TLP:CLEAR

ILLUSTRATION DES PROBLÉMATIQUES LIÉES À L'INTÉGRATION DE LOGICIELS NON MAITRISÉS

LE CAS DE GOLDENSPY

Version 2022

23 novembre 2022

TLP:CLEAR

Sommaire

1 Intégration de logiciels non maitrisés

Les cadres réglementaires de certains pays peuvent imposer aux entreprises françaises implantées sur leur territoire l'utilisation de logiciels spécifiques. Si leur intégration ne pose généralement pas de problèmes techniques particuliers, ces logiciels peuvent poser des risques de sécurité. De plus, ils représentent une opportunité d'attaques pour des adversaires qui pourraient cibler spécifiquement ces logiciels dont l'utilisation est circonscrite géographiquement pour atteindre des entreprises dans un pays donné.

L'installation de certaines versions des logiciels chinois *GoldenTax* et de *Beijing One Pass*, détaillés ci-dessous, auraient entrainé l'ajout de fonctions utilisables comme porte dérobée. Les premières versions affectées de ces logiciels auraient été publiées dès 2018, mais la problématique qu'ils illustrent perdure. Ainsi, en 2022 des entreprises françaises implantées en Chine ont rapporté à l'ANSSI que l'installation de logiciels imposés entrainaient l'émission de multiples alertes par leurs solutions de sécurité. Cependant, à ce jour, aucune information n'a été publiée concernant l'exploitation éventuelle des accès ouverts par les codes GoldenSpy, GoldenHelper ou celui inclus dans certaines versions de *Beijing One Pass*. Les objectifs poursuivis par l'installation de ces portes dérobées ne sont ainsi pas connus, mais elles pourraient avoir été utilisées comme portes d'entrée pour des compromissions plus larges au sein des entreprises affectées.

Si l'ajout d'une fonctionnalité assimilable à une porte dérobée peut être le fait de son éditeur, celui-ci peut également être victime d'une attaque sur la chaîne d'approvisionnement visant à compromettre ses clients *via* ses logiciels. Le code de sabotage NotPetya a ainsi été distribué par une mise à jour malveillante du logiciel de comptabilité ukrainien M.E.Doc, alors utilisé par une majorité des entreprises opérant dans le pays [1]. Une compromission de l'autorité gouvernementale de certification du Vietnam en 2020 a également conduit à la distribution d'une version compromise d'un logiciel utilisé pour des signatures électroniques de documents [2].

1.1 GoldenSpy

Pour le traitement numérique des déclarations relatives à la taxe sur la valeur ajoutée (TVA), le gouvernement chinois a mis en œuvre le programme *Golden Tax*. Les entreprises opérant en Chine ont ainsi l'obligation d'utiliser le logiciel *Golden Tax* pour faire leurs déclarations de TVA. Le logiciel *Golden Tax* n'est cependant pas directement distribué par l'État, mais par deux entreprises, Baiwang et Aisino, qui intègrent celui-ci dans leurs produits. Il semble que la sélection de l'un ou l'autre de ces éditeurs soit décidée par les banques chinoises des entreprises.

Le 25 juin 2020, l'entreprise singapourienne de cybersécurité Trustwave a publié un rapport [3] révélant que l'installation du logiciel de gestion de TVA chinoise Aisino Intelligent Tax conduisait au déploiement de ce qui s'apparente à une porte dérobée, baptisée « GoldenSpy » par l'éditeur.

Deux heures après l'installation du logiciel de gestion de TVA, des codes sont téléchargés puis exécutés de manière silencieuse. Ils disposent de mécanismes de persistance, communiquent à une fréquence aléatoire avec un serveur distant et permettent d'exécuter des codes arbitraires avec un niveau de privilèges d'administrateur système sans interaction de l'utilisateur. La présence de GoldenSpy n'est pas mentionnée dans la documentation et **celui-ci persiste lors de la désinstallation du logiciel Aisino Intelligent Tax.**

Selon les analyses de Trustwave, la distribution de GoldenSpy aurait débuté en avril 2020. Mais le 28 juin 2020, alors que la publication de l'éditeur a bénéficié d'un large écho, un nouveau code est téléchargé et exécuté de manière silencieuse par le logiciel Aisino Intelligent Tax. Ce code a pour effet de désinstaller GoldenSpy et d'effacer toutes les traces de sa présence sur la machine [4]. Enfin, à partir du 1er juillet, une nouvelle version du code de désinstallation est envoyée, comprenant une modification qui semble être destinée à éviter d'être détectée par les règles YARA publiées par Trustwave [5].

GoldenSpy n'est pas le premier code suspect à avoir été distribué en parallèle de suites logicielles associées à *Golden Tax*.

