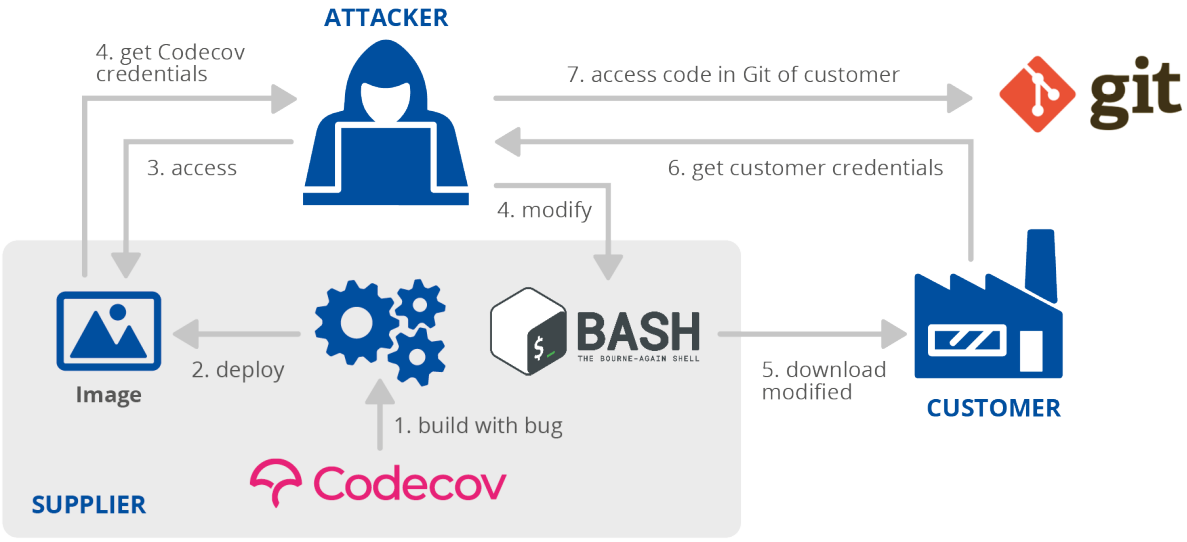
Tableau 6: Taxinomie d'attaque de la chaîne d'approvisionnement appliquée à l'attaque impliquant la société Codecov. Les pirates ont exploité une vulnérabilité de la configuration de Codecov, qui a ensuite été utilisée pour modifier le code du fournisseur. Les pirates ont abusé de la relation de confiance entre Codecov et ses clients afin d'extraire les données nécessaires pour accéder au code source du logiciel du client.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour	Actifs du fournisseur ciblés par l'attaque de la	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement

[8] Codecov supply chain attack breakdown, GitGuardian, https://blog.gitguardian.com/codecov-supply-chain-breach/. Consulté le 27/06/2021.
[9] Bash Uploader Security Update, Codecov, https://about.codecov.io/security-update/. Consulté le 27/06/2021.
[10] Codecov hackers gained access to Monday.com source code, Bleeping Computer. https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/. Consulté le 27/06/2021.
[11] Rapid7 Source Code Breached in Codecov Supply-Chain Attack, The Hacker News, https://thehackernews.com/2021/05/rapid7-source-code-breached-in-codecov.html. Consulté le 27/06/2021.

compromettre la chaîne d'approvisionnement	chaîne d'approvisionnement		
Exploitation d'une vulnérabilité de la configuration	Code	Relation de confiance [T1199]	Logiciel

Figure 1: Schéma du processus d'attaque de la chaîne d'approvisionnement de Codecov. Le processus de création de conteneurs de Codecov présentait un bug sur les conteneurs déployés en ligne (1). Les pirates ont accédé au conteneur et obtenu les identifiants de Codecov (2). Ils ont alors modifié le script bash de Codecov (3), qui a ensuite été mise à jour chez les clients (4). Le script bash malveillant a extrait les identifiants du client pour le pirate (5), qui les a utilisés pour accéder aux données des clients (6).



2.7. TAXINOMIE DE LA CHAINE D'APPROVISIONNEMENT ET AUTRES CADRES

2.7.1. Base de connaissances MITRE ATT&CK®

MITRE ATT&CK® est une base de connaissances et un modèle de comportement des cyberadversaires. La taxinomie proposée dans le rapport diffère de la taxinomie MITRE ATT&CK®[12] car les finalités des deux sont très différentes. Par conséquent, il n'est pas possible d'utiliser MITRE ATT&CK® dans la taxinomie de la chaîne d'approvisionnement, étant donné que nous avons choisi de mettre l'accent sur les quatre aspects qui caractérisent généralement une attaque liée à la chaîne d'approvisionnement et, en particulier, la relation fournisseur-client. Alors que MITRE ATT&CK® dresse une carte complète des options et des étapes du cycle de vie de tous les types d'attaques, sa couverture des détails d'une chaîne d'approvisionnement n'est pas encore très développée.

Par exemple, dans la catégorie «Accès initial» de MITRE ATT&CK®, il existe une technique appelée «compromission de la chaîne d'approvisionnement»[13]. Ceci est très utile pour permettre aux entreprises d'identifier une chaîne d'approvisionnement comme un risque, mais trop générique lorsqu'il s'agit de se concentrer explicitement sur les attaques de la chaîne d'approvisionnement elles-mêmes. La taxinomie proposée recense tous les détails de l'attaque liée à la chaîne d'approvisionnement elle-même et pourrait donc compléter la base de connaissances MITRE ATT&CK®.

[12] MITRE ATT&CK®, MITRE, https://attack.mitre.org/. Consulté le 08/07/2021.
[13] Supply Chain Compromise, Technique T1195 – Enterprise, MITRE ATT&CK®, https://attack.mitre.org/techniques/T1195/. Consulté le 08/07/2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

2.7.2. Cadre de la Cyber Kill Chain® de Lockheed Martin

La taxinomie proposée a également une finalité différente de celle du célèbre cadre de la Cyber Kill Chain® de Lockheed Martin [14]. La Cyber Kill Chain est un cadre qui a été conçu pour identifier les mesures prises par les pirates pour atteindre leurs objectifs. Si ces mesures peuvent être prises dans le cadre d'une attaque liée à la chaîne d'approvisionnement, elles sont trop génériques pour permettre de classer, comprendre et comparer les attaques de la chaîne d'approvisionnement. La taxinomie présentée ici propose une analyse plus détaillée de ces attaques et, surtout, elle permet de cartographier les deux attaques perpétrées dans une chaîne d'approvisionnement donnée, l'une contre le fournisseur et l'autre contre le client.

[14] Cyber Kill Chain®, Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Consulté le 08/07/2021.

3. LE CYCLE DE VIE D'UNE ATTAQUE DE LA CHAINE D'APPROVISIONNEMENT

On peut observer qu'une attaque de la chaîne d'approvisionnement se compose généralement d'une attaque visant un ou plusieurs fournisseurs, puis d'une attaque ultérieure contre la cible finale, à savoir le client. Chacune de ces attaques peut ressembler très étroitement au cycle de vie des attaques APT.

Bien qu'il soit difficile de se mettre d'accord sur une définition unique de ce qu'est une attaque APT, nous avons considéré tout au long du présent rapport qu'une attaque APT correspond à toute attaque ciblée, permettant d'obtenir un accès non autorisé à une organisation (généralement par l'exécution de codes), qui s'étale sur une longue période et dont l'objectif final est spécifique à la cible (par opposition, par exemple, au minage de cryptomonnaie). Bien entendu, une telle définition n'est pas complète et beaucoup d'autres peuvent exister. Toutefois, il est important d'établir une définition pour comprendre que les attaques de la chaîne d'approvisionnement sont généralement ciblées, complexes et coûteuses, et que les pirates les planifient probablement longtemps à l'avance. Le simple fait qu'un incident typique de la chaîne d'approvisionnement implique au moins deux types d'attaques réussies est un indicateur du degré de sophistication des pirates, mais aussi de leur persistance et de leur intention de réussir.

Il convient de noter que de nombreuses attaques APT n'ont pas été considérées comme «avancées» par la communauté en ce qui concerne la qualité de leur code, les exécutions et les logiciels malveillants. Toutefois, on peut considérer que la qualification d'une attaque «avancée» renvoie à l'ensemble de l'opération et pas nécessairement au code. En fin de compte, la planification, l'échelonnement, le développement et l'exécution de deux attaques dans deux organisations constituent une tâche complexe.

Ces distinctions sont essentielles pour comprendre **qu'une organisation pourrait être vulnérable à une attaque de la chaîne d'approvisionnement même lorsque ses propres moyens de défense sont assez bons** et que, par conséquent, les pirates tentent d'explorer de nouveaux canaux potentiels pour les infiltrer en s'orientant vers leurs fournisseurs comme cible. En outre, les effets potentiels des attaques de la chaîne d'approvisionnement qui touchent de nombreux clients d'un même fournisseur sont probablement immenses. C'est une autre raison pour laquelle ces types d'attaques deviennent de plus en plus fréquents, car ils fournissent aux pirates un moyen de renforcer leur réputation et, éventuellement, de réaliser d'importants gains financiers.

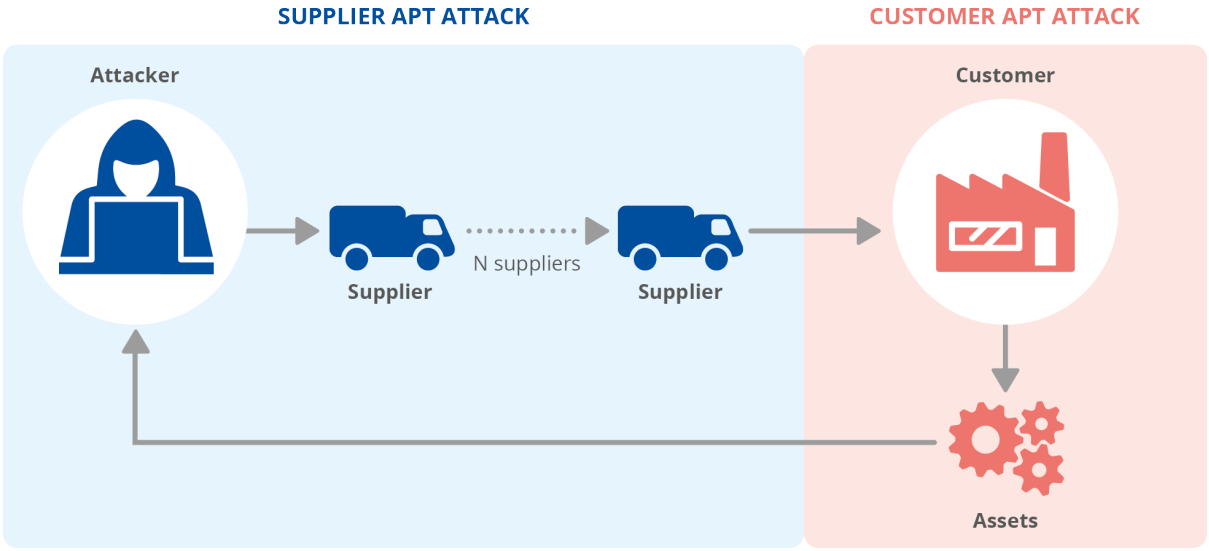
Une autre caractéristique des attaques liées à la chaîne d'approvisionnement réside dans la complexité de leur gestion et dans les efforts requis pour atténuer ces attaques et y faire face. Le simple fait qu'au moins deux entités organisationnelles soient concernées et que l'utilisation probable de vecteurs d'attaque sophistiqués complique l'analyse scientifique et la gestion globale de l'incident. La relation fournisseur-client évolue en permanence et tant les fournisseurs que les clients mettent constamment à jour leurs systèmes, c'est pourquoi il est nécessaire d'établir une sécurité continue de la chaîne d'approvisionnement ainsi qu'une évaluation et une gestion active des risques.

Le cycle de vie d'une attaque de la chaîne d'approvisionnement comporte deux parties principales: l'attaque contre le fournisseur et l'attaque contre le client. Chacune de ces attaques est généralement complexe et nécessite un vecteur d'attaque, un plan d'action et une exécution minutieuse. Ces attaques peuvent prendre des mois avant d'être couronnées de succès et, dans de nombreux cas, ne pas être détectées pendant longtemps. Le cycle de vie d'une attaque de la chaîne d'approvisionnement est illustré en figure 2.

La première attaque dans le cycle de vie est appelée «Attaque APT du fournisseur» et vise à compromettre un ou plusieurs fournisseurs. La deuxième attaque dans le cycle de vie est appelée «Attaque APT du client» et se concentre sur la cible finale de l'attaque. Ces deux parties sont liées par l'accès au fournisseur, mais elles peuvent être très

différentes en ce qui concerne les techniques utilisées, les vecteurs d'attaque exploités et le temps consacré à l'attaque.

Figure 2: Le cycle de vie des attaques de la chaîne d'approvisionnement peut être considéré comme deux attaques APT interconnectées. La première attaque vise un ou plusieurs fournisseurs et la seconde vise les clients. Ces attaques nécessitent une planification et une exécution minutieuses.



Dans au moins onze attaques sur l'ensemble des cas étudiés dans le présent rapport, des enquêtes ont confirmé que les attaques de la chaîne d'approvisionnement étaient menées par des groupes APT connus. Ces imputations ont été effectuées par les sociétés de sécurité responsables des rapports mentionnés à l'annexe A. Dans les treize autres cas, les incidents n'ont pas fait l'objet d'une enquête approfondie ou aucune imputation n'a été possible. Ces imputations soutiennent l'idée que les deux parties du cycle de vie d'une attaque de la chaîne d'approvisionnement peuvent ressembler au travail des attaques APT. Il convient de noter que l'identification d'un coupable est très difficile, sujette à erreur, imprécise et politiquement difficile, mais pas impossible.

Étant donné que chaque partie de l'attaque de la chaîne d'approvisionnement peut être considérée comme une attaque APT, son cycle de vie individuel suivrait généralement les mêmes étapes que les autres attaques APT. Ces étapes sont détaillées, par exemple, dans le MITRE ATT&CK® Tactics for Enterprises[15].

[15] MITRE ATT&CK® Tactics - Enterprise Version 9, MITRE, https://attack.mitre.org/tactics/enterprise/. Consulté le 29/06/2021.

4. PRINCIPALES ATTAQUES DE LA CHAINE D'APPROVISIONNEMENT

La présente section établit un résumé des principales attaques de la chaîne d'approvisionnement entre janvier 2020 et début juillet 2021, ainsi qu'une classification suivant la taxinomie proposée. Ces cas ont été sélectionnés en raison de l'impact important produit dans la communauté ou parce qu'ils mettent en évidence certaines caractéristiques (comme indiqué dans les éléments de la taxinomie) importantes. La liste complète et la description de toutes les attaques de la chaîne d'approvisionnement entre janvier 2020 et début juillet 2021 figurent à l'annexe A.

4.1. SOLARWINDS ORION: GESTION INFORMATIQUE ET TELESURVEILLANCE

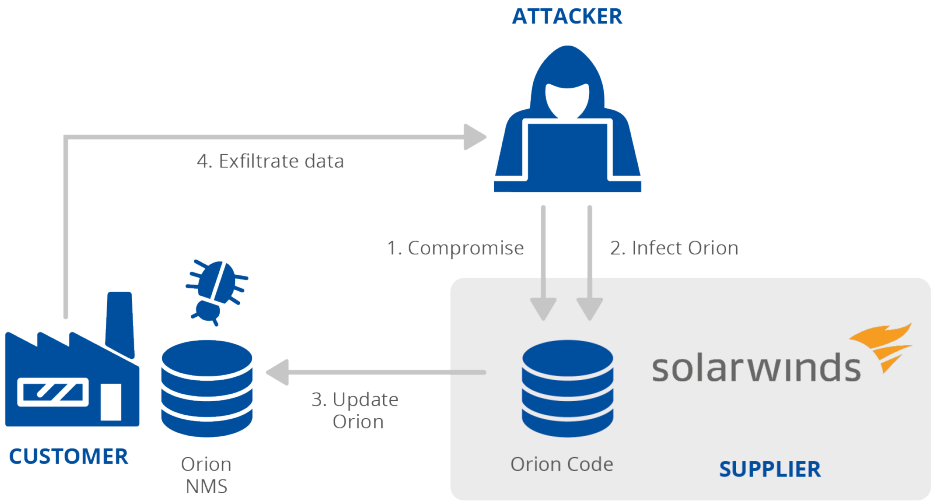
SolarWinds est une société qui propose des logiciels de gestion et de surveillance[16]. Orion est le produit du système de gestion réseau (NMS) de SolarWinds[17]. En décembre 2020, on a découvert qu'Orion avait été victime d'une attaque. Une enquête approfondie a montré que les pirates avaient eu accès au réseau de SolarWinds, éventuellement par exploitation d'une vulnérabilité jour zéro dans une application ou un dispositif tiers, par attaque par force brute ou par ingénierie sociale. Une fois l'attaque lancée, les pirates ont recueilli des informations pendant une période prolongée. Le logiciel malveillant a été injecté dans Orion au cours du processus de construction[18,19]. Le logiciel compromis a ensuite été téléchargé directement par les clients et utilisé pour recueillir et voler des informations[20]. L'attaque a été attribuée au groupe APT29[21,22].

Tableau 7: Taxinomie d'attaque de la chaîne d'approvisionnement appliquée à l'attaque impliquant SolarWinds. Les pirates ont utilisé de multiples techniques d'attaque pour compromettre le logiciel SolarWinds Orion. Ils ont modifié le code du fournisseur et abusé de la relation de confiance avec les clients de SolarWinds pour les inciter à effectuer une mise à jour contenant un logiciel malveillant. La cible finale des pirates était constituée par les données des clients.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Exploitation d'une vulnérabilité de logiciel, Attaque par force brute, Ingénierie sociale	Processus, Code	Relation de confiance [T1199], Infection par logiciel malveillant	Données

[16] What You Need To Know About the SolarWinds Supply-Chain Attack, SANS Institute, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. Consulté le 08/07/2021.
[17] Orion Platform - Scalable IT Monitoring, SolarWinds, https://www.solarwinds.com/solutions/orion. Consulté le 08/07/2021.
[18] An Investigative Update of the Cyberattack, Orange Matter, https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/. Consulté le 08/07/2021.
[19] SUNSPOT Malware: A Technical Analysis, CrowdStrike, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. Consulté le 08/07/2021.
[20] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, FireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. Consulté le 08/07/2021.
[21] SolarWinds: Advancing the Story, RiskIQ Community Edition, https://community.riskiq.com/article/9a515637. Consulté le 08/07/2021.
[22] Russian hacker group 'Cozy Bear' behind Treasury and Commerce breaches, The Washington Post, https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html. Consulté le 08/07/2021.

Figure 3: Schéma de l'attaque de la chaîne d'approvisionnement de SolarWinds. Les pirates ont compromis SolarWinds et modifié le code du logiciel ORION. Les logiciels ORION installés chez les clients ont été mis à jour à l'aide d'un logiciel malveillant, ce qui a permis aux auteurs des attaques d'accéder aux données des clients.



4.2. MIMECAST: SERVICES CLOUD DE CYBERSECURITE

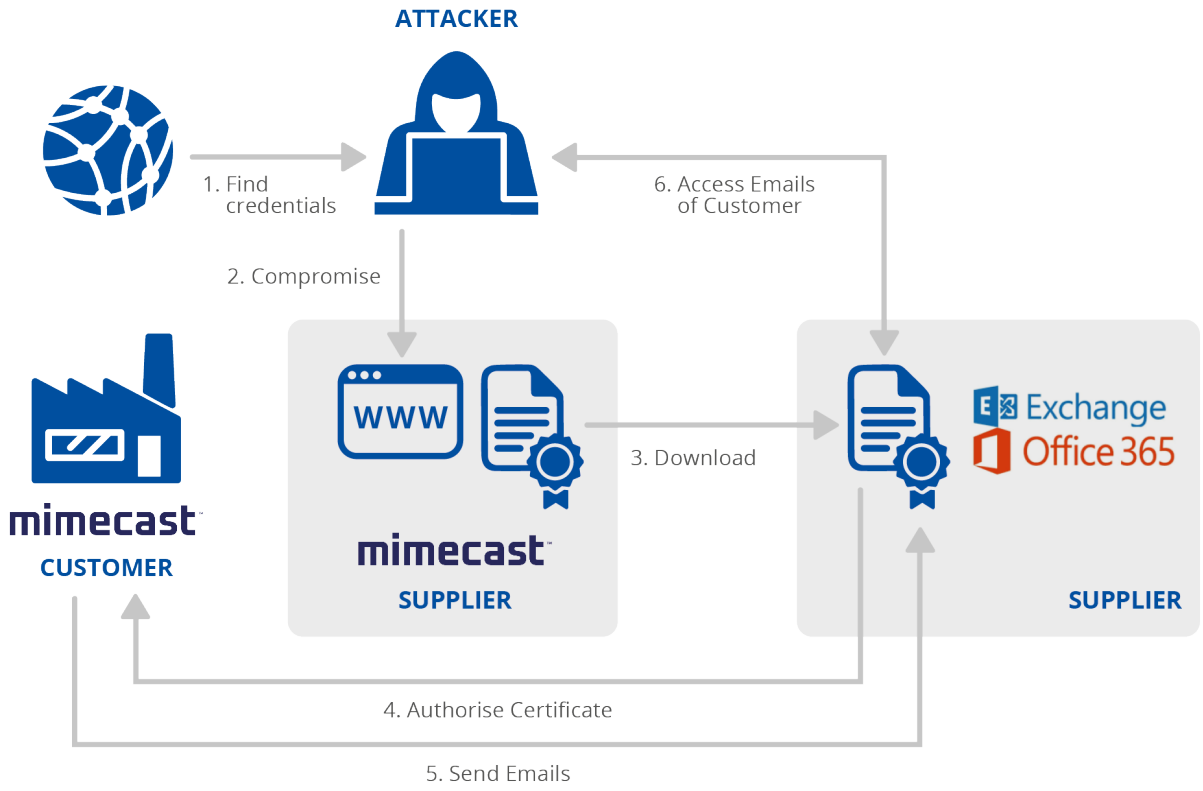
Mimecast est un fournisseur de services cloud de cybersécurité. Mimecast propose, entre autres, des services de sécurité des courriers électroniques, qui exigent des clients qu'ils se connectent de manière sécurisée aux serveurs Mimecast pour utiliser leurs comptes Microsoft 365. En janvier 2021, on a découvert que des pirates avaient compromis Mimecast (par l'intermédiaire du fournisseur SolarWinds). Après cette attaque, les pirates ont pu accéder à un certificat délivré par Mimecast et utilisé par les clients pour accéder aux services Microsoft 365, ce qui leur a permis d'intercepter les connexions réseau et de se connecter aux comptes Microsoft 365 pour voler des informations[23,24]. L'attaque a été attribuée au groupe APT29[25]. L'attaque du fournisseur aurait été liée à SolarWinds, mais aucune information concrète ne permet de le valider.

Tableau 8: Taxinomie d'attaque de la chaîne d'approvisionnement appliquée à l'attaque de Mimecast. On ignore comment les pirates ont ciblé les données des fournisseurs, en particulier un certificat délivré par Mimecast. Les pirates ont abusé de la relation de confiance des clients qui ont chargé leurs données dans Mimecast. Les pirates ont accédé aux données des clients de Mimecast.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Données	Relation de confiance [T1199]	Données

[23] Important Update from Mimecast, Mimecast Blog, https://www.mimecast.com/blog/important-update-from-mimecast/. Consulté le 08/07/2021.
[24] Mimecast Certificate Hacked in Supply-Chain Attack, Threatpost, https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/. Consulté le 08/07/2021.
[25] Important Security Update, Mimecast Blog, https://www.mimecast.com/blog/important-security-update/. Consulté le 08/07/2021.

Figure 4: Schéma de l'attaque de la chaîne d'approvisionnement de Mimecast. Les auteurs des attaques ont trouvé des identifiants qui leur ont permis de compromettre le fournisseur et d'accéder à ses certificats. Ils ont ensuite utilisé les certificats pour accéder aux données des clients, après que ceux-ci ont validé et sécurisé le certificat.



4.3. LEDGER: PORTEFEUILLE DE CRYPTOMONNAIES

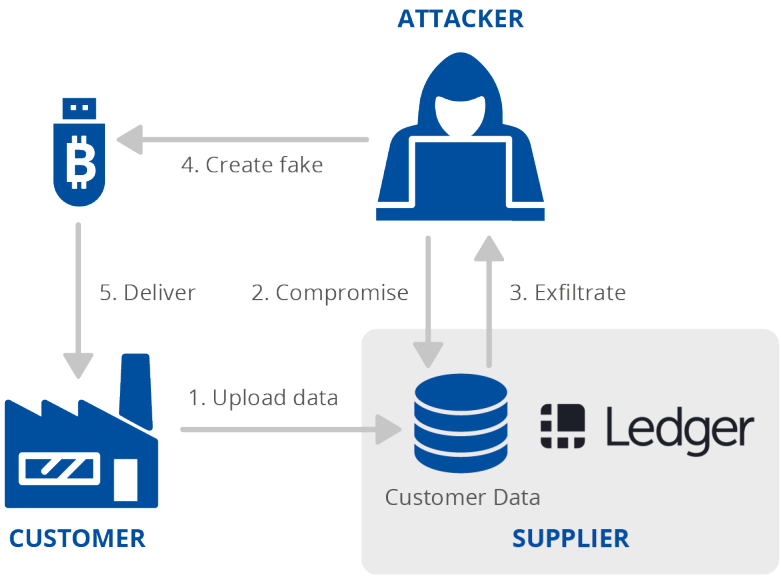
Ledger est une société qui propose une technologie de portefeuille de cryptomonnaies. En juillet 2020, des pirates ont obtenu des identifiants valides pour accéder à la base de données de commerce électronique de Ledger[26]. Les données volées ont été publiées sur un forum en ligne[27]. Les auteurs de l'attaque ont utilisé les données volées pour hameçonner et extorquer des utilisateurs en ligne[28,29], et pour voler l'argent des utilisateurs au moyen d'une attaque physique après avoir fourni aux utilisateurs des portefeuilles Ledger contrefaits qui, lorsqu'ils étaient connectés à un ordinateur et demandaient aux utilisateurs leurs clés de sécurité, infecteraient l'ordinateur avec un logiciel malveillant et renverraient les informations volées aux pirates[30]. L'attaque n'a pas été attribuée à un groupe.

Tableau 9: Taxinomie d'attaque de la chaîne d'approvisionnement appliquée à l'attaque impliquant Ledger. Les pirates ont utilisé des techniques de renseignement de sources ouvertes pour trouver les identifiants et accéder aux registres Ledger, puis voler les données des clients. Grâce à ces données, les pirates ont abusé de la relation de confiance des clients de Ledger en envoyant des courriels de hameçonnage et de faux portefeuilles de cryptomonnaies USB pour voler les cryptomonnaies des clients.

[26] Addressing the July 2020 e-commerce and marketing data breach -- A Message From Ledger's Leadership, Ledger, https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach. Consulté le 08/07/2021.
[27] Hackers Leak Customer Info From Crypto Wallet Ledger, Investopedia, https://www.investopedia.com/hackers-leak-customer-info-from-crypto-wallet-ledger-5093577. Consulté le 08/07/2021.
[28] Message by LEDGER's CEO - Update on the July data breach. Despite the leak, your crypto assets are safe, Ledger, https://www.ledger.com/message-ledgers-ceo-data-leak. Consulté le 08/07/2021.
[29] Threat Actors Target Ledger Data Breach Victims in New Extortion Campaign, Bitdefender HOTforSecurity, https://web.archive.org/web/20210520120353/https://hotforsecurity.bitdefender.com/blog/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign-25820.html, Consulté le 08/07/2021.
[30] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq, https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17. Consulté le 08/07/2021.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
OSINT	Données	Relation de confiance [T1199], Hameçonnage [T1566], Contrefaçon	Finances

Figure 5: Schéma de l'attaque de la chaîne d'approvisionnement de Ledger. Les auteurs des attaques ont trouvé les identifiants de Ledger en ligne, consulté la base de données de leurs clients et utilisé ces informations pour attaquer les clients.



4.4. KASEYA: SERVICES DE GESTION INFORMATIQUE COMPROMIS AVEC RANÇONGICIEL

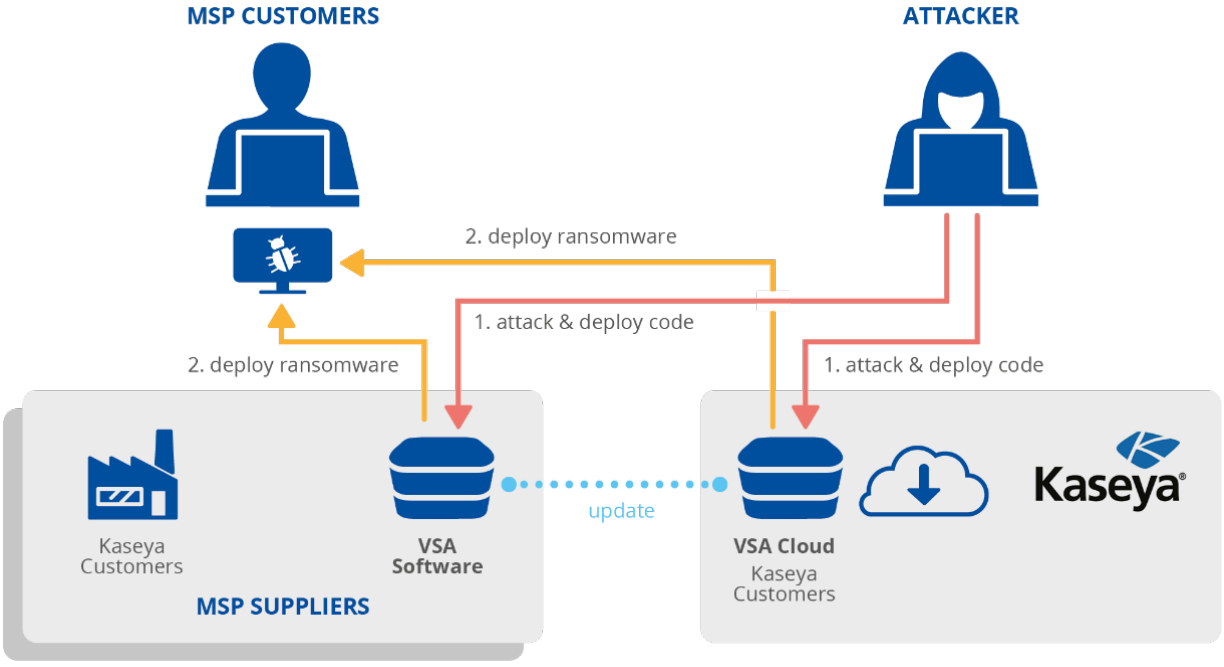
Kaseya est un fournisseur de logiciels spécialisé dans les outils de télésurveillance et de gestion. Il propose à ses clients de télécharger des logiciels VSA (Virtual System/Server Administrator) et de travailler par l'intermédiaire de ses propres serveurs cloud. Les prestataires de services gérés (Managed Service Providers, ou MSP) peuvent utiliser le logiciel VSA dans leurs locaux ou concéder des licences sur les serveurs VSA cloud de Kaseya. Les MSP proposent en retour divers services informatiques à d'autres clients[31]. En juillet 2021, des pirates ont exploité une vulnérabilité jour zéro dans les systèmes de Kaseya (CVE-2021-30116[32]), qui leur a permis d'exécuter à distance des commandes sur les appareils VSA des clients de Kaseya. Kaseya peut envoyer des mises à jour à distance à tous les serveurs VSA et, le vendredi 2 juillet 2021, une mise à jour a été distribuée aux VSA des clients de Kaseya, qui a exécuté le code des pirates. Ce code malveillant a alors déployé un rançongiciel[33,34] chez les clients gérés par ces VSA.

[31] Ransomware Hits Hundreds of US Companies, Security Firm Says, NBC10 Philadelphia, https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/. Consulté le 08/07/2021.
[32] CVE-2021-30116, MITRE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116. Consulté le 08/07/2021.
[33] Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware, Blocks and Files, https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/. Consulté le 08/07/2021.
[34] Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack, The New York Times, https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html. Consulté le 08/07/2021.

Tableau 10: Taxinomie d'attaque de la chaîne d'approvisionnement appliquée à l'attaque de Kaseya. En exploitant une vulnérabilité logicielle, les pirates ont eu accès au logiciel de Kaseya. Ils ont tiré parti de cet accès pour installer un rançongiciel sur les infrastructures des clients. L'attaque visait les données et les ressources financières des clients de Kaseya par le biais de demandes de rançon.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Exploitation d'une vulnérabilité de logiciel	Logiciels préexistants	Relation de confiance [T1199], Infection par logiciel malveillant	Données, finances

Figure 6: Schéma de l'attaque de la chaîne d'approvisionnement de Kaseya. Les pirates ont déployé des codes dans les contenus VSA des MSP (une enquête est toujours en cours afin de déterminer si cela s'est passé dans le cloud ou dans les locaux). Certains MSP ont alors été exploités pour déployer un logiciel malveillant et un rançongiciel auprès de leurs clients.



4.5. UN EXEMPLE A NOMBREUSES INCONNUES: SYSTEME DE SERVICE DE PASSAGERS DE SITA

Le cas de SITA est important en raison des nombreuses composantes des attaques de la chaîne d'approvisionnement qui demeurent **inconnues** et des conséquences possibles de leur impact. Il montre qu'il peut y avoir de nombreuses circonstances dans lesquelles les détails des attaques ne sont jamais publiés, en raison d'une impossibilité technique ou de décisions politiques et commerciales prises par les entreprises. Il y a un compromis à trouver entre un avantage pour la communauté, qui peut en améliorer sa sécurité en tirant les leçons des attaques

des autres, et les avantages pour les entreprises individuelles, par exemple dans les domaines financier, de la réputation et du marché[35].

SITA est une société spécialisée dans les technologies de l'information aérienne et les informations relatives aux transports. Le système de services de passagers de SITA est utilisé pour fournir aux compagnies aériennes des informations sur les passagers au moment de l'embarquement, y compris les risques que les passagers peuvent présenter dans un pays donné[36].

En mars 2021, il a été révélé que des pirates avaient compromis les serveurs de SITA pour accéder aux données passagers que possédaient des clients de SITA. Certains clients de SITA ont également signalé des violations de données, comme Air India, Singapore Airlines et Malaysia Airlines[36].

À la suite d'informations faisant état de fuites de données sur l'internet, Air India a également signalé que ses réseaux étaient compromis et que des données avaient été volées.[37] La compromission des réseaux internes d'Air India serait liée à l'incident de SITA; en effet une société de sécurité aurait constaté que le nom d'un ordinateur au sein d'Air India était «SITASERVER4». À ce jour, on ignore comment les pirates ont eu accès aux serveurs de SITA et on ne sait pas non plus comment ils ont pu accéder à Air India, ni s'ils l'ont effectivement fait. L'attaque interne contre les réseaux d'Air India a été imputée au groupe APT41[37].

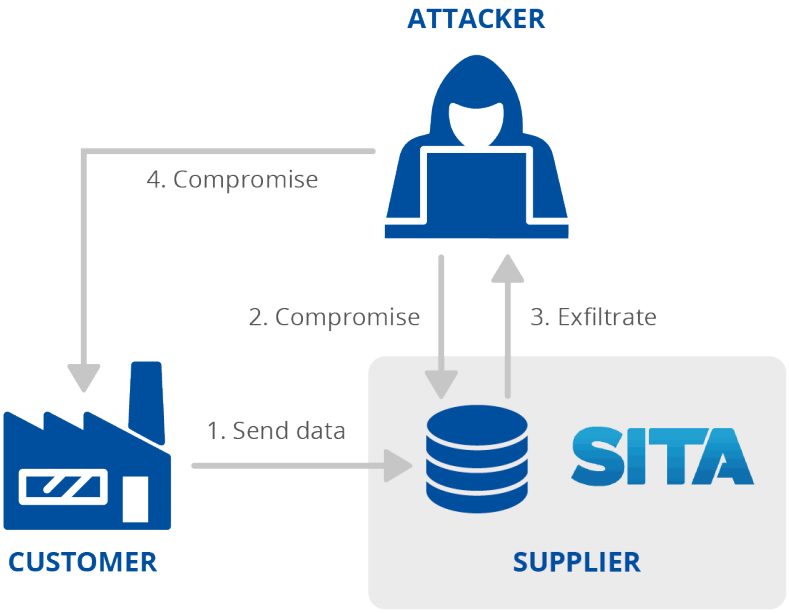
Le nombre de variables inconnues dans cet incident est un exemple du paysage des menaces en ce qui concerne les attaques de la chaîne d'approvisionnement. Le degré de maturité des enquêtes en matière de cybersécurité et la préparation de nombreuses organisations devraient également s'étendre à leurs fournisseurs, en raison de leurs relations complexes et étroitement liées.

Tableau 11: Taxinomie d'attaque de la chaîne d'approvisionnement appliquée à l'attaque impliquant SITA. On ignore comment les pirates ont eu accès au fournisseur. Les pirates ont accédé à des données chez le fournisseur concernant ses clients. On ignore comment les pirates ont réussi à infiltrer Air India. Les informations disponibles indiquent que l'objectif principal des pirates était les données clients.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Données	Inconnu	Données à caractère personnel

Figure 7: Schéma de l'attaque de la chaîne d'approvisionnement de SITA. Les pirates collectent les données relatives aux passagers des sociétés clientes de SITA. À ce jour, on ignore comment les pirates ont eu accès aux serveurs de SITA et on ne sait pas non plus comment ils ont pu accéder à Air India, ni s'ils l'ont effectivement fait.

[35] Investors in SolarWinds sold millions in stock before Russia breach revealed, The Washington Post, https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/. Consulté le 09/07/2021.
[36] SITA Advance Passenger Processing, SITA, https://www.sita.aero/solutions/sita-at-borders/border-management/sita-advance-passenger-processing/. Consulté le 08/07/2021.
[37] Big airline heist: APT41 likely behind massive supply chain attack, Group-IB, https://blog.group-ib.com/colunmtk_apt41. Consulté le 08/07/2021.


ATTACKER
4. Compromise
2. Compromise
3. Exfiltrate
1. Send data
SITA
CUSTOMER
SUPPLIER

5. ANALYSE DES INCIDENTS DE LA CHAINE D'APPROVISIONNEMENT

Dans cette section, nous présentons une analyse des attaques de la chaîne d'approvisionnement sur la base des attaques signalées entre le début de l'année 2020 et début juillet 2021. Cette analyse se concentre sur les attaques de chaînes d'approvisionnement connues du public, et une vue d'ensemble détaillée figure en annexe A. Comme discuté plus loin, certaines attaques ont été perçues comme des attaques de la chaîne d'approvisionnement, mais ce n'était finalement pas le cas et elles ont donc été retirées de l'analyse. Le tableau 12 présente un résumé de tous les incidents analysés dans le rapport.

Tableau 12: Résumé des attaques de la chaîne d'approvisionnement recensées, analysées et validées entre janvier 2020 et début juillet 2021.

FOURNISSEUR	CATÉGORIE DE FOURNISSEUR	ANNÉE	IMPACT	GROUPES AUXQUELS LES ATTAQUES ONT ÉTÉ IMPUTÉES
Mimecast	Logiciels de sécurité	2021	Mondial	APT29
SITA	Secteur aérien	2021	Mondial	APT41
Ledger	Chaîne de blocs	2021	Mondial	-
Verkada	Sécurité physique	2021	Mondial	Groupe hacktiviste
Bignox NoxPlayer	Logiciel	2021	Régional	-
Courtier d'investissement en actions	Logiciels financiers	2021	Régional	Thallium APT
ClickStudios	Logiciels de sécurité	2021	Régional	-
Apple Xcode	Logiciels de développement	2021	Mondial	-
Site web de la présidence du Myanmar	Administration publique	2021	Régional	Mustang Panda APT
Ukraine SEI EB	Administration publique	2021	Régional	-
Codecov	Logiciels d'entreprise	2021	Mondial	-
Fujitsu ProjectWEB	Collaboration dans le cloud	2021	Régional	-
Kaseya	Gestion informatique	2021	Mondial	Groupe REvil
MonPass	Organisme de certification	2021	Régional	Groupe Winnti APT
SYNNEX	Distributeur de technologies	2021	Régional	APT 29
Microsoft Windows HCP	Logiciel	2021	Mondial	-
SolarWinds	Gestion cloud	2020	Mondial	APT29
Accellion	Logiciels de sécurité	2020	Mondial	UNC2546
Wizvera VeraPort	Gestion d'identité	2020	Régional	Lazarus APT
Able Desktop	Logiciels d'entreprise	2020	Régional	TA428

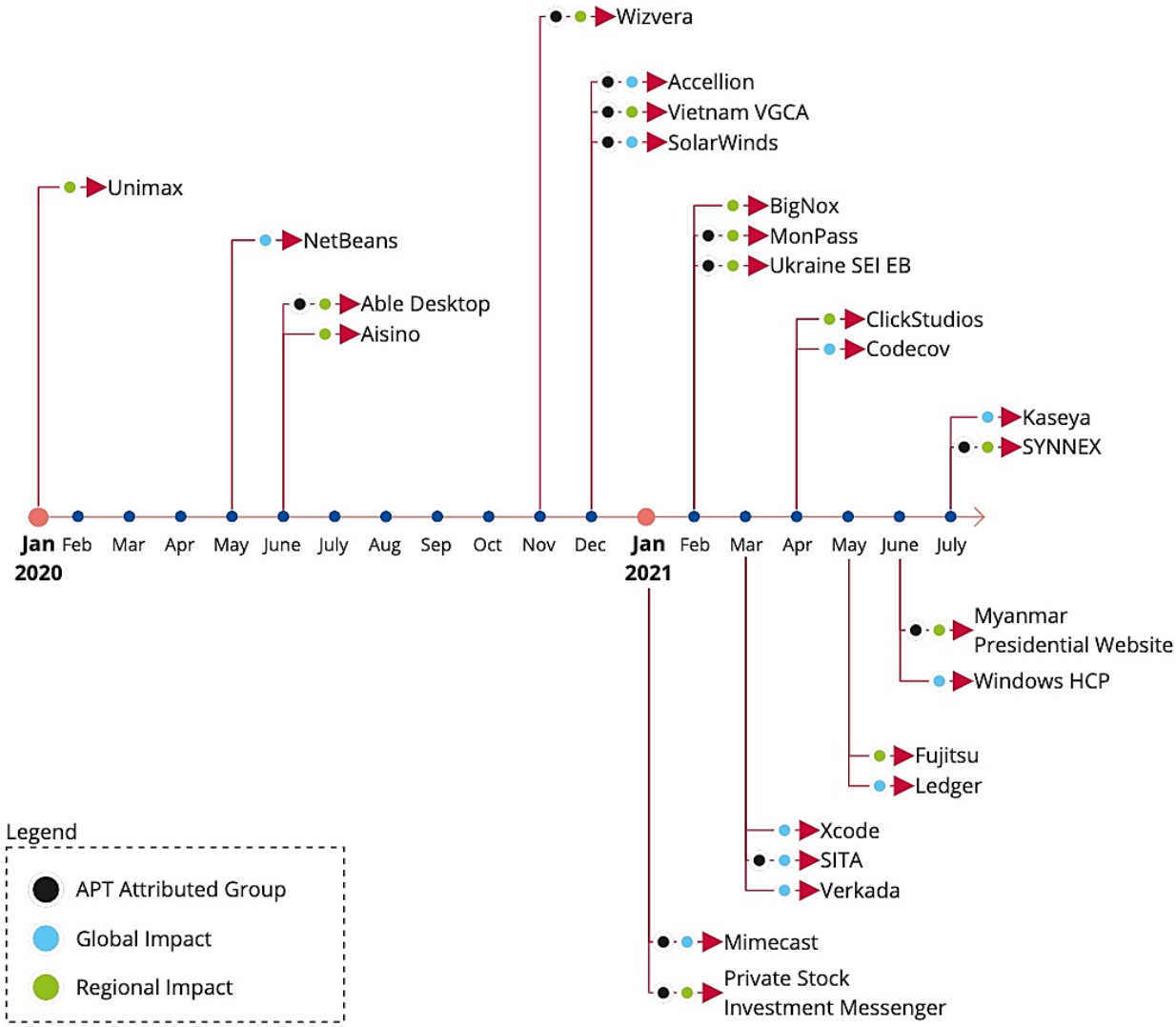
Aisino	Logiciels financiers	2020	Régional	-
Vietnam VGCA	Organisme de certification	2020	Régional	TA413, TA428
NetBeans	Logiciels de développement	2020	Mondial	-
Unimax	Télécommunications	2020	Régional	-

5.1. CHRONOLOGIE DES ATTAQUES DE LA CHAINE D'APPROVISIONNEMENT

L'analyse montre que sur les 24 attaques de la chaîne d'approvisionnement confirmées, 8 (33 %) ont été signalées en 2020 et 16 (66 %) entre janvier 2021 et début juillet 2021. **Sur la base de ces données, les prévisions de tendance indiquent que 2021 pourrait voir 4 fois plus d'attaques que 2020.**

La figure 8 présente une chronologie des attaques analysées dans le présent rapport, en soulignant les incidents qui ont été attribués à des groupes APT et s'ils ont eu un impact global ou régional. L'impact est classé dans chaque attaque comme mondial ou régional. Les attaques sont considérées comme ayant une incidence mondiale si leur clientèle est mondiale ou si le nombre d'utilisateurs finaux potentiellement touchés se compte en millions. Sinon, les attaques qui touchent des utilisateurs dans une région ou un pays donné, ou qui ne touchent qu'une poignée d'utilisateurs, sont considérées comme ayant un impact régional.

Figure 8: Chronologie des attaques de la chaîne d'approvisionnement signalées entre janvier 2020 et début juillet 2021. Le mois indiqué dans la figure correspond au mois au cours duquel l'incident a été signalé et non à la date à laquelle l'attaque s'est produite. Les incidents attribués aux groupes APT sont marqués d'un point noir, les incidents ayant un impact mondial sont signalés par un point violet, et les incidents ayant un impact régional sont marqués d'un point vert. Un résumé détaillé de chaque incident est disponible en annexe A.



5.2. COMPRENDRE LE FLUX DES ATTAQUES

Chacun des incidents présentés dans la figure 7 a été analysé, résumé et classé selon la taxinomie proposée. La taxinomie soutient et facilite l'étude des attaques de la chaîne d'approvisionnement dans leur ensemble de manière structurée.

La figure 8 est un diagramme de Sankey[38], qui illustre le flux des techniques d'attaques et des actifs visés les plus couramment observés dans le cadre des attaques de la chaîne d'approvisionnement étudiées dans le présent rapport. **Les techniques d'attaque [ST] sont utilisées contre les actifs du fournisseur [SA], qui sont ensuite utilisés dans les techniques d'attaque [CT] pour compromettre les actifs des clients [CA].**

Il ressort clairement de la figure 8 que la plupart des techniques d'attaque utilisées pour compromettre le fournisseur (première colonne [ST]) sont les suivantes:

- **Inconnu (66 %)**, suivi par
- **Exploitation des vulnérabilités logicielles (16 %)**.

[38] Les diagrammes Sankey sont un type spécifique de diagramme dans lequel la largeur des flèches est proportionnelle à la quantité de flux.

En ce qui concerne les actifs des fournisseurs ciblés (deuxième colonne [SA]), la plupart des attaques visaient à compromettre les actifs suivants:

- **Code (66 %)**,
- **Données (20 %)**
- **Processus (12 %)**.

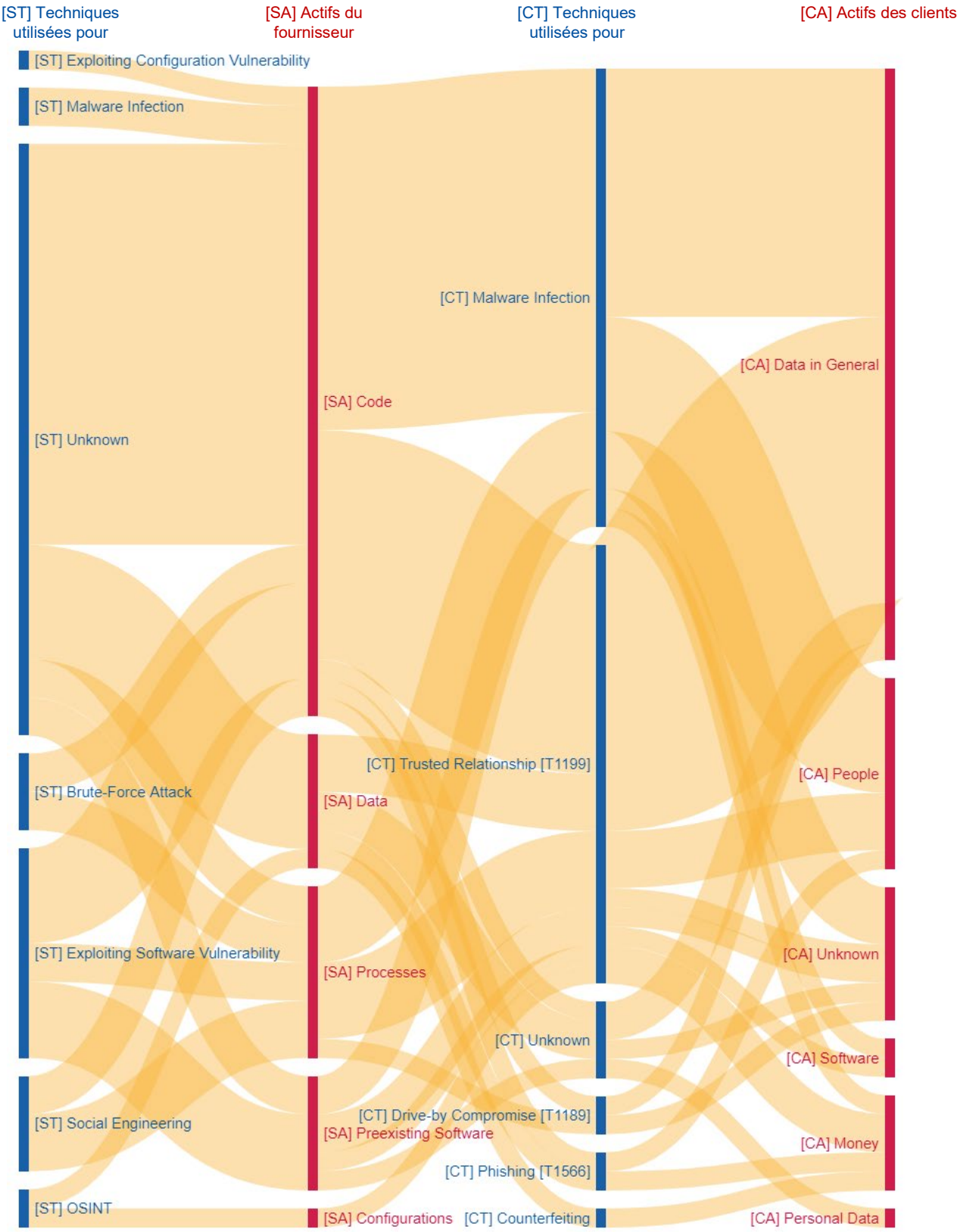
Les actifs des fournisseurs compromis sont utilisés comme vecteurs d'attaque pour compromettre les clients. Ces attaques sont principalement perpétrées (troisième colonne [CT]) des manières suivantes:

- En **abusant de la confiance du client (62 %)** dans le fournisseur, ou
- En utilisant **un logiciel malveillant (62 %)**.

Indépendamment de la technique utilisée, la plupart des attaques liées à la chaîne d'approvisionnement visent à obtenir l'accès (quatrième colonne [CA]) aux actifs suivants:

- **Données** clients **(58 %)**,
- **Personnes** clés **(16 %)** et
- **Ressources financières (8 %)**.

Figure 9: Analyse des incidents de la chaîne d'approvisionnement sur la base de la taxinomie proposée. Le diagramme de Sankey décrit le flux des techniques d'attaque [ST] utilisées contre les actifs du fournisseur [SA], qui sont ensuite utilisées dans les techniques d'attaque [CT] pour compromettre les actifs des clients [CA]. La largeur des connexions entre les différents éléments augmente lorsque la relation a été observée dans un plus grand nombre d'attaques de la chaîne d'approvisionnement.



5.3. PIRATES AXES SUR L'OBJECTIF

Lors de l'examen des actifs ciblés, dans **66 %** des incidents, les agresseurs se sont concentrés sur **le code** des fournisseurs afin de compromettre davantage les clients ciblés. Dans **20 %** des incidents analysés, les pirates ciblaient les **données** et dans **12 %** des cas, les cibles de l'attaque contre le fournisseur étaient des **processus internes**. Ceci est essentiel pour comprendre où concentrer les efforts en matière de protection de la cybersécurité. Les organisations devraient concentrer leurs efforts sur la validation des codes et logiciels tiers afin de s'assurer qu'il n'ont pas été altérés ou manipulés.

Les actifs du client final ciblés par ces attaques de la chaîne d'approvisionnement semblent être principalement des données clients, y compris des données à caractère personnel et des droits de propriété intellectuelle. C'était le cas pour 58 % des incidents de la chaîne d'approvisionnement analysés. Les pirates visaient également, dans une moindre mesure, d'autres actifs, notamment des personnes, des logiciels et des ressources financières.

5.4. LA PLUPART DES VECTEURS D'ATTAQUE VISANT A COMPROMETTRE LES FOURNISSEURS DEMEURENT INCONNUS

Nos constatations montrent que pour **66 %** des attaques de la chaîne d'approvisionnement analysées, **les fournisseurs ne savaient pas** qu'ils avaient été compromis ou n'ont pas été transparents à cet égard. En revanche, moins de **9 %** des clients compromis par des attaques de la chaîne d'approvisionnement ne savaient pas comment ces attaques s'étaient déroulées. **Cela met en évidence l'écart de maturité en matière de notification des incidents de cybersécurité entre les fournisseurs et les entreprises qui font face à des utilisateurs finaux.**

Étant donné que **83 %** des fournisseurs appartiennent au secteur de la **technologie**, le manque de connaissances sur la manière dont les attaques ont été perpétrées pourrait indiquer soit **un faible niveau de maturité** en ce qui concerne la cyberdéfense des infrastructures des fournisseurs, soit un manque de volonté de partager les informations pertinentes. D'autres facteurs peuvent contribuer à un manque de compréhension de la manière dont les fournisseurs ont été compromis, notamment la complexité et la sophistication des attaques et la lenteur de la découverte des attaques, ce qui peut également entraver les enquêtes.

5.5. ATTAQUES SOPHISTIQUEES ATTRIBUEES AUX GROUPES APT

Plus de **50 % des attaques de la chaîne d'approvisionnement ont été attribuées à** des groupes bien connus en matière de cybercriminalité, dont APT29, APT41, Thallium APT, UNC2546, Lazarus APT, TA413 et TA428. L'analyse montre que les groupes APT semblent avoir une légère préférence pour des cibles ayant un impact régional et qu'un grand nombre de ces attaques visaient à obtenir l'accès aux données des clients.

Sur les 24 incidents analysés, 10 n'ont pas été attribués à un groupe particulier. La principale raison de ce manque d'imputation peut être le fait que sept de ces attaques ont eu lieu au cours des sept derniers mois. Les enquêtes de ce type d'incidents peuvent prendre plus de temps et même lorsqu'elles sont terminées, dans certains cas, il n'est toujours pas possible d'attribuer les incidents à leurs auteurs. Toutefois, compte tenu de la sophistication de ces attaques, les fournisseurs devraient s'attendre à être la cible de groupes organisés de cybercriminalité et se préparer en conséquence.

6. TOUTES LES ATTAQUES NE SONT PAS FORCEMENT DES ATTAQUES DE LA CHAINE D'APPROVISIONNEMENT

De janvier 2020 à début juillet 2021, il y a eu de nombreux incidents qui, à l'origine, **semblaient** être des attaques de la chaîne d'approvisionnement ou étaient considérés comme faisant partie d'une future attaque probable de la chaîne d'approvisionnement. De nombreuses vulnérabilités logicielles traditionnelles qui ont été constatées ont été signalées comme présentant un «risque» pour de futures attaques de la chaîne d'approvisionnement. Certains cas concernaient des vulnérabilités qui étaient considérées comme étant délibérément placées dans des logiciels ou du matériel, mais qui se sont révélées ultérieurement être des bugs ou des erreurs involontaires. Bon nombre de ces cas n'étaient pas des attaques liées à la chaîne d'approvisionnement, car ils n'impliquaient pas la compromission d'un fournisseur.

Au moins à trois reprises, des pirates ont ciblé des dépendances ou bibliothèques logicielles. Dans l'un de ces cas, signalé en décembre 2020, les auteurs de l'attaque ont chargé des packages malveillants dans le répertoire de RubyGems[39]. Un cas très similaire a été signalé en mars 2021, lorsqu'un chercheur en sécurité est parvenu à charger des packages de NPM malveillants en utilisant des noms connus comme étant les noms de composants ou d'infrastructures utilisés par des entreprises célèbres[40]. Un troisième cas a été signalé en avril 2021, lorsque des pirates ont chargé un package NPM malveillant en tentant délibérément de le faire passer pour un package bien connu dans le cadre d'une attaque nommée «brandjacking»[41]. Dans tous ces cas, les pirates n'ont pas compromis les packages existants ni les répertoires de logiciels eux-mêmes, de sorte que, sans une attaque claire contre les actifs des fournisseurs, nous ne pouvons les considérer comme des attaques de la chaîne d'approvisionnement.

Dans de nombreux cas, des vulnérabilités logicielles ont été découvertes mais n'ont pas été utilisées lors d'attaques, ou ont été considérées comme des erreurs qui n'avaient pas été introduites intentionnellement. Le premier exemple d'un tel cas a été rapporté en février 2020, dans lequel un chercheur en sécurité a révélé une vulnérabilité jour zéro dans le micrologiciel développé par la société Xiaongmai et utilisé pour les DVD, RNV et caméras IP[42]. Parmi les autres exemples figurent les vulnérabilités signalées dans les extensions de Visual Studio Code en mai 2021[43] et les places de marché des logiciels libres et open source (FOSS) basés sur Pling en juin 2021[44]. Dans tous ces cas, des vulnérabilités ont été découvertes, mais aucune attaque active n'avait été signalée au moment de la rédaction du présent rapport. Comme indiqué dans les sections précédentes, une attaque de la chaîne d'approvisionnement implique au moins deux attaques, l'une contre un fournisseur et l'autre contre un client. Sans ces éléments, l'attaque ne peut être considérée comme une attaque de la chaîne d'approvisionnement.

[39] Russian Sandworm hackers only hit orgs with old Centreon software, Bleeping Computer, https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-only-hit-orgs-with-old-centreon-software/. Consulté le 08/07/2021.
[40] Malicious NPM packages target Amazon, Slack with new dependency attacks, Bleeping Computer, https://www.bleepingcomputer.com/news/security/malicious-npm-packages-target-amazon-slack-with-new-dependency-attacks/. Consulté le 08/07/2021.
[41] Damaging Linux \& Mac Malware Bundled within Browserify npm Brandjack Attempt, Sonatype, https://blog.sonatype.com/damaging-linux-mac-malware-bundled-within-browserify-npm-brandjack-attempt. Consulté le 08/07/2021.
[42] Full disclosure: 0day vulnerability (backdoor) in firmware for Xiaongmai-based DVRs, NVRs and IP cameras, Habr, https://habr.com/en/post/486856/. Consulté le 08/07/2021.
[43] Newly Discovered Bugs in VSCode Extensions Could Lead to Supply Chain Attacks, The Hacker News, https://thehackernews.com/2021/05/newly-discovered-bugs-in-vscode.html. Consulté le 08/07/2021.
[44] Unpatched Flaw in Linux Pling Store Apps Could Lead to Supply-Chain Attacks, The Hacker News, https://thehackernews.com/2021/06/unpatched-critical-flaw-affects-pling.html. Consulté le 08/07/2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

En outre, il y a eu d'autres cas d'attaques et de vulnérabilités liées à la cybersécurité qui n'étaient pas des attaques de la chaîne d'approvisionnement. L'un de ces cas est l'attaque contre les systèmes du Centreon. Centreon est une entreprise qui fournit des services de surveillance informatique et propose un outil de suivi informatique en logiciel libre. En janvier 2021, on a découvert que des pirates avaient exploité des instances publiques dépassées de Centreon pour compromettre les infrastructures des clients[45,46,47]. Les pirates, que l'on pensait appartenir au groupe Sandworm APT, ont mené leur campagne pendant trois ans avant d'être découverts. L'attaque visait à extraire des informations auprès des clients concernés. Elle ciblait des fournisseurs informatiques français. Il s'agit d'un cas où une vulnérabilité logicielle particulière a été exploitée dans un logiciel installé par des clients. Toutefois, le fournisseur lui-même n'a pas été compromis et les vulnérabilités n'étaient pas intentionnelles.

[45] Campagne d'attaque du mode opératoire Sandworm ciblant des serveurs Centreon, CERT-FR, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf. Consulté le 08/07/2021.
[46] France Reveals 3-Year Long Supply Chain Attack, Secure World Expo, https://www.secureworldexpo.com/industry-news/france-supply-chain-attack-centreon-software. Consulté le 08/07/2021.
[47] Russian Sandworm hackers only hit orgs with old Centreon software, Bleeping Computer, https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-only-hit-orgs-with-old-centreon-software/. Consulté le 08/07/2021.

7. RECOMMANDATIONS

Les attaques de la chaîne d'approvisionnement **tirent parti de l'interconnexion des marchés mondiaux**. Lorsque plusieurs clients dépendent du même fournisseur, les conséquences d'une cyberattaque contre ce fournisseur sont amplifiées, ce qui pourrait avoir une incidence à grande échelle au niveau national, voire transfrontalier. Pour certains produits, tels que les logiciels et les codes exécutables, l'existence d'une chaîne d'approvisionnement est opaque, voire totalement dissimulée à l'utilisateur final. Les logiciels de l'utilisateur final dépendent, directement ou indirectement, des logiciels fournis par le fournisseur. Ces dépendances comprennent des packages, des bibliothèques et des modules, qui sont tous utilisés de manière pérenne pour réduire les coûts de développement et accélérer les délais d'expédition.

Plus les organisations sont protégées contre les cyberattaques, plus l'attention est portée aux fournisseurs. Le calcul est simple: les fournisseurs deviennent le maillon faible de la chaîne d'approvisionnement. En même temps, les clients demandent des produits plus cybersécurisés mais qui restent bon marché, deux besoins qu'il n'est pas toujours possible de concilier.

Comme nous l'avons observé lors de nombreux incidents d'attaques de la chaîne d'approvisionnement, les organisations sont de plus en plus conscientes de la nécessité **d'évaluer la maturité de leurs fournisseurs en matière de cybersécurité** et le **niveau d'exposition au risque découlant de cette relation client/fournisseur**. Les clients doivent évaluer et prendre en compte la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs, notamment le fait qu'ils appliquent des procédures de développement sûres. En outre, les clients devraient faire preuve d'une vigilance accrue dans la sélection et la vérification de leurs fournisseurs, ainsi que dans la gestion du risque découlant de ces relations.

Pour **gérer le risque de cybersécurité de la chaîne d'approvisionnement**, les clients devraient[48]:

- identifier et documenter les types de fournisseurs et de fournisseurs de services,
- définir des critères de risque pour différents types de fournisseurs et de services (par exemple, dépendances importantes des fournisseurs et des clients, dépendances logicielles critiques, points uniques de défaillance),
- évaluer les risques liés à la chaîne d'approvisionnement en fonction de leurs propres analyses d'impact et exigences en matière de continuité des activités,
- définir des mesures de traitement des risques fondées sur les bonnes pratiques,
- surveiller les risques et les menaces pesant sur la chaîne d'approvisionnement, en s'appuyant sur des sources d'information internes et externes et sur les conclusions de la surveillance et des examens des performances des fournisseurs,
- sensibiliser leur personnel au risque.

Pour **gérer la relation avec les fournisseurs**, les clients devraient:

- gérer les fournisseurs tout au long du cycle de vie d'un produit ou d'un service, y compris les procédures de traitement des produits ou composants hors d'usage,
- classer les actifs et les informations qui sont partagés avec les fournisseurs ou accessibles à ceux-ci, et définir les procédures pertinentes pour leur accès et leur traitement,
- définir les obligations des fournisseurs en ce qui concerne la protection des actifs de l'organisation, le partage d'informations, les droits d'audit, la continuité de l'activité, le filtrage du personnel et le traitement des incidents en termes de responsabilités, d'obligations de notification et de procédures,
- définir des exigences de sécurité pour les produits et services acquis,
- inclure toutes ces obligations et exigences dans les contrats, convenir de règles pour la sous-traitance et les éventuelles exigences en cascade,

[48] Sources: contrôles de cybersécurité des normes ISO/IEC 27002, ISO 9001 et ISO 31000.

- contrôler la performance des services et effectuer des audits de sécurité de routine afin de vérifier le respect des exigences de cybersécurité dans les accords. Il s'agit notamment de la gestion des incidents, des vulnérabilités, des correctifs, des exigences en matière de sécurité, etc.,
- obtenir de la part des fournisseurs et des fournisseurs de services l'assurance qu'aucune fonctionnalité cachée ou porte dérobée n'est délibérément incluse,
- veiller à ce que les exigences réglementaires et juridiques soient prises en considération,
- définir les processus permettant de gérer les changements dans les accords de fournisseurs, par exemple les changements dans les outils, les technologies, etc.

D'autre part, les fournisseurs devraient garantir le **développement sûr de produits et de services** qui soit conforme aux pratiques de sécurité communément admises[49]. Les fournisseurs devraient:

- veiller à ce que l'infrastructure utilisée pour concevoir, développer, fabriquer et fournir des produits, des composants et des services respecte les pratiques en matière de cybersécurité[50,51],
- mettre en œuvre un processus de développement, de maintenance et de soutien de produits qui soit cohérent avec les processus de développement de produits communément acceptés,
- mettre en œuvre un procédé d'ingénierie sécurisé conforme aux pratiques communément admises en matière de sécurité[52, 53],
- examiner l'applicabilité des exigences techniques en fonction de la catégorie de produits et des risques[54],
- proposer des déclarations de conformité aux clients pour des normes connues, à savoir ISO/IEC 27001, IEC 62443-4-1, IEC 62443-4-2 (ou des normes spécifiques telles que la matrice de contrôle cloud CSA pour les services cloud), et garantir et attester, dans la mesure du possible, l'intégrité et l'origine des logiciels libres utilisés dans n'importe quelle portion d'un produit,
- définir des objectifs de qualité tels que le nombre de défauts ou de vulnérabilités identifiés dans des rapports externes ou les problèmes de sécurité signalés en externe, et les utiliser comme un instrument pour améliorer la qualité globale,
- maintenir des données exactes et à jour sur l'origine du code ou des composants logiciels, ainsi que sur les contrôles appliqués aux composants, outils et services logiciels internes et tiers présents dans les processus de développement de logiciels,
- réaliser des audits réguliers pour s'assurer que les mesures susmentionnées sont respectées.

En outre, étant donné que tout produit ou service est construit à partir de composants et de logiciels soumis à des vulnérabilités ou s'appuyant sur de tels composants ou logiciels, les fournisseurs **devraient mettre en œuvre de bonnes pratiques en matière de gestion de la vulnérabilité**[55], telles que:

- le suivi des vulnérabilités de sécurité signalées par des sources internes et externes, y compris les composants de tiers utilisés,
- l'analyse des risques des vulnérabilités à l'aide d'un système de notation des vulnérabilités (CVSS[56], par exemple),
- les politiques de maintenance pour le traitement des vulnérabilités identifiées en fonction du risque,
- les processus d'information des clients,

[49] Par exemple IEC 62443-4-1.
[50] Par exemple, celles de la norme ISO/CEI 27001.
[51] Il peut s'agir de mesures techniques, telles que (a) la séparation des environnements; (b) l'audit des relations de confiance; (c) la mise en place d'une authentification multifactorielle fondée sur le risque et d'un accès conditionnel dans l'ensemble de l'organisation; (d) la réduction au minimum des dépendances à l'égard des produits qui font partie des environnements utilisés pour développer, construire et éditer des logiciels; (e) le chiffrement des données; (f) la surveillance des opérations et alertes, et la réactions aux tentatives échouées et réussies de cyberattaques.
[52] Par exemple IEC 62443-2-4
[53] Il peut s'agir notamment de l'utilisation d'outils automatisés, ou de processus comparables, pour maintenir des chaînes d'approvisionnement en codes sources fiables, garantissant ainsi l'intégrité du code; ou l'utilisation d'outils automatisés, ou de processus comparables, permettant de détecter les vulnérabilités connues et potentielles et d'y remédier.
[54] Des normes telles que la norme CEI 62443-4-2 fournissent un ensemble complet d'exigences de sécurité qui sont classées pour les exigences applicables à tous les produits, aux applications logicielles (SAR), aux dispositifs embarqués (EDR), aux dispositifs hôtes (HDR) et aux dispositifs réseau (NDR).
[55] Les normes IEC 62443-4-1, IEC 62443-2-4 et IEC TR 62443-2-3 fournissent davantage d'indications sur la gestion des vulnérabilités et correctifs.
[56] Voir https://www.first.org/cvss/specification-document ;.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- la vérification et le test des correctifs pour s'assurer que les exigences opérationnelles, de sécurité, juridiques et de cybersécurité sont respectées et que les correctifs sont compatibles avec les composants tiers non intégrés,
- les procédures de livraison sécurisée des correctifs et la documentation relative aux correctifs aux clients, ou
- la participation à un programme de divulgation des vulnérabilités comprenant un processus de déclaration et de divulgation.

Les vulnérabilités devraient être gérées par les fournisseurs sous la forme de correctifs. De même, un client devrait surveiller le marché en cas de vulnérabilités potentielles ou recevoir les notifications de vulnérabilité correspondantes de la part de ses fournisseurs. Parmi les **bonnes pratiques en matière de gestion des correctifs** figurent[57]:

- la tenue d'un inventaire des actifs comprenant des informations pertinentes en matière de correctifs,
- l'utilisation des ressources d'informations pour identifier les vulnérabilités techniques pertinentes,
- l'évaluation des risques liés aux vulnérabilités identifiées et la mise en place d'une politique de maintenance documentée et intégrée,
- la réception de correctifs provenant uniquement de sources légitimes, et leur test avant leur installation,
- l'application de mesures alternatives au cas où un correctif ne serait pas disponible ou applicable,
- l'application de procédures de démantèlement et de sauvegarde efficaces et de processus de restauration.

Au-delà de ce que peuvent faire les clients et les fournisseurs individuellement, des initiatives peuvent être prises au niveau de l'industrie. Google a présenté, en juin 2021, un cadre de bout en bout visant à garantir l'intégrité des artéfacts logiciels tout au long de la chaîne d'approvisionnement des logiciels, baptisé SLSA (Supply chain Levels for Software Artifacts)[58]. L'objectif de SLSA est d'améliorer la situation de l'industrie, en particulier de source ouverte, afin de se défendre contre les menaces les plus importantes à l'encontre de l'intégrité des produits. Bien que SLSA se concentre sur les attaques de la chaîne d'approvisionnement des logiciels et non sur tous les autres types, il s'agit d'un bon point de départ qui peut bénéficier aux organisations.

Un ensemble plus général mais étendu de recommandations pour la défense contre les menaces en matière de cybersécurité a été publié en juin 2021 par le MITRE, connu sous le nom de projet MITRE D3FEND[59].
MITRE D3FEND est un cadre ou une base de connaissances structurée qui permet aux organisations de trouver des mesures d'atténuation spécifiques pour prévenir des attaques spécifiques, comme le montre le cadre MITRE ATT&CK®. Ce projet n'est pas spécifique à la chaîne d'approvisionnement ni aux attaques APT, mais les recommandations peuvent être utilisées pour accroître le niveau fondamental de sécurité des organisations.

Il n'en demeure pas moins que tous les risques liés à la chaîne d'approvisionnement ne peuvent pas être atténués par les bonnes pratiques mises en œuvre par les clients, les fournisseurs ou les organisations. En particulier, les fonctions cachées et les capacités d'accès non documentées (portes dérobées) dans les composants du matériel ne peuvent être identifiées de manière exhaustive par les certifications ou les tests de pénétration standard les plus courants. En outre, les vulnérabilités jour zéro, c'est-à-dire les vulnérabilités connues uniquement d'un groupe spécifique et utilisées par celui-ci, continuent de poser problème. Par conséquent, une action peut s'avérer nécessaire au niveau national, voire européen. Les autorités nationales compétentes pourraient procéder à des évaluations nationales des risques en matière de sécurité pour les risques liés à la chaîne d'approvisionnement, qui tiendraient compte des acteurs connus afin de déterminer les mesures relatives au sourçage des fournisseurs au niveau national. En outre, les attaques de la chaîne d'approvisionnement peuvent être soutenues par des acteurs étatiques dotés de capacités avancées et, dans ce cas, l'assistance des autorités compétentes peut être nécessaire pour atténuer les risques d'attaques appuyées par l'État.

[57] Source: norme ISO/CEI 27002.
[58] Google Online Security Blog: Introducing SLSA, an End-to-End Framework for Supply Chain Integrity, Google, https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html. Consulté le 08/07/2021.
[59] MITRE D3FEND™, D3FEND Matrix, Version 0.9.2-BETA-3, https://d3fend.mitre.org/. Consulté le 29/06/2021.

8. CONCLUSIONS

À mesure que le coût des attaques directes contre des organisations bien protégées augmente, les pirates préfèrent attaquer leur chaîne d'approvisionnement, ce qui constitue la motivation supplémentaire d'un impact potentiellement à grande échelle et transfrontalier. Cette migration a donné lieu à **un nombre plus important que d'habitude de cas d'attaques de la chaîne d'approvisionnement**, avec une prévision de **quatre fois plus d'attaques de la chaîne d'approvisionnement en 2021 qu'en 2020**. Le caractère intrinsèquement mondial des chaînes d'approvisionnement actuelles accroît l'impact potentiel de ces attaques et élargit la surface d'attaque des acteurs malveillants. Le présent rapport couvre un certain nombre d'attaques connues mais, en réalité, il peut y avoir d'autres d'attaques de la chaîne d'approvisionnement qui n'ont pas été détectées, qui n'ont pas fait l'objet d'une enquête ou qui sont imputables à d'autres causes.

En particulier dans le domaine des logiciels, les attaques de la chaîne d'approvisionnement sapent la confiance dans l'écosystème logiciel. Les incidents décrits mettent en évidence la possibilité pour les acteurs malveillants de **compromettre la chaîne d'approvisionnement des logiciels dès ses tout premiers stades** (phase de développement). De nouvelles approches doivent être élaborées pour sécuriser la chaîne d'approvisionnement dès la conception. De nouvelles initiatives telles que Google SLSA et MITRE D3FEND semblent assez prometteuses en ce sens.

L'analyse figurant dans le présent rapport montre qu'il subsiste un grand nombre de facteurs inconnus dans les incidents faisant l'objet de l'enquête. **66 % des vecteurs d'attaque utilisés sur les fournisseurs demeurent inconnus**. Le manque de transparence ou la capacité d'enquête posent un risque sérieux pour la confiance dans la chaîne d'approvisionnement. L'optimisation du processus de transparence et de responsabilité constitue la première étape pour améliorer la sécurité de tous les maillons de la chaîne d'approvisionnement et protéger les clients finaux.

Les attaques de la chaîne d'approvisionnement peuvent être complexes, nécessiter une planification minutieuse et prendre souvent des mois ou des années à exécuter. Si **plus de 50 % de ces attaques sont attribuées à des groupes APT ou à des pirates bien connus**, l'efficacité des attaques de la chaîne d'approvisionnement peut faire des fournisseurs une cible intéressante pour d'autres types de pirates, plus génériques, à l'avenir. Il est donc essentiel que les organisations concentrent leur sécurité non seulement sur leurs propres organisations, mais aussi sur leurs fournisseurs. C'est notamment le cas pour les fournisseurs de services cloud et de services gérés, où les attaques récentes mettent en évidence le besoin accru de contrôles de cybersécurité dans ces secteurs.

En raison de l'accroissement des interdépendances et de la complexité, l'impact des attaques sur les fournisseurs peut avoir **des conséquences considérables**. Non seulement cela est dû au grand nombre de parties concernées, mais cela peut aussi, en particulier dans les cas où des informations classifiées sont exfiltrées, susciter des inquiétudes en matière de sécurité nationale ou provoquer des conséquences de nature géopolitique.

Dans cet environnement complexe pour les chaînes d'approvisionnement, l'établissement de **bonnes pratiques au niveau de l'UE et des actions coordonnées sont importants** pour aider tous les États membres à développer des capacités similaires, et ce, afin d'atteindre un niveau commun de sécurité.

ANNEXE A: RÉSUMÉ DES ATTAQUES DE LA CHAÎNE D'APPROVISIONNEMENT

La présente section résume 24 incidents de la chaîne d'approvisionnement recensés et analysés dans le présent rapport. Chaque incident est identifié par le fournisseur impliqué dans l'attaque. La taxinomie proposée dans le présent rapport est ensuite appliquée à chaque cas et un schéma illustrant la manière dont l'attaque s'est produite est inclus par souci de clarté. Les informations contenues dans les résumés renvoient aux informations disponibles au moment de la rédaction du présent rapport.

LISTE DES INCIDENTS DE LA CHAINE D'APPROVISIONNEMENT:

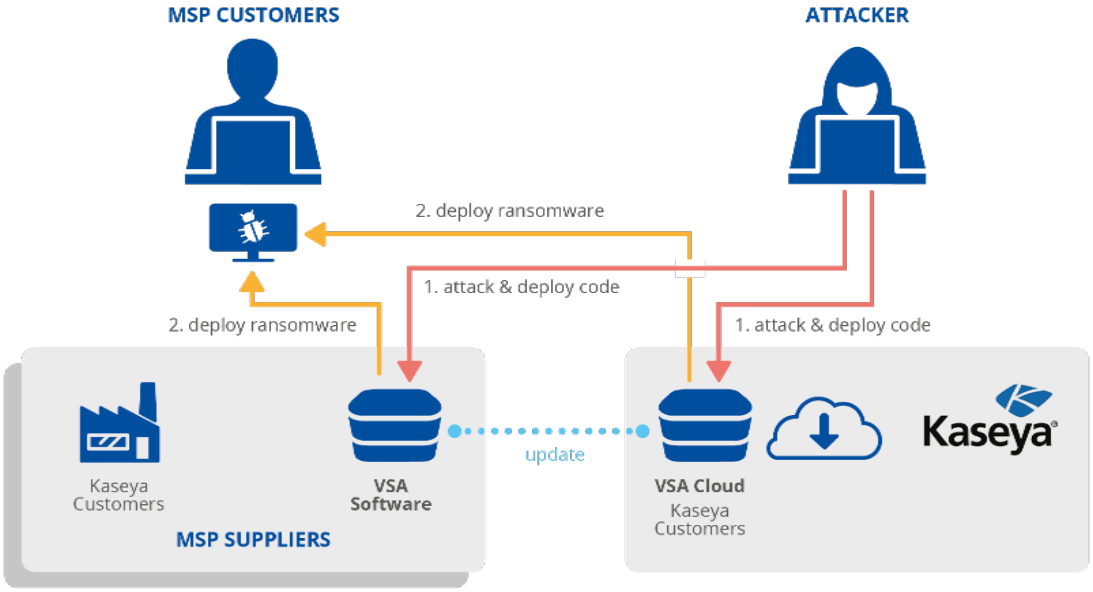
A.1 KASEYA: GESTION DE LOGICIELS INFORMATIQUES

Kaseya[60] est un fournisseur de logiciels spécialisé dans les outils de télésurveillance et de gestion. Il propose un logiciel VSA (Virtual System/Server Administrator) et fournit ses propres serveurs cloud. Les prestataires de services gérés (Managed Service Providers, ou MSP) peuvent utiliser le logiciel VSA dans leurs locaux ou concéder des licences sur les serveurs VSA cloud de Kaseya. Les MSP proposent en retour divers services informatiques à d'autres clients[61].

En juillet 2021, des pirates ont exploité une vulnérabilité jour zéro dans les systèmes de Kaseya (CVE-2021-30116[62]). Les pirates ont pu exécuter à distance des commandes sur les appareils VSA des clients de Kaseya. Kaseya peut envoyer des mises à jour à distance à tous les serveurs VSA et, le vendredi 2 juillet 2021, une mise à jour a été distribuée aux VSA des clients de Kaseya, qui a exécuté le code des pirates. Ce code malveillant a alors déployé un rançongiciel[63,64] chez les clients gérés par ces VSA.

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Exploitation d'une vulnérabilité de logiciel	Logiciels préexistants

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Relation de confiance [T1199], Infection par logiciel malveillant	Données, Finances



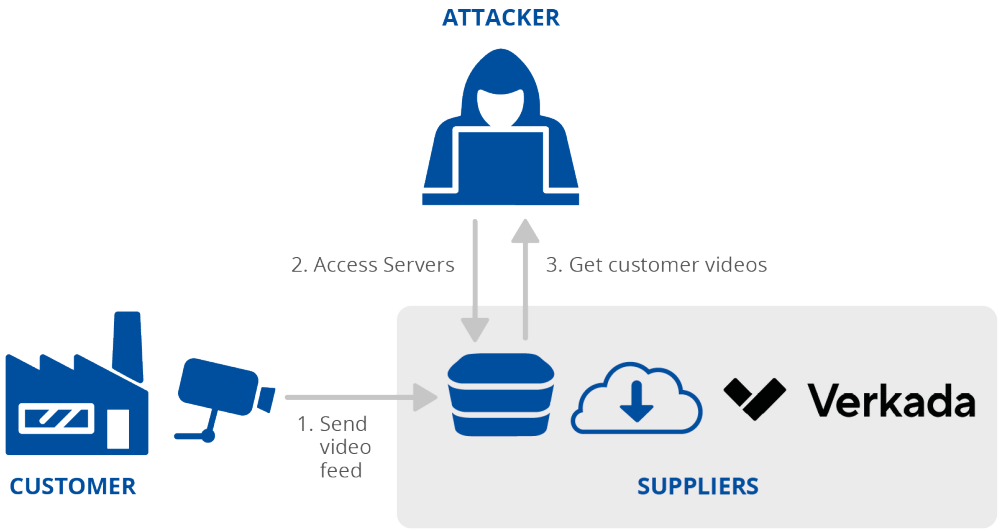
[60] IT Management Software - for MSPs and IT Teams, Kaseya, https://www.kaseya.com/. Consulté le 09/07/2021.
[61] Ransomware Hits Hundreds of US Companies, Security Firm Says, NBC10 Philadelphia, https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/. Consulté le 09/07/2021.
[62] CVE-2021-30116, MITRE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116, Consulté le 09/07/2021.
[63] Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware, Blocks and Files, https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/, Consulté le 09/07/2021.
[64] Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack, The New York Times, https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html. Consulté le 09/07/2021.

A.2 VERKADA: SOLUTIONS DE SURVEILLANCE DE SECURITE DANS LE CLOUD

Verkada propose des solutions de surveillance de sécurité dans le cloud à plus de 5 000 clients[65]. En mars 2021, un serveur de production a été compromis, ce qui a permis aux pirates ayant obtenu les identifiants privilégiés d'accéder aux caméras de sécurité déployées dans les installations des clients[66]. Les identifiants auraient été trouvés «sur l'internet»[67]. Les pirates ont eu accès aux vidéos et aux images des clients auprès de plus de 150 000 caméras situées dans des écoles, des prisons, des hôpitaux, des commissariats de police et des usines Tesla[68]. Un groupe hacktiviste a revendiqué l'attaque[69].

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
OSINT	Configurations, Données

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Relation de confiance [T1199]	Données



[65] The Future of Physical Security for the Enterprise: About Verkada, Verkada, https://www.verkada.com/about/. Consulté le 09/07/2021.
[66] Verkada Security Update, Verkada, https://www.verkada.com/security-update/. Consulté le 09/07/2021.
[67] Verkada Mass Hack, IPVM, https://ipvm.com/reports/verkada-hack. Consulté le 09/07/2021.
[68] A hacker who exposed Verkada's surveillance camera snafu has been raided, The Verge, https://www.theverge.com/2021/3/12/22328344/tillie-kottmann-hacker-raid-switzerland-verkada-cameras. Consulté le 09/07/2021.
[69] Tesla (TSLA), Cloudfare (NET) Breached in Verkada Security Camera Hack, Bloomberg, https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams. Consulté le 09/07/2021.

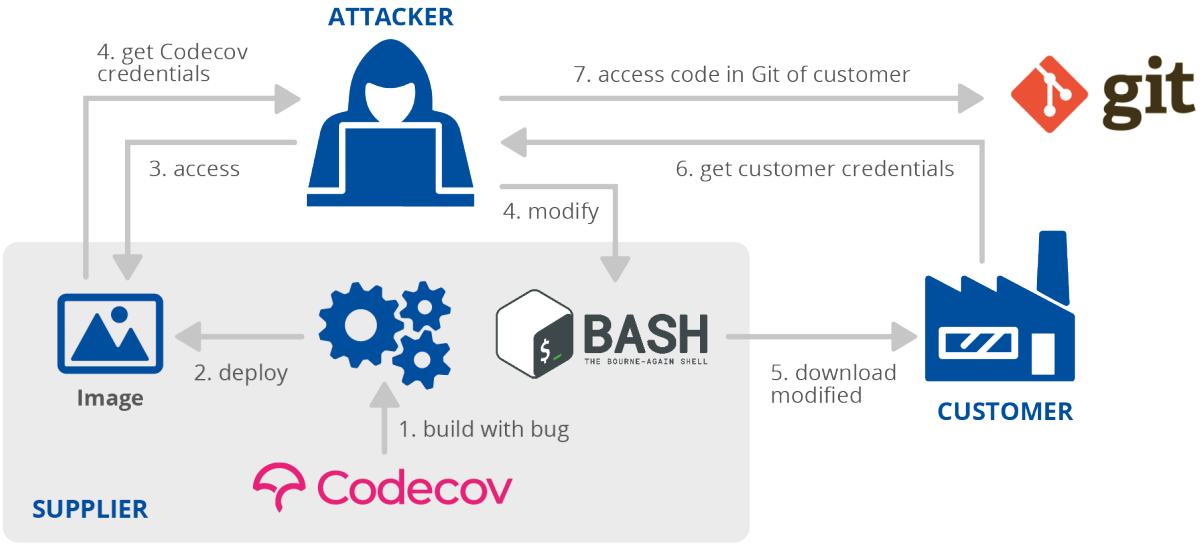
A.3 CODECOV: SOLUTIONS DE GESTION ET D'AUDIT DE CODES

Codecov est une société qui propose des logiciels de couverture de codes et d'outils de test. La société fournit des outils à d'autres sociétés telles qu'IBM et Hewlett Packard Enterprise. En avril 2021, Codecov a indiqué que des pirates avaient obtenu une partie de ses identifiants valides à partir d'une image Docker en raison d'une erreur de création de ces images Docker.

Une fois que les auteurs des attaques ont obtenu ces identifiants, ils les ont utilisés pour compromettre un «chargement de script bash»[70] utilisé par les clients de Codecov. Lorsque les clients ont téléchargé et exécuté ce script, les pirates ont été en mesure d'extraire des données des clients de Codecov, y compris des informations sensibles qui leur permettraient d'accéder aux ressources des clients[71]. Plusieurs clients de Codecov ont indiqué que les pirates avaient pu accéder à leur code source en utilisant des informations volées provenant de cette attaque sur Codecov[71]. L'attaque n'a pas été attribuée à un groupe.

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Exploitation d'une vulnérabilité de la configuration	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Relation de confiance [T1199]	Logiciel



[70] Codecov supply chain attack breakdown, https://blog.gitguardian.com/codecov-supply-chain-breach/. Consulté le 27/06/2021.

[71] Codecov hackers gained access to Monday.com source code, Bleeping Computer. https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/. Consulté le 27/06/2021.

[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A.4 WIZVERA VERAPORT: PROGRAMME D'INTEGRATION D'INSTALLATION

Wizvera est une société qui fournit des solutions pour la vérification de l'identité, la gestion des mots de passe et les certificats cloud[72]. Wizvera possède un produit appelé VeraPort, un programme d'intégration d'installation qui permet aux utilisateurs d'installer des logiciels de sécurité requis par leurs employeurs[73]. En novembre 2020, des pirates ont compromis un site web légitime pris en charge par VeraPort. Ils ont remplacé la configuration de VeraPort sur le site web compromis afin de fournir un logiciel malveillant au lieu du logiciel de sécurité attendu.

La configuration a été signée numériquement par Wizvera[73]. VeraPort vérifie si le logiciel téléchargé est muni d'une signature numérique en cours de validité, mais il ne vérifie pas qui a délivré le certificat. Grâce à ce mécanisme, les utilisateurs sud-coréens ayant accédé au site web compromis ont téléchargé le logiciel malveillant. L'attaque a été attribuée au groupe APT Lazarus[73].

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Processus	Compromission «drive-by» [T1189], Infection par logiciel malveillant	Données

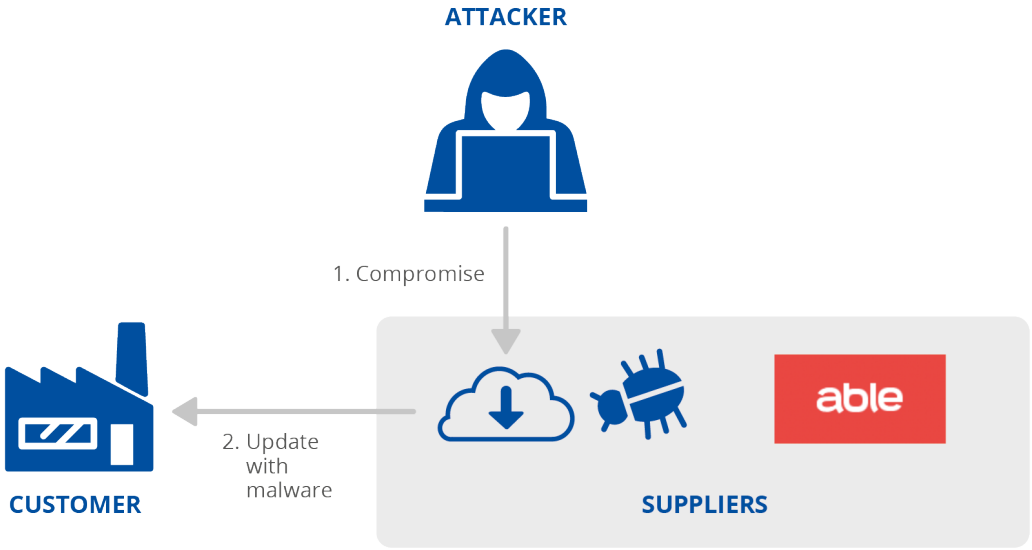
[72] Wizvera Company Profile & Funding, Crunchbase, https://www.crunchbase.com/organization/wizvera. Consulté le 09/07/2021.
[73] Lazarus supply-chain attack in South Korea, WeLiveSecurity, https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/. Accessed le 09/07/2021.

A.5 ABLE DESKTOP: LOGICIEL DE MESSAGERIE INSTANTANEE

Able est une société établie en Mongolie qui fournit des solutions logicielles aux agences gouvernementales et aux entreprises de la région[74]. En juin 2020, des pirates semblent avoir accédé au serveur dorsal d'Able et compromis le système qui fournit des mises à jour logicielles à tous les clients. Les pirates ont ajouté un logiciel malveillant à l'application «Able Desktop» (un programme additionnel qui fournit une messagerie instantanée au produit principal d'Able)[75]. Bien que l'on ignore comment le fournisseur a été compromis, les pirates ont pu contraindre les utilisateurs à installer un logiciel malveillant[75]. Ce logiciel malveillant a ensuite été utilisé pour voler des informations provenant des appareils infectés des clients[75]. L'attaque a été attribuée au groupe APT TA428.

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Relation de confiance [T1199], Infection par logiciel malveillant	Données



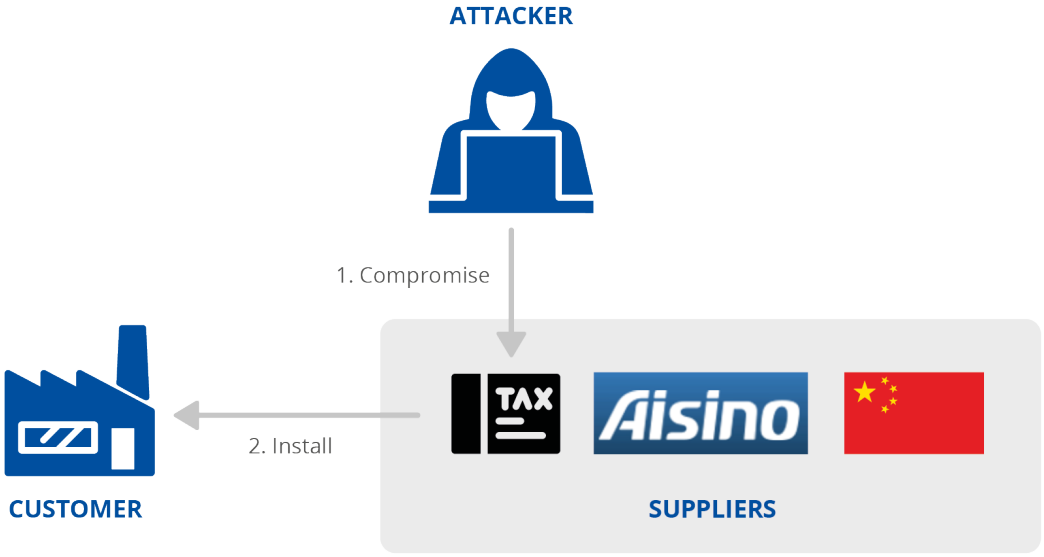
[74] Able - Working online, Able, https://web.able.mn/, Consulté le 09/07/2021.
[75] Operation StealthyTrident: corporate software under attack, WeLiveSecurity, https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/. Consulté le 09/07/2021.

A.6 SUITE LOGICIELLE FISCALE INTELLIGENTE AISINO

Aisino Credit Information Company fournit un logiciel de paiement de l'impôt à des clients internationaux par l'intermédiaire de son département «Golden Tax», notamment la «Suite logicielle fiscale Aisino». En juin 2020, des chercheurs ont révélé que la «Suite logicielle fiscale Aisino» avait été compromise pour y inclure un logiciel malveillant[76]. On ignore comment le logiciel a été compromis et quel était l'objectif de l'attaque[76]. L'attaque visait des entreprises en Chine, étant donné que ce logiciel fait partie d'un programme national dans ce pays[77]. L'attaque n'a pas été attribuée à un groupe.