Une quatrième publication de Trustwave [6] détaille une campagne active de janvier 2018 à juillet 2019 et im-

pliquant un code distinct, baptisé « GoldenHelper ». Celui-ci aurait été intégré au logiciel *Golden Tax Invoicing software (Baiwang Edition)* qui, bien qu'il soit chargé de transmettre les informations fiscales à l'infrastructure administrée par Baiwang, est un logiciel édité par une filiale d'Aisino. Bien que la charge finale n'ait pas été étudiée par Trustwave, son analyse de GoldenHelper permet de déterminer que le téléchargement de celle-ci s'effectue depuis différentes sources, qu'elle est enregistrée dans des répertoires variables et que son exécution se fait avec des privilèges d'administrateur système sans déclenchement d'alerte utilisateur (*UAC bypass*). De tels mécanismes ne correspondent pas à des fonctionnalités attendues sur un logiciel légitime de gestion de TVA, mais sont courants pour des portes dérobées.

Trustwave rapporte également des cas de fourniture de stations de travail physiques destinées à l'utilisation de *Golden Tax* sur lesquelles le code GoldenHelper aurait été présent dès la livraison [6].

Plusieurs entreprises françaises ayant des activités en République populaire de Chine ont rapporté avoir détecté la présence de GoldenSpy sur leurs systèmes d'information.

Des indicateurs de compromission ont été publiés dans les rapports Trustwave mentionnés en bibliographie.

1.2 Beijing One Pass

En juillet 2021, l'éditeur Recorded Future a publié un rapport affirmant que le logiciel *Beijing One Pass* présentait également des fonctionnalités susceptibles d'être utilisées comme porte dérobée [7]. Ce logiciel, distribué par l'entreprise publique Beijing Certificate Authority, est destiné à faciliter l'accès à un catalogue de services accordés aux entreprises par la municipalité de Pékin.

2 Recommandations

Au-delà des situations illustrées par les codes malveillants précités, l'installation d'un « logiciel de moindre confiance » peut exposer les actifs métiers et le système d'information (SI) d'une entité à de nombreuses menaces. Afin de limiter l'impact de ces menaces, il convient de respecter plusieurs recommandations pour contenir le logiciel dans une zone isolée et dédiée à cet usage. Ces recommandations portent sur les thèmes suivants :

- Infrastructure ;
- Accès au logiciel ;
- Maintien en conditions de sécurité ;
- Détection.

De plus, il est recommandé de mettre à jour la cartographie du SI pour faciliter le contrôle de la zone cloisonnée et l'identification des chemins de compromission potentiels.

2.1 Infrastructure

R1

Installer le logiciel dans une zone isolée

Il est recommandé d'installer le logiciel dans une zone isolée du SI de l'entité et de préférence avec des équipements dédiés et affectés à cet usage.

R2

Filtrer les flux réseau « depuis » et « vers » la zone isolée au juste besoin opérationnel

Les flux réseaux depuis et vers la zone isolée doivent être filtrés par un pare-feu afin de limiter au juste besoin opérationnel les communications à des adresses ou plages d'adresses IP définies. À noter que les flux de la zone isolée vers le SI de l'entité sont dans la mesure du possible à prohiber.

R3

Filtrer les flux avec un équipement pare-feu distinct de la machine sur laquelle le logiciel est installé

Un pare-feu autre que celui de la machine sur lequel le logiciel est installé doit être utilisé pour filtrer les flux. L'objectif est d'éviter que le logiciel soit en capacité de désactiver le pare-feu s'il parvient à élever ses privilèges.

Isoler une zone dans un SI « on-premise » est une tâche qui peut s'avérer chronophage ou complexe si l'urbanisation du SI n'a pas prévu ce cas. Lorsque qu'une connexion vers le SI interne n'est pas nécessaire, l'externalisation (par exemple usage d'un service Cloud) dans une zone isolée et dédiée est une option envisageable lorsque la sensibilité de la donnée manipulée le permet. Les recommandations suivantes doivent être observées.

R4

Utiliser un compte Cloud dédié pour isoler la zone de moindre confiance

Si l'usage d'un Cloud est retenu pour mettre en place une zone isolée, il est recommandé d'utiliser un compte dédié. L'objectif est de limiter les risques d'élévation de privilège depuis la zone d'installation du logiciel pouvant affecter d'autres ressources, mais aussi d'éviter tout déplacement latéral sur d'autres ressources instanciées sans rapport avec le logiciel.

La zone isolée ne doit pas utiliser les services d'infrastructure communs (système d'authentification, DNS, etc.). L'objectif est d'éviter une compromission ou un potentiel déni de service en prohibant tout accès aux services du SI interne de l'entité.