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Relation de confiance [T1199], Infection par logiciel malveillant	Inconnu



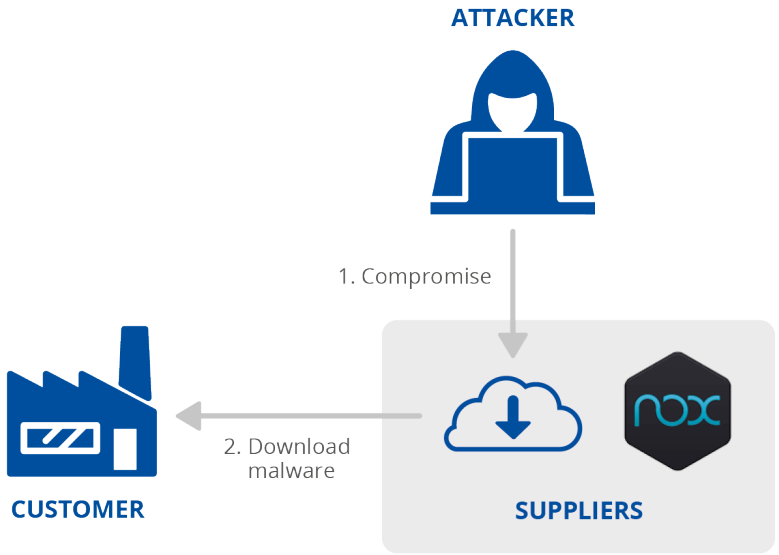
[76] The Golden Tax Department and Emergence of GoldenSpy Malware, Trustwave SpiderLabs, https://trustwave.azureedge.net/media/16929/the-golden-tax-department-and-emergence-of-goldenspy-malware.pdf. Consulté le 09/07/2021.
[77] GoldenSpy Chapter 4: GoldenHelper Malware Embedded in Official Golden Tax Software, Trustwave, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/. Consulté le 09/07/2021.

A.7 BIGNOX NOXPLAYER: EMULATEUR ANDROID POUR PC ET MAC

BigNox est une société qui fournit des logiciels d'émulation. Son principal produit, NoxPlayer, est un émulateur Android très populaire pour Windows et Mac[78]. En février 2021, des chercheurs ont signalé que l'infrastructure de NoxPlayer avait été compromise. L'attaque a pu abuser du mécanisme de mise à jour de l'outil et, au lieu des mises à jour, fournir un logiciel malveillant[79].

Une fois la charge utile initiale fournie, les pirates ont pu recueillir des informations sur leurs victimes et fournir d'autres logiciels malveillants à des cibles spécifiques[79]. Il semblerait que l'objectif des pirates était la capacité de recenser des cibles spécifiques[79]. L'attaque n'a pas été attribuée à un groupe.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code	Relation de confiance [T1199], Infection par logiciel malveillant	Personnes, Données



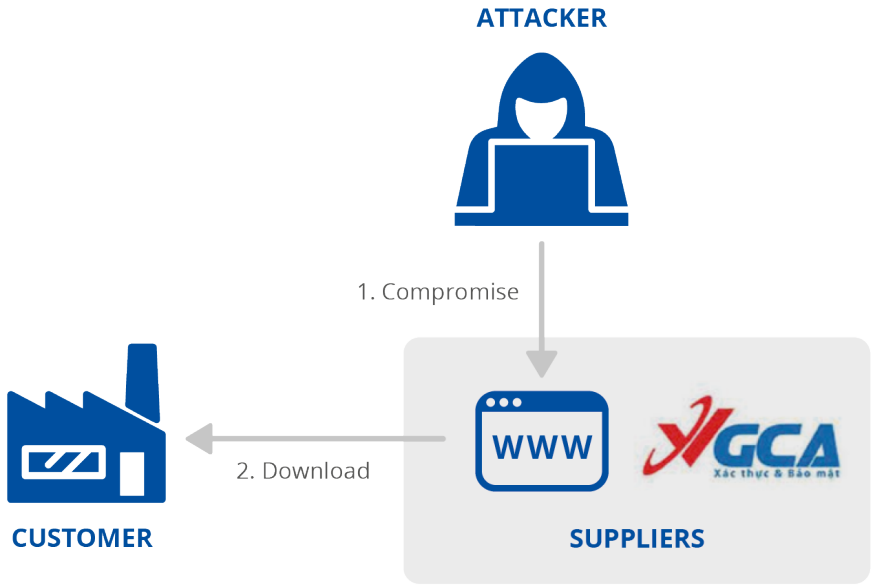
[78] NoxPlayer - Free Android Emulator on PC and Mac, BigNox, https://www.bignox.com/. Consulté le 09/07/2021.
[79] Operation NightScout: Supply-chain attack targets online gaming in Asia, WeLiveSecurity, https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/. Consulté le 09/07/2021.

A.8 AUTORITE DE CERTIFICATION DU GOUVERNEMENT VIETNAMIEN (VGCA)

L'autorité de certification du gouvernement vietnamien (VGCA) fournit des certificats numériques et un ensemble d'applications qui aident les citoyens et les entreprises à signer numériquement des documents[80]. En décembre 2020, des chercheurs ont indiqué que le site web de l'infrastructure VGCA avait été compromis pour remplacer des binaires légitimes par des applications trojanisées[81]. L'objectif de l'attaque n'est pas clair, mais les chercheurs estiment que cela pourrait s'inscrire dans le cadre d'une attaque de plus grande ampleur[81]. Les outils utilisés indiquent que des groupes APT (TA413, TA428) pourraient être à l'origine de l'attaque[82].

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Relation de confiance [T1199], Infection par logiciel malveillant	Personnes



[80] Vietnam targeted in complex supply chain attack, ZDNet, https://www.zdnet.com/article/vietnam-targeted-in-complex-supply-chain-attack/. Consulté le 09/07/2021.
[81] Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia, WeLiveSecurity, https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/. Consulté le 09/07/2021.
[82] Panda's New Arsenal: Part 3 Smanager, Hiroki Hada, https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager. Consulté le 09/07/2021.

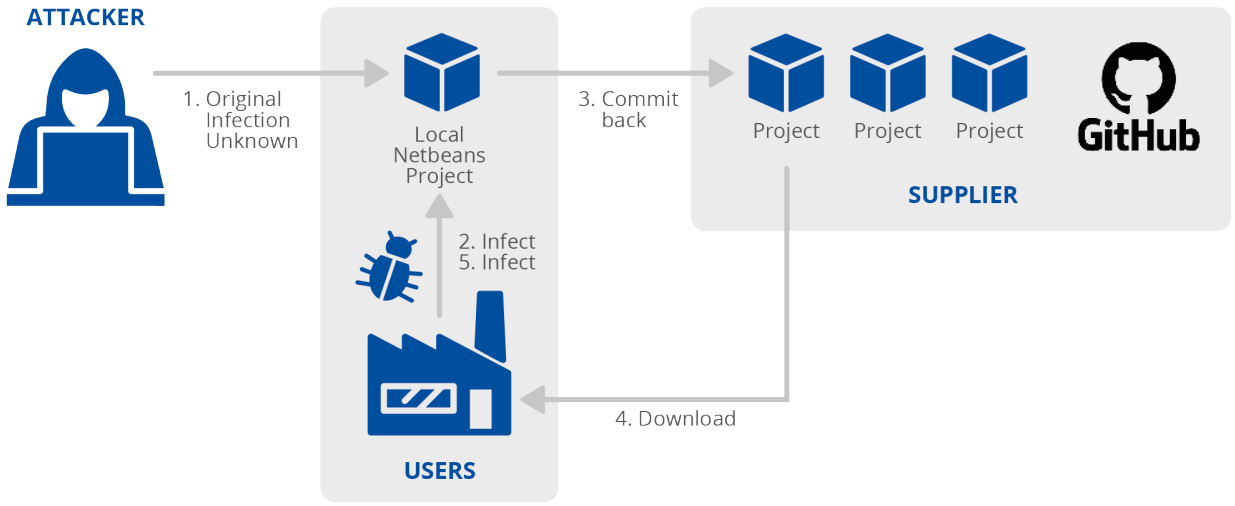
A.9 APACHE NETBEANS: PLATEFORME DE DEVELOPPEMENT

NetBeans est une plateforme intégrée de développement Java par Apache. En mai 2020, des chercheurs ont indiqué que certains projets NetBeans sur GitHub contenaient un logiciel malveillant à l'insu des propriétaires. Tous ceux qui téléchargeaient et utilisaient ces projets se verraient infectés et trojanisés sur tous leurs projets NetBeans locaux, et les téléchargeraient sur GitHub.

Les utilisateurs ont également été infectés par un logiciel malveillant RAT[83,84]. L'objectif des pirates semblait être la collecte d'informations confidentielles. Cette attaque semble faire partie d'une attaque de la chaîne d'approvisionnement de plus grande ampleur. Dans ce cas, les utilisateurs sont à la fois fournisseurs et victimes. GitHub est le seul moyen de partage utilisé. L'attaque n'a pas été attribuée à un groupe.

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Infection par logiciel malveillant	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Infection par logiciel malveillant	Logiciels, Données

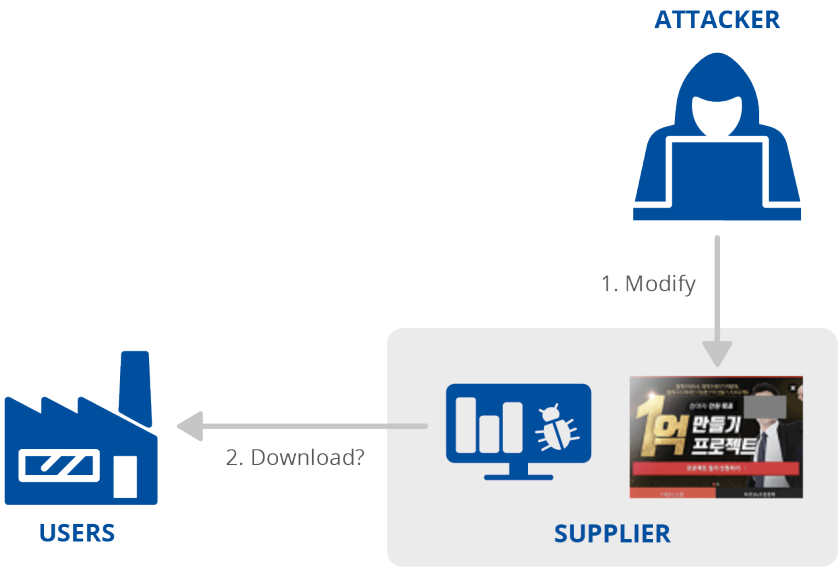


[83] The Octopus Scanner Malware: Attacking the open source supply chain, GitHub Security Lab, https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain/. Consulté le 09/07/2021.
[84] Supply Chain Attack Event - Targeted Attacks on Java Projects in GitHub, NSFOCUS, https://nsfocusglobal.com/supply-chain-attack-event-targeted-attacks-on-java-projects-in-github/. Consulté le 09/07/2021.

A.10 COURTIER PRIVE D'INVESTISSEMENT EN ACTIONS

En janvier 2021, des chercheurs ont indiqué que des investisseurs en bourse étaient ciblés par le groupe Thallium APT, ce qui compromettait une application de messagerie d'investissement privé largement utilisée[85]. Les pirates ont trojanisé les installateurs de l'application de messagerie pour y inclure un logiciel malveillant[86]. Ce logiciel malveillant a ensuite été utilisé pour espionner les utilisateurs infectés[87]. Il n'existe pas d'informations fiables sur l'attaque ou les méthodes utilisées.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code	Infection par logiciel malveillant	Personnes

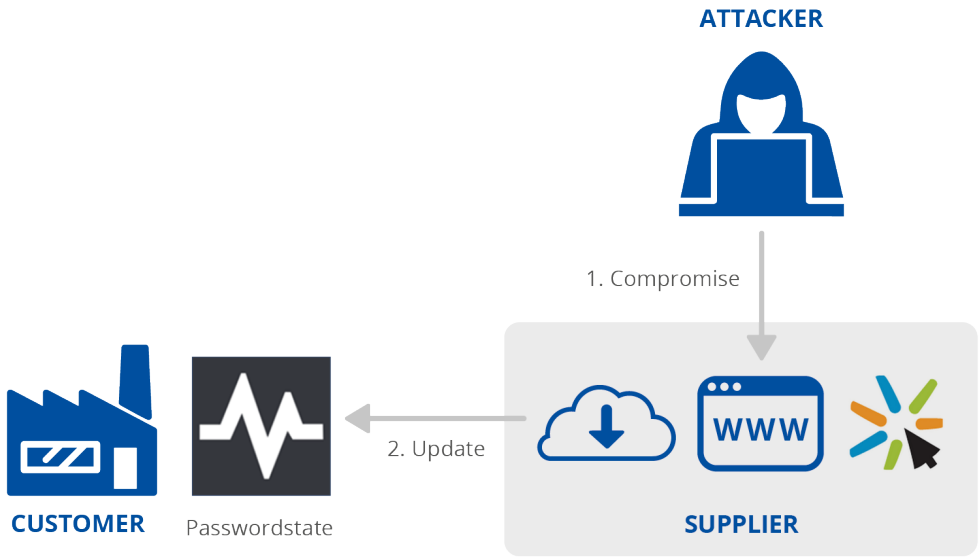


[85] Thallium Hacker Targeted Users of Private Stock Investment Messenger, Cyware Alerts - Hacker News, https://cyware.com/news/thallium-hacker-targeted-users-of-private-stock-investment-messenger-ac33d20d. Consulté le 09/07/2021.
[86] Thallium Altered the Installer of a Stock Investment App, E Hacking News, https://www.ehackingnews.com/2021/01/thallium-altered-installer-of-stock.html. Consulté le 09/07/2021.
[87] Thallium organization exploits private equity investment messenger to launch software supply chain attack, ESTsecurity, https://blog.alyac.co.kr/3489. Consulté le 09/07/2021.

A.11 CLICKSTUDIOS PASSWORDSTATE: GESTIONNAIRE DE MOT DE PASSE

ClickStudios est une société qui fournit des solutions de gestion de mots de passe d'entreprise[88]. Son principal produit est un outil appelé «Passwordstate». En avril 2021, le mécanisme web «upgrade director» de Passwordstate utilisé pour mettre à jour l'outil a été compromis[89], réorientant les utilisateurs vers le téléchargement d'un logiciel malveillant au lieu des mises à jour attendues. Le logiciel malveillant installé a été conçu pour voler les informations provenant des systèmes compromis[89, 90]. L'attaque n'a pas été attribuée à un groupe.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code	Relation de confiance [T1199], Infection par logiciel malveillant	Données



[88] Enterprise Password Management Software - Web based Server Password Manager, ClickStudios https://www.clickstudios.com.au/. Consulté le 09/07/2021.
[89] ClickStudios PASSWORDSTATE Incident Management Advisory #01, ClickStudios, https://www.clickstudios.com.au/advisories/Incident_Management_Advisory-01-20210424.pdf. Consulté le 09/07/2021.
[90] Moserpass supply chain, CSIS Security Group, https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/. Consulté le 09/07/2021.

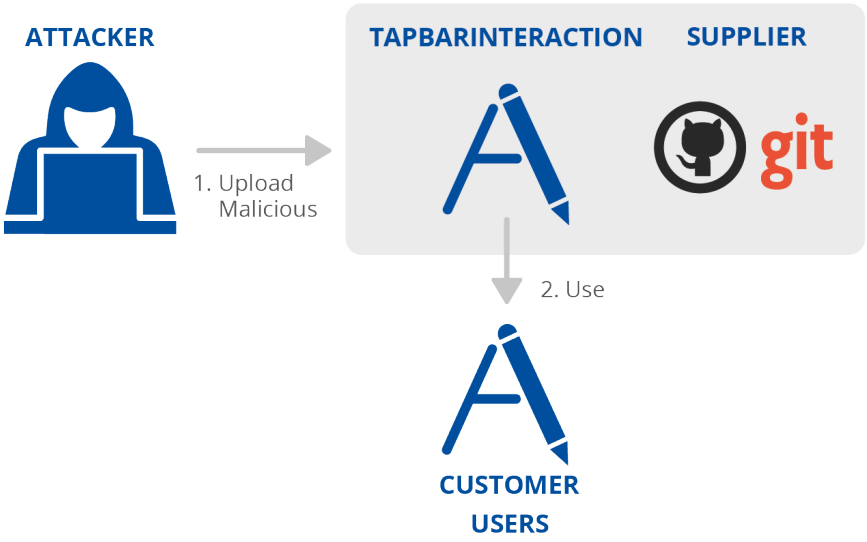
A.12 APPLE XCODE: ENVIRONNEMENT DE DEVELOPPEMENT INTEGRE

Apple Xcode est un environnement de développement utilisé pour développer des applications OSX et iOS[91]. En mars 2021, des chercheurs ont signalé qu'un projet Xcode malveillant avait été utilisé pour infecter les développeurs de Xcode au moyen d'une porte dérobée[92]. Le projet Xcode malveillant était une copie d'un projet réel. Il a contaminé l'utilisateur en exploitant une faiblesse de Xcode qui a permis aux pirates de démarrer automatiquement un script lors du lancement du projet[92].

Cette attaque n'a été attribuée à aucun groupe et il est difficile de savoir si des clients ont jamais été attaqués[93]. Par ailleurs, il n'est pas établi clairement comment le projet Xcode trojanisé a été livré à des victimes potentielles, ou même s'il l'a été.

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Infection par logiciel malveillant	Inconnu



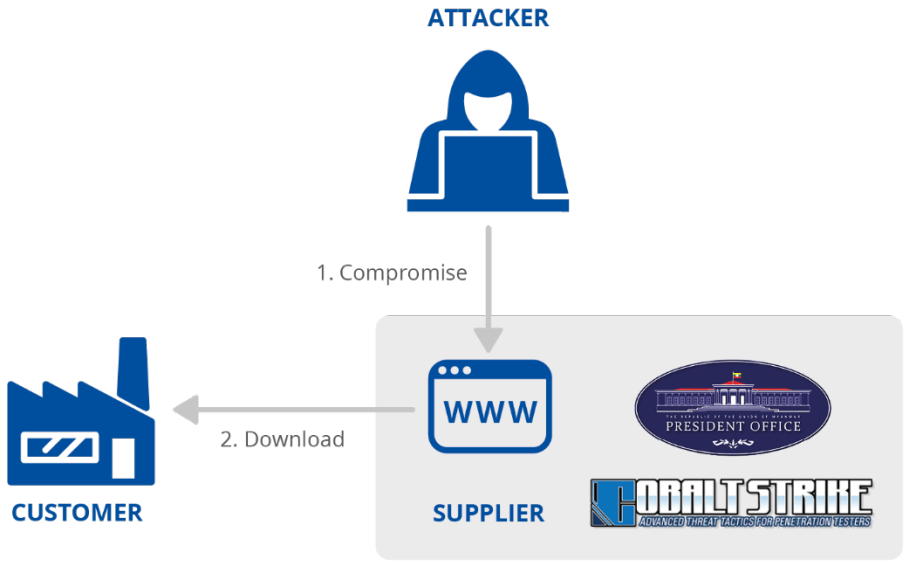
[91] Xcode 13 Overview, Apple Developer, https://developer.apple.com/xcode/. Consulté le 09/07/2021.
[92] New macOS Malware XcodeSpy Targets Xcode Developers with EggShell Backdoor, SentinelLabs, https://labs.sentinelone.com/new-macos-malware-xcodespy-targets-xcode-developers-with-eggshell-backdoor/, Consulté le 09/07/2021.
[93] XcodeSpy Mac Malware Targets Developers, SecureMac, https://www.securemac.com/news/xcodespy-mac-malware-targets-developers. Consulté 09/07/2021.

A.13 SITE WEB DE LA PRESIDENCE DU MYANMAR

En juin 2021, des chercheurs ont indiqué que les ressources hébergées sur le site web de la présidence du Myanmar avaient été trojanisées pour fournir un logiciel malveillant[94]. L'attaque n'a pas été officiellement attribuée à un groupe ATP spécifique[95], mais des ressemblances avec le groupe APT Mustang Panda ont été mises en évidence[94,96].

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Hameçonnage [T1566], Infection par logiciel malveillant	Personnes



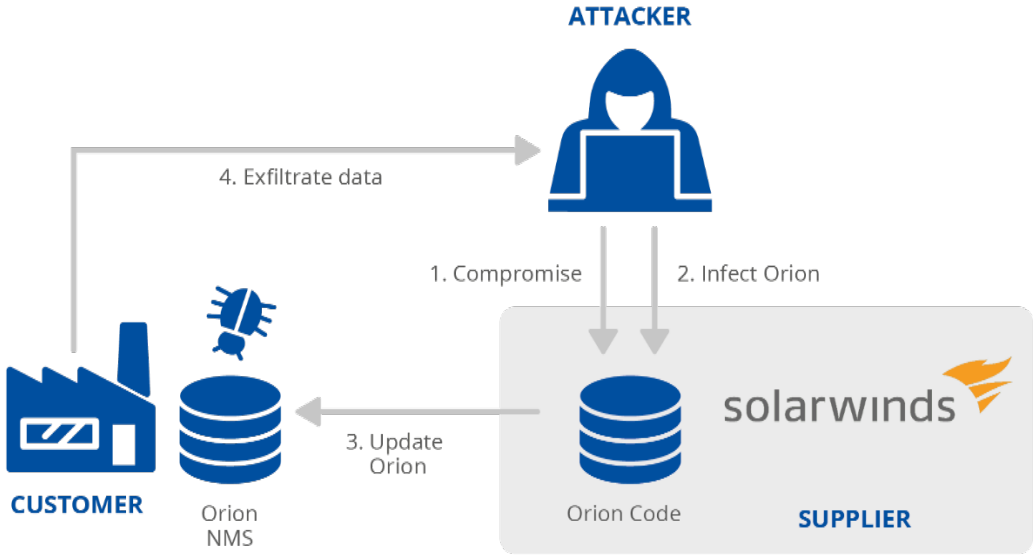
[94] "ESETresearch uncovered a supply chain attack on the Myanmar president office website", Twitter, https://twitter.com/ESETresearch/status/1400165767488970764. Consulté le 09/07/2021.
[95] Backdoor malware found on the Myanmar president's website, again, The Record by Recorded Future, https://therecord.media/backdoor-malware-found-on-the-myanmar-presidents-website-again/. Consulté le 09/07/2021.
[96] Cobalt Strike Beacons Being Hosted on Myanmar President's Website, Binary Defense, https://www.binarydefense.com/threat_watch/cobalt-strike-beacons-being-hosted-on-myanmar-presidents-website/. Consulté le 09/07/2021.

A.14 SOLARWINDS ORION: GESTION INFORMATIQUE ET TELESURVEILLANCE

SolarWinds est une société qui propose des logiciels de gestion et de surveillance[97]. Orion est le produit du système de gestion réseau (NMS) de SolarWinds[98]. En décembre 2020, on a découvert qu'Orion avait été victime d'une attaque. Une enquête approfondie a montré que les pirates avaient eu accès au réseau de SolarWinds, éventuellement par exploitation d'une vulnérabilité jour zéro dans une application ou un dispositif tiers, par attaque par force brute ou par ingénierie sociale[99]. Une fois l'attaque lancée, les pirates ont recueilli des informations pendant une période prolongée.

Après la compromission, un logiciel malveillant a été injecté dans le processus de construction d'Orion[99,100]. Le logiciel compromis a ensuite été directement téléchargé et exécuté par les clients, puis a été utilisé pour recueillir et voler des informations[101,102]. L'attaque a été attribuée au groupe APT29[103].

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Exploitation d'une vulnérabilité de logiciel, Attaque par force brute, Ingénierie sociale	Processus, Code	Relation de confiance [T1199], Infection par logiciel malveillant	Données



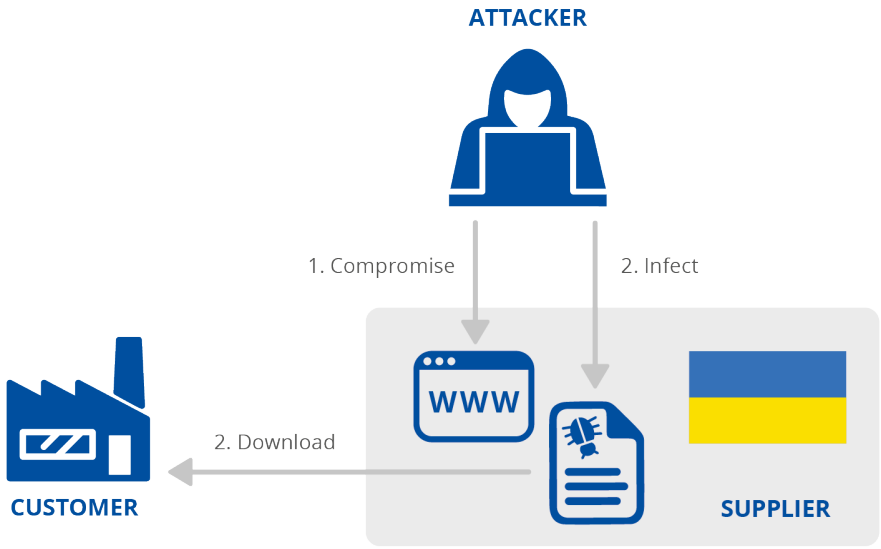
[97] What You Need To Know About the SolarWinds Supply-Chain Attack, SANS Institute, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. Consulté le 09/07/2021.
[98] Orion Platform, SolarWinds, https://www.solarwinds.com/solutions/orion. Consulté le 09/07/2021.
[99] An Investigative Update of the Cyberattack, Orange Matter, https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/. Consulté le 09/07/2021.
[100] SUNSPOT Malware: A Technical Analysis, CrowdStrike, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. Consulté le 09/07/2021.
[101] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, ireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. Consulté le 09/07/2021.
[102] SUNBURST Additional Technical Details, FireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html. Consulté le 09/07/2021.
[103] SolarWinds: Advancing the Story, RiskIQ Community Edition, https://community.riskiq.com/article/9a515637. Consulté le 09/07/2021.

A.15 UKRAINE SEI EB: SYSTEME D'INTERACTION ELECTRONIQUE DES ORGANISMES EXECUTIFS

Le gouvernement et les pouvoirs publics ukrainiens utilisent le système d'interaction électronique des organismes exécutifs (SEI EB), un portail web conçu pour échanger des documents[104]. En février 2021, on a signalé que le système avait été compromis par des pirates ayant réussi à charger des documents malveillants sur le portail[105]. Les documents malveillants auraient par la suite infecté les utilisateurs par des logiciels malveillants conçus pour recueillir et voler des informations. L'attaque a été attribuée à divers groupes APT, mais non à un seul groupe particulier[104].

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Infection par logiciel malveillant	Personnes, Données



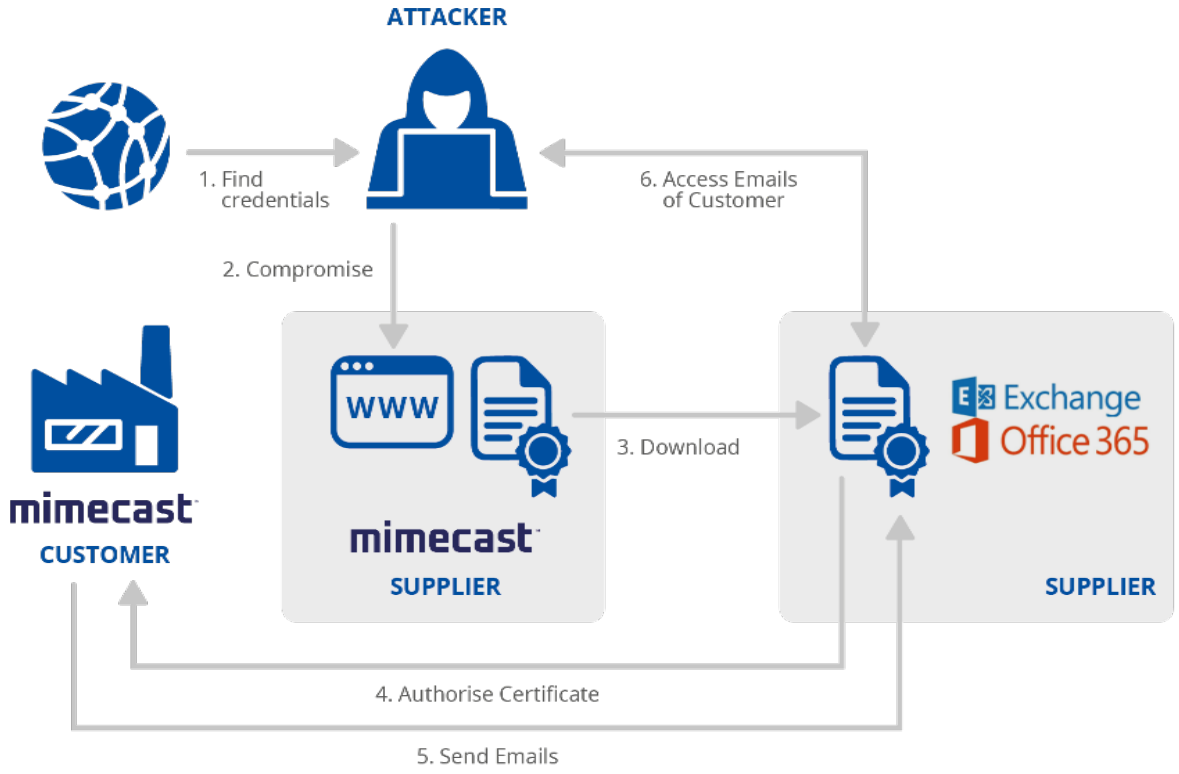
[104] Russian hackers aim cyber attack on Ukrainian government agencies, Teiss News, https://www.teiss.co.uk/russian-hackers-targeting-ukrainian-government-agencies/. Consulté le 09/07/2021.
[105] The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies, National Security and Defense Council of Ukraine, https://www.rnbo.gov.ua/en/Diialnist/4823.html. Consulté le 09/07/2021.

A.16 MIMECAST: SERVICES CLOUD DE CYBERSECURITE

Mimecast est un fournisseur de services cloud de cybersécurité[106]. Mimecast propose, entre autres, des services de sécurité des courriers électroniques, qui exigent des clients qu'ils se connectent de manière sécurisée aux serveurs Mimecast pour utiliser leurs comptes Microsoft 365. En janvier 2021, on a découvert que des pirates avaient compromis Mimecast (par l'intermédiaire du fournisseur SolarWinds). Après cette attaque, les pirates ont pu accéder à un certificat délivré par Mimecast et utilisé par les clients pour accéder aux services Microsoft 365, ce qui leur a permis d'intercepter les connexions réseau et de se connecter aux comptes Microsoft 365 pour voler des informations[107,108]. L'attaque a été attribuée au groupe APT29[109]. La compromission du fournisseur a été liée à SolarWinds, mais il n'existe pas d'informations fiables sur la manière dont cela s'est produit.

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Données

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Relation de confiance [T1199]	Données



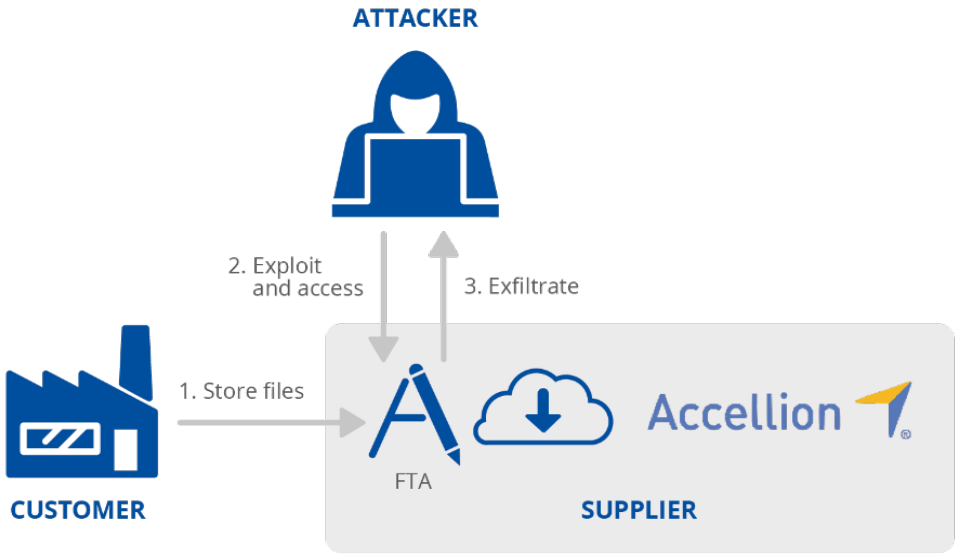
[106] Our Company, Mimecast, https://www.mimecast.com/company/. Consulté le 09/07/2021.
[107] Important Update from Mimecast, Mimecast Blog, https://www.mimecast.com/blog/important-update-from-mimecast/. Consulté le 09/07/2021.
[108] Mimecast Certificate Hacked in Supply-Chain Attack, Threatpost, https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/. Consulté le 09/07/2021.
[109] Important Security Update, Mimecast Blog, https://www.mimecast.com/blog/important-security-update/. Consulté le 09/07/2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A.17 ACCELLION: LOGICIEL DE TRANSFERT DE FICHIERS (FTA)

Accellion est une société qui fournit des logiciels de sécurité aux entreprises, en particulier des applications pour le partage sécurisé de fichiers et la collaboration[110]. En décembre 2020, Accellion a indiqué que des pirates avaient exploité de multiples vulnérabilités jour zéro dans son logiciel de transfert de fichiers (FTA) pour accéder aux archives des clients[111,112] et les extraire à l'aide d'un code encoquillé (webshell). De nombreuses entreprises touchées par ces vulnérabilités ont été extorquées après que des pirates ont menacé de publier leurs dossiers volés. L'attaque a été attribuée à un groupe de cybercriminalité connu sous le nom de UNC2546[112].

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Exploitation d'une vulnérabilité de logiciel	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Relation de confiance [T1199]	Données



[110] About Accellion, Accellion, https://www.accellion.com/company/. Consulté le 09/07/2021.
[111] File Transfer Appliance (FTA) Security Assessment, Accellion, https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf. Consulté le 09/07/2021.
[112] Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion, FireEye Inc, https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html. Consulté le on 09/07/2021.

A.18 SYSTEME DE SERVICE DE PASSAGERS DE SITA

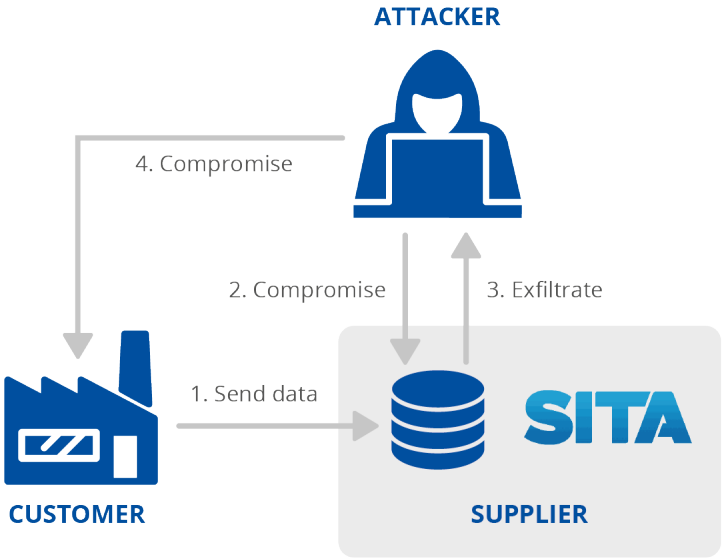
SITA est une société spécialisée dans les technologies de l'information aérienne et les informations relatives aux transports[113]. Le système de services de passagers de SITA est utilisé pour fournir aux compagnies aériennes des informations sur les passagers au moment de l'embarquement, y compris les risques que les passagers peuvent présenter dans un pays donné[114]. En mars 2021, il a été révélé que des pirates avaient compromis les serveurs de SITA pour accéder aux données passagers que possédaient des clients de SITA. Certains clients de SITA ont également signalé des violations de données, comme Air India, Singapore Airlines et Malaysia Airlines.

À la suite d'informations faisant état de fuites de données sur l'internet, Air India a également signalé que ses réseaux étaient compromis et que des données avaient été volées. La compromission des réseaux internes d'Air India serait liée à l'incident de SITA; en effet une société de sécurité aurait constaté que le nom d'un ordinateur au sein d'Air India était «SITASERVER4».

À ce jour, on ignore comment les pirates ont eu accès aux serveurs de SITA et on ne sait pas non plus comment ils ont pu accéder à Air India, ni s'ils l'ont effectivement fait. L'attaque interne contre les réseaux d'Air India a été attribuée au groupe APT41[115].

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Données

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Données à caractère personnel



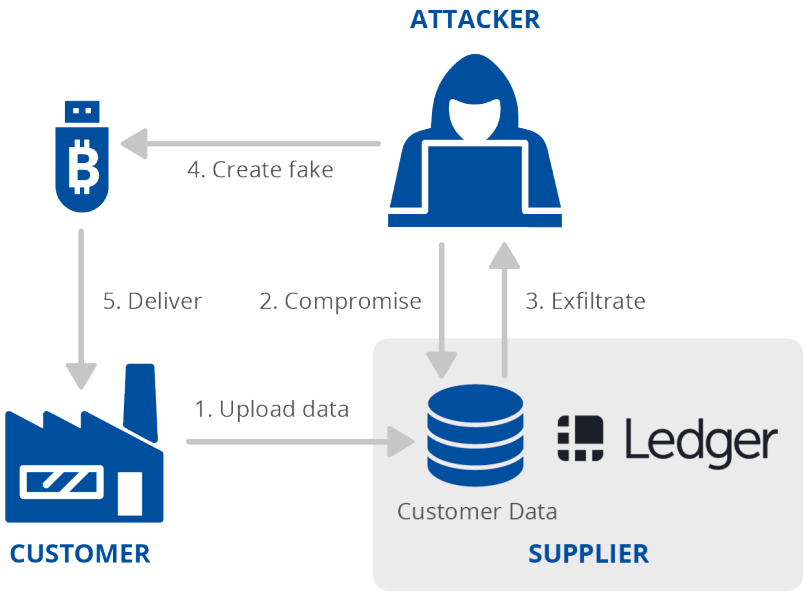
[113] About us, SITA, https://www.sita.aero/about-us/. Consulté le 09/07/2021.
[114] SITA Advance Passenger Processing, SITA, https://www.sita.aero/solutions/sita-at-borders/border-management/sita-advance-passenger-processing/. Consulté le 09/07/2021.
[115] Big airline heist: APT41 likely behind massive supply chain attack, Group-IB, https://blog.group-ib.com/colunmtk_apt41. Consulté le 09/07/2021.

A.19 LEDGER: PORTEFEUILLE DE CRYPTOMONNAIES

Ledger est une société qui propose une technologie de portefeuille de cryptomonnaies[116]. En juillet 2020, des pirates ont obtenu des identifiants valides pour accéder à la base de données de commerce électronique Ledger[117]. La manière dont les pirates ont accédé à ces identifiants est inconnue. Les données volées ont été publiées sur un forum en ligne[118].

Les auteurs de l'attaque ont utilisé les données volées pour hameçonner et extorquer des utilisateurs en ligne[119,120], et pour voler l'argent des utilisateurs au moyen d'une attaque physique après avoir fourni aux utilisateurs des portefeuilles Ledger contrefaits qui, lorsqu'ils étaient connectés à un ordinateur et demandaient aux utilisateurs leurs clés de sécurité, infecteraient l'ordinateur d'un logiciel malveillant et renverraient les informations volées aux pirates[121]. L'attaque n'a pas été attribuée à un groupe.

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Données	Relation de confiance [T1199], Hameçonnage [T1566], Contrefaçon	Finances



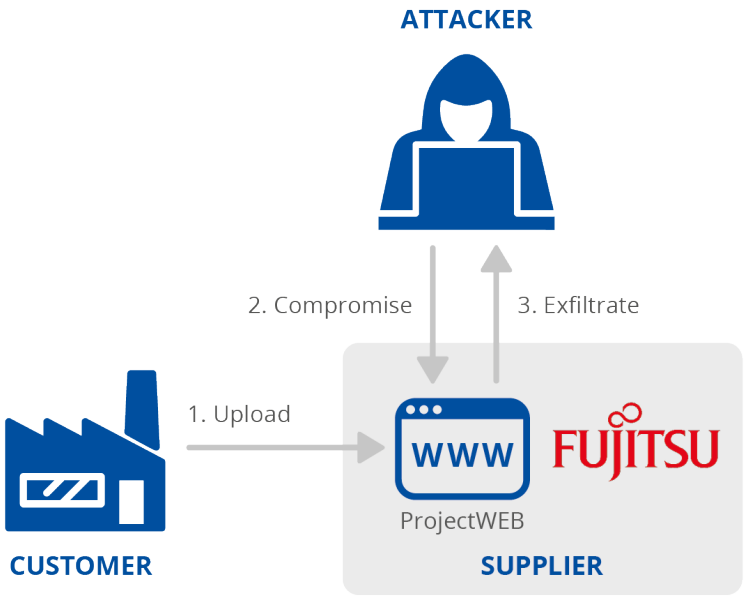
[116] Hardware Wallet, Ledger, https://www.ledger.com/. Consulté le 09/07/2021.
[117] Addressing the July 2020 e-commerce and marketing data breach -- A Message From Ledger's Leadership | Ledger, https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach. Consulté le 09/07/2021.
[118] Hackers Leak Customer Info From Crypto Wallet Ledger, Investopedia, https://www.investopedia.com/hackers-leak-customer-info-from-crypto-wallet-ledger-5093577. Consulté le 09/07/2021.
[119] Message by LEDGER's CEO - Update on the July data breach. Despite the leak, your crypto assets are safe, Ledger, https://www.ledger.com/message-ledgers-ceo-data-leak. Consulté le 09/07/2021.
[120] Threat Actors Target Ledger Data Breach Victims in New Extortion Campaign, HOTforSecurity, https://web.archive.org/web/20210520120353/https://hotforsecurity.bitdefender.com/blog/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign-25820.html. Consulté le 09/07/2021.
[121] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq, https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17. Consulté le 09/07/2021.

A.20 FUJITSU PROJECTWEB: LOGICIEL DE COLLABORATION ET DE GESTION DE PROJET

Fujitsu ProjectWEB est un logiciel cloud utilisé par les entreprises pour la collaboration en ligne, la gestion de logiciels et le partage de fichiers[122]. Cet outil est populaire auprès des agences gouvernementales japonaises. En mai 2021, des pirates ont eu accès aux données du gouvernement japonais[123] après avoir exploité les faiblesses des installations de ProjectWEB[122,124]. En raison de la localisation des serveurs compromis, les données du contrôle du trafic aérien japonais ont également été volées lors de l'attaque[122,125]. L'attaque n'a pas été attribuée à un groupe.

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code, Données

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Données



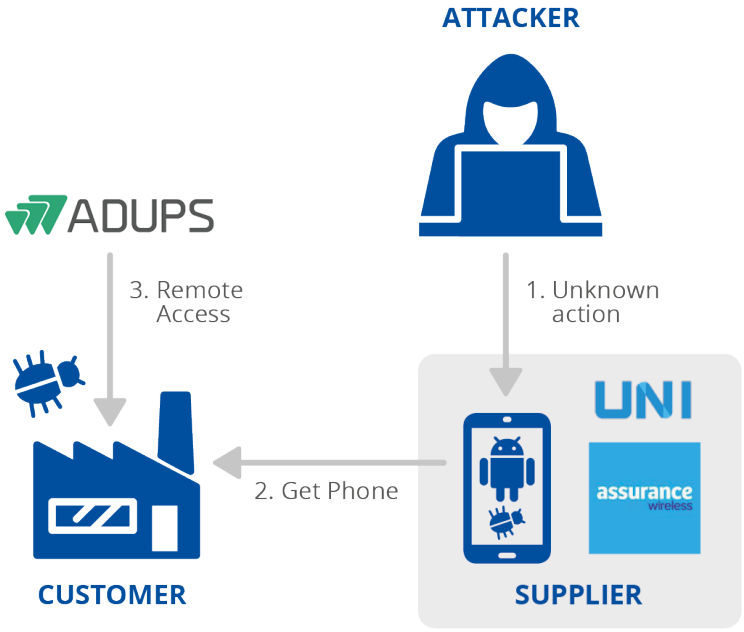
[122] Japanese government agencies suffered breaches after ProjectWEB hack, Teiss News, https://www.teiss.co.uk/japanese-government-agencies-suffered-breaches-following-fujitsus-projectweb-hack/. Consulté le 09/07/2021.
[123] Japanese government agencies suffer data breaches after Fujitsu hack, Bleeping Computer, https://www.bleepingcomputer.com/news/security/japanese-government-agencies-suffer-data-breaches-after-fujitsu-hack/. Consulté le 09/07/2021.
[124] Data theft via Fujitsu ProjectWEB, INCIBE-CERT, https://www.incibe-cert.es/en/early-warning/cybersecurity-highlights/data-theft-fujitsu-projectweb. Consulté le 09/07/2021.
[125] Fujitsu pulls ProjectWEB tool offline after apparent supply chain attack sees Japanese infosec agency data stolen, The Register, https://www.theregister.com/2021/05/27/fujitsu_projectweb_supply_chain_attack/. Consulté le 09/07/2021.

A.21 TELEPHONES MOBILES DE COMMUNICATIONS UNIMAX

Unimax, également connu sous le nom d'UMX, fournit des appareils mobiles bon marché. Parmi les clients des téléphones UMX figuraient des personnes qui recevaient leur téléphone par l'intermédiaire du programme d'aide «Lifeline Assistance» du gouvernement des États-Unis[126]. En janvier 2020, des chercheurs ont indiqué que les appareils mobiles étaient équipés de logiciels malveillants permanents préinstallés conçus pour espionner les utilisateurs[127,128]. Il n'a pas été possible de retirer les logiciels malveillants, même avec une réinitialisation matérielle. Un autre fabricant de téléphones mobiles dotés du logiciel malveillant préchargé, Transsion, a jeté la faute sur un vendeur non identifié tout au long de la chaîne d'approvisionnement[126]. L'attaque n'a pas été attribuée à un groupe[126].

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Inconnu	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Relation de confiance [T1199], Infection par logiciel malveillant	Personnes



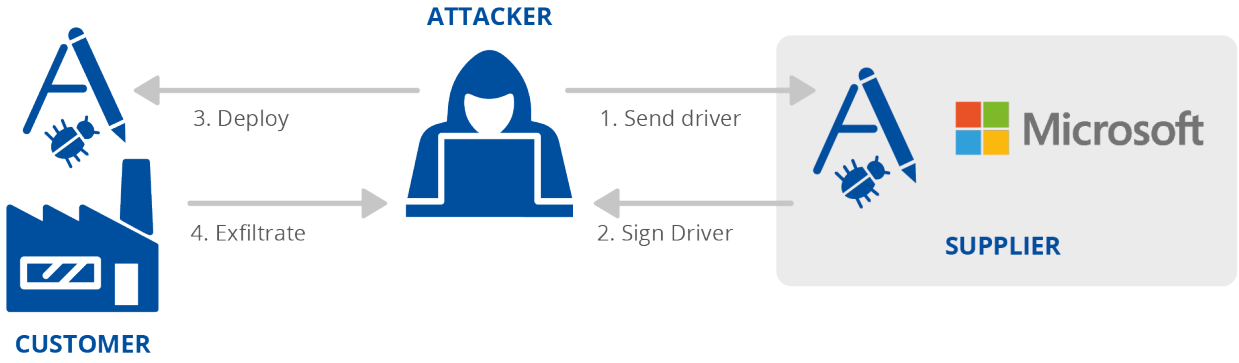
[126] Chinese Cell Phones Ship Preloaded with Malware, BlueVoyant, https://www.bluevoyant.com/blog/chinese-cell-phone-malware/. Consulté le 09/07/2021.
[127] UMX Phone: US-funded Gov Phones come pre-installed with malicious apps, Malwarebytes Labs, https://blog.malwarebytes.com/android/2020/01/united-states-government-funded-phones-come-pre-installed-with-unremovable-malware/. Consulté le 09/07/2021.
[128] We found yet another phone with pre-installed malware via the Lifeline Assistance program, Malwarebytes Labs, https://blog.malwarebytes.com/android/2020/07/we-found-yet-another-phone-with-pre-installed-malware-via-the-lifeline-assistance-program/. Consulté le 09/07/2021.

A.22 PROGRAMME DE COMPATIBILITE PHYSIQUE DE MICROSOFT WINDOWS

En juin 2021, il a été révélé que des pirates avaient abusé des processus de signature de code que Microsoft utilise pour valider des pilotes tiers afin de s'infiltrer et de distribuer un logiciel malveillant rootkit[129]. Grâce à une signature valide, le logiciel malveillant pouvait être installé dans les systèmes des utilisateurs[130]. L'attaque semblait viser le secteur des jeux en Chine[129]. Elle n'a pas été attribuée à un groupe.

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Ingénierie sociale	Processus

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Relation de confiance [T1199]	Données



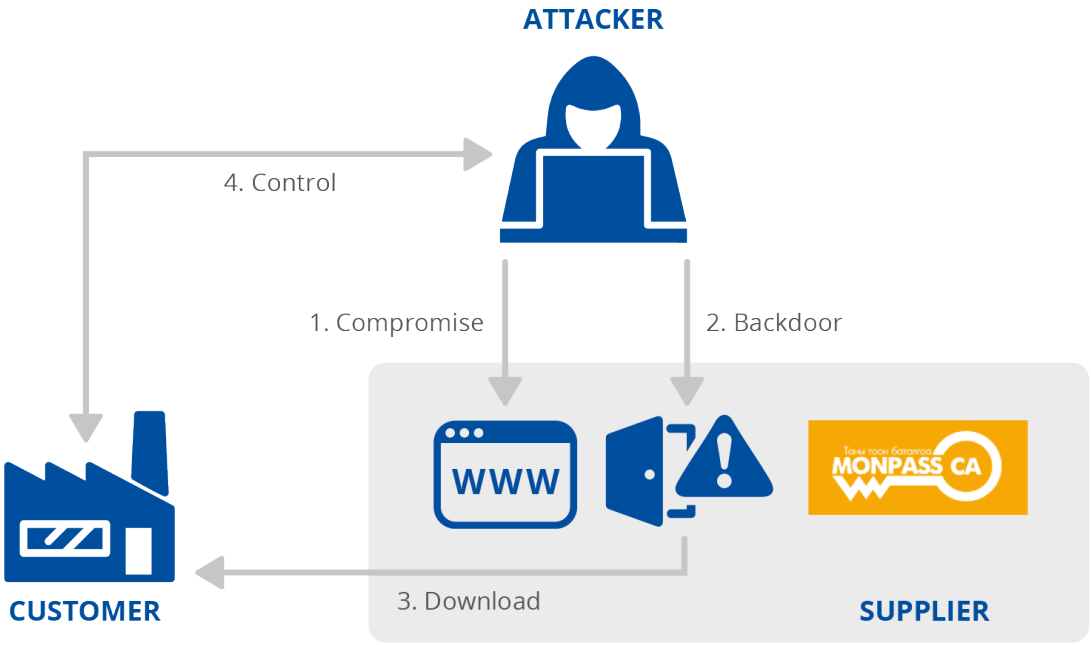
[129] Microsoft admits to signing rootkit malware in supply-chain fiasco, Bleeping Computer, https://www.bleepingcomputer.com/news/security/microsoft-admits-to-signing-rootkit-malware-in-supply-chain-fiasco/. Consulté le 09/07/2021.
[130] Microsoft signed a malicious Netfilter rootkit, G DATA, https://www.gdatasoftware.com/blog/microsoft-signed-a-malicious-netfilter-rootkit. Consulté le 09/07/2021.

A.23 ORGANISME DE CERTIFICATION MONPASS

MonPass est le principal organisme de certification de Mongolie. En février 2021, son site web a été compromis et au moins un installateur binaire reçu un binaire Cobalt Strike par porte dérobée[131]. Le site web a été mis en péril à plusieurs reprises et plusieurs codes encoquillés et portes dérobées ont été trouvés[132]. Le code malveillant a été téléchargé par les visiteurs sur le site web MonPass, qui a exécuté le logiciel malveillant lors du téléchargement. Avast Software a découvert qu'au moins un client a été infecté[131].

FOURNISSEUR	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement
Exploitation d'une vulnérabilité de logiciel	Code

CLIENT	
Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Compromission «drive-by» [T1189], Infection par logiciel malveillant	Inconnu

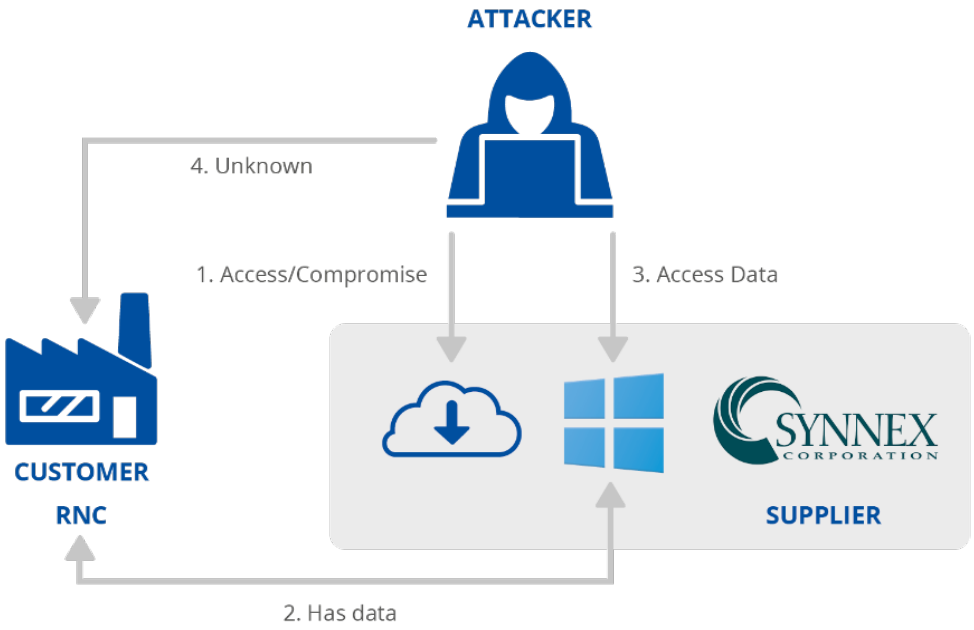


[131] Backdoored Client from Mongolian CA MonPass, Avast Threat Labs, https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/. Consulté le 09/07/2021.
[132] Mongolian Certificate Authority Hacked to Distribute Backdoored CA Software, The Hacker News, https://thehackernews.com/2021/07/mongolian-certificate-authority-hacked.html. Consulté le 09/07/2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A.24 SOCIETE DE CONCEPTION ET DE DISTRIBUTION INFORMATIQUES SYNNEX

Synnex est un distributeur et intégrateur technologique. En juillet 2021, ses systèmes ont fait l'objet d'une attaque[133]. Synnex a admis que les attaques pouvaient avoir été liées aux récentes attaques des MSP de Kaseya[134]. Les pirates ont utilisé Synnex pour accéder à des applications clients dans l'environnement informatique cloud de Microsoft. Parmi ces applications figurait celle du comité national du Parti républicain américain (RNC), qui a signalé avoir été victime d'une attaque par l'intermédiaire de Synnex[135].

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs du fournisseur ciblés par l'attaque de la chaîne d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Actifs du client ciblés par l'attaque de la chaîne d'approvisionnement
Exploitation d'une vulnérabilité de logiciel	Code	Compromission «drive-by» [T1189], Infection par logiciel malveillant	Inconnu



[133] Mega-distie SYNNEX attacked and Microsoft cloud accounts it tends tampered, The Register, https://www.theregister.com/2021/07/07/synnex_rnc_microsoft_attack/. Consulté le 09/07/2021.
[134] SYNNEX Responds to Recent Cybersecurity Attacks and Media Mentions, SYNNEX Corporation, https://ir.synnex.com/news/press-release-details/2021/SYNNEX-Responds-to-Recent-Cybersecurity-Attacks-and-Media-Mentions/default.aspx. Consulté le 09/07/2021.
[135] Russia 'Cozy Bear' Breached GOP as Ransomware Attack Hit, The Washington Post, https://www.washingtonpost.com/business/on-small-business/russia-cozy-bear-breached-gop-as-ransomware-attack-hit/2021/07/06/3e9e200a-de9b-11eb-a27f-8b294930e95b_story.html. Consulté le 09/07/2021.

TP-05-21-171-FR-N

À PROPOS DE L'ENISA

L'Agence européenne pour la cybersécurité (ENISA) est l'agence de l'Union européenne qui vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis informatiques de demain. Par le partage des connaissances, le renforcement des capacités et des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations sur l'ENISA et ses travaux, consultez le site suivant: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-509-8
DOI: 10.2824/168593