R5

Appliquer le principe de moindre privilège sur l'ensemble des services et équipements

Les comptes utilisés doivent posséder des privilèges les plus réduits possibles, adaptés à chaque opération d'exploitation et d'administration de la zone isolée. Dans la mesure du possible, le logiciel ne doit pas s'exécuter avec un compte possédant les droits administrateurs. De façon générale, les comptes utilisateurs et administrateurs doivent s'appuyer sur des comptes locaux.

2.2 Accès au logiciel

L'accès au logiciel se fait par un accès direct à la machine sur laquelle le logiciel est installé. Dans les cas où l'utilisateur doit interagir à distance avec la zone isolée, il est préférable d'utiliser une solution d'accès à distance (qui peut être un service Cloud) avec les précautions suivantes.

R6

Désactiver le partage du presse-papier et la redirection de disque

Le partage du presse-papier et la redirection de disques dans les solutions de déport d'affichage doivent être désactivés.

Lorsque l'échange de fichiers entre le SI interne et la machine hébergeant le logiciel est nécessaire, alors une zone de stockage partagée peut être envisagée si elle est hébergée dans la zone isolée.

R7

Configurer un partage de fichier dédié et isolé

Lorsqu'une zone de stockage entre le SI interne et la zone isolée est nécessaire, elle doit être mise en place dans la zone isolée. Une alternative possible est l'usage d'un service SaaS dans un Cloud, qui rend de fait la zone de stockage séparée du SI interne.

2.3 Maintien en conditions de sécurité

Bien que la zone soit isolée du SI de l'entité, le maintien en condition de sécurité des composants logiciels et matériels s'avère important. L'administration de cette zone isolée, limitée à un faible nombre d'équipements, se fera

manuellement, directement sur les équipements ou depuis un poste dédié à cet usage.

R8

Réaliser le maintien en condition de sécurité depuis Internet

Les dépôts nécessaires au maintien en condition de sécurité (MCS) de la zone isolée ne doivent pas communiquer avec le SI de l'entité, mais doivent accéder aux mises à jour directement sur Internet. Les règles de pare-feu doivent autoriser les flux réseaux nécessaires au MCS de façon stricte.

Lorsque le besoin d'utilisation du logiciel est peu fréquent, des mesures complémentaires peuvent être mises place pour limiter l'exposition de la zone isolée.

R9

Eteindre le service lorsqu'il n'est pas utilisé

Il est recommandé d'éteindre le service lorsqu'il n'est pas utilisé.

2.4 Détection

La journalisation des événements est un prérequis pour mettre en œuvre une capacité de détection et d'analyse post-incident. Pour plus d'information sur les bonnes pratiques de journalisation en fonction de la confiance entre plusieurs zones, se reporter au guide ANSSI portant sur les « recommandations de sécurité pour l'architecture d'un système de journalisation » [8].

R10

Activer et configurer la journalisation

La journalisation des composants systèmes et réseau de la zone isolée doit être activée et configurée afin de détecter et d'analyser les incidents de sécurité. Cette journalisation est complétée par l'analyse des événements des pare-feu situés en bordure de la zone isolée.

R11

Mettre en place un collecteur de logs dédié dans la zone isolée

Il est recommandé de centraliser les logs *via* un collecteur dédié en zone isolée et de régulièrement récupérer ces journaux depuis le SI interne de l'entité. Ainsi, seul le SI interne initie des connexions vers la zone de moindre confiance, et non l'inverse.

3 Bibliographie

[1] ESET. *Analysis of TeleBots' Cunning Backdoor*. 4 juillet 2017.
URL : https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/.

[2] ESET. *Operation SignSight : Supply chain Attack against a Certification Authority in Southeast Asia*. 17 décembre 2020.
URL : https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/.

[3] TRUSTWAVE. *The Golden Tax Department and the Emergence of GoldenSpy Malware*. 25 juin 2020.
URL : https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/.

[4] TRUSTWAVE. *GoldenSpy : Chapter Two – The Uninstaller*. 30 juin 2020.
URL : https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-two-the-uninstaller/.

[5] TRUSTWAVE. *GoldenSpy Chapter 3 : New and Improved Uninstaller*. 2 juillet 2020.
URL : https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-3-new-and-improved-uninstaller/.

[6] TRUSTWAVE. *GoldenSpy Chapter 4 : GoldenHelper Malware Embedded in Official Golden Tax Software*. 14 juillet 2020.
URL : https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/.

[7] RECORDED FUTURE. « "Beijing One Pass" Employee Benefits Software Exhibits Spyware Characteristics ». 29 juillet 2021.
URL : https://go.recordedfuture.com/hubfs/reports/cta-2021-0729.pdf.

[8] ANSSI. *Publication : Recommandations de sécurité pour l'architecture d'un système de journalisation*. 28 janvier 2022.
URL : https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/.

Version 2022 - 23 novembre 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
cert.ssi.gouv.fr / cert-fr@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité