PREMIÈRE MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 05/02/2024
N°

Recherche de marqueurs d'utilisation d'AnyDesk

Communication relative à l'incident chez AnyDesk

ANSSI/SDO
05/02/2024

TLP:CLEAR

Version : 1.0
Nombre de pages : 6

Niveau de diffusion

TLP:CLEAR	Pas de restriction, partage libre entre les différentes communautés (publication large, y compris Internet)

Message

Ce document est une notice d'utilisation de l'outil FastFind développé par l'ANSSI et partagé dans le cadre d'une communication concernant les logiciels de la société AnyDesk.

Vous trouverez dans les pages suivantes des instructions plus détaillées et, en pièce jointe, une procédure technique.

1 Contexte

L'outil FastFind présenté dans cette documentation vous permet de rechercher des marqueurs indiquant la présence, l'exécution ou l'installation d'AnyDesk sur un système d'exploitation Windows.

Ces marqueurs ne sont pas des indicateurs de compromission : ils ne révèlent par une compromission avérée d'un système d'information.

L'analyse des résultats détaillée plus bas dans ce document a pour but d'aider à qualifier l'utilisation d'AnyDesk sur un système d'information. Ces éléments pourront ensuite permettre de prendre les mesures nécessaires en accord avec les risques identifiés.

2 Outil de recherche FastFind

2.1 Présentation de l'outil

Un fichier exécutable a dû vous être transmis en même temps que les présents documents. Ce programme est l'outil FastFind.

2.1.1 Principes

L'outil FastFind est un outil de recherche de traces sur des ordinateurs utilisant le système d'exploitation Microsoft Windows.

Le logiciel contient la description de marqueurs à rechercher. A l'exécution, il va parcourir tout le disque de la machine examinée à la recherche de marqueurs précis. Au terme de la recherche, le programme produit un rapport indiquant les traces éventuelles découvertes.

Régulièrement utilisé dans des traitements d'incident, l'outil a été déployé sur des parcs de quelques machines à plusieurs dizaines de milliers de postes et serveurs.

Le FastFind a été publié en logiciel libre par l'ANSSI avec la suite d'outils DFIR-Orc.
Il vous est donc possible d'en inspecter le code source qui peut être trouvé à l'adresse : `https://github.com/dfir-orc`.

Les informations contenues dans l'outil sont adaptées spécifiquement dans le cadre de cette campagne, Ils vous est demandé de ne pas le diffuser et de ne pas le téléverser sur les sites d'antivirus en ligne.

2.1.2 Usage de l'outil

Il suffit de l'exécuter avec un compte privilégié pour déclencher la recherche.

Suivant le nombre de fichiers présents, l'ancienneté du système examiné et ses performances, la recherche peut prendre de quelques minutes à 5 heures. Afin de ne pas perturber le fonctionnement du système d'information, FastFind est écrit pour s'exécuter de manière non prioritaire.

La recherche génère une liste de fichiers ou d'entrées suspects accompagnée de rapports sur le contexte d'exécution (description technique du poste analysé, et journal d'exécution). Cette liste est stockée sous forme de fichiers textes dans des archives non chiffrées au format 7z.

L'outil dispose de fonctions intégrées permettant de transférer automatiquement les résultats vers un partage de fichier ou un serveur BITS. Ces fonctions sont surtout utiles dans des campagnes de grande ampleur couvrant des milliers de postes et serveurs.

Le traitement de ces informations permet de détecter la présence d'éléments caractéristiques d'une attaque ou de l'exécution d'un logiciel malveillant spécifique.

2.2 Déploiement

Si vous exécutez l'outil manuellement, il suffit pour cela de l'exécuter sur la machine à analyser et de récupérer les fichiers générés en fin d'exécution dans le répertoire courant. Cette façon d'opérer n'est généralement pas pratique au delà d'une poignée de machines.

Pour effectuer plus efficacement la recherche avec FastFind, vous pouvez utiliser vos outils d'administration habituels : Powershell, taches programmées à distance, orchestrateurs ou outils de gestion de parc. La seule difficulté éventuelle est généralement la récupération des résultats.

Si vos outils ne le permettent pas directement, FastFind propose plusieurs options pour téléverser automatiquement les résultats vers des partages de fichiers SMB ou des serveurs BITS.

Cependant, sur un parc important géré par un domaine Active Directory, le plus simple est souvent d'utiliser des Stratégies de Groupe(GPO). Dans ce cas, il est possible de mettre en place un partage de fichier destiné à la collecte des résultats. On peut alors créer par GPO des taches à exécution immédiate pour déployer l'outil sur tout un système d'information.

Vous trouverez en annexe un document détaillant une procédure de déploiement utilisant ce mécanisme.

Dans tous les cas, il convient d'exécuter l'outil avec un compte *Administrateur local* ou membre d'un groupe *Administrateurs systèmes* des machines à examiner et d'éviter d'utiliser un compte *Administrateur de domaine* de l'Active Directory.

Pour plus de détails, une documentation complète de l'outil peut être trouvée à l'adresse : `https://dfir-orc.github.io/FastFind.html`.

3 Traitement des résultats

Quand vous avez collecté les résultats de recherche, vous pouvez qualifier les éléments afin de savoir quels marqueurs FastFind ont été retrouvés.

Il est fortement recommandé de mettre ces résultats sous séquestre afin de favoriser d'éventuels futurs traitements.

3.1 Examen manuel des résultats

Les résultats d'exécution sont dans des formats ouverts permettant de s'assurer des informations qui y figurent.

Les fichiers résultants sont des archives compressées au format 7Zip. Ils peuvent être ouverts avec l'outil libre du même nom `https://www.7-zip.org/`.

Si vous décompressez l'archive, vous pourrez inspecter le fichier `FastFind_result.xml` en l'ouvrant dans n'importe quel éditeur de texte. Le fichier est au format XML et peut facilement s'inspecter pour y constater les détections éventuelles.

Les autres fichiers présents dans l'archive donnent des informations sur la bonne exécution l'outil afin d'assister au diagnostic en cas d'éventuel disfonctionnement. Ils peuvent aussi être consultés dans un éditeur de texte.

3.1.1 Présence d'AnyDesk sur le système

Les résultats de recherche de marqueurs indiquant la présence d'AnyDesk sur le système se trouvent dans le fichier *FastFind_result.txt*.

Deux types d'entrées sont recherchées :

— Les fichiers présents sur le système (balise XML <*filesystem*>). Un fichier trouvé est décrit dans une balide <*record*> ;
— Les clés de registre (balise XML <*registry*>). Une clé de registre trouvée est décrite dans une balise <*regfind_match*> qui contient les valeurs du registre dans des balides enfant <*value*>.

Si le contenu du fichier *FastFind_result.txt* contient des entrées trouvées comme décrit ci-dessus, cela indique que des marqueurs de la présence d'AnyDesk sont présents sur votre système.

Plus de détails sur le contenu du fichier peuvent être trouvés à l'adresse `https://dfir-orc.github.io/FastFind.html`

3.1.2 Collecte des artefacts AnyDesk

Certains des artefacts laissés par AnyDesk sur le système sont collectés par FastFind (logs, configurations, binaire AnyDesk).

Le résultat de la collecte est présent dans une sous archive nommée *Artefacts.7z*.

3.1.3 Collecte de la signature des binaires

Les signatures de certains binaires sont également collectées et enregistrées dans l'archive *NTFSInfo_detail.7z*.

Cette archive contient un fichier csv qui liste différentes informations sur chaque ligne, notamment :

— Le nom de la machine ;
— Le chemin complet du fichier ;
— Les informations de signature du fichier.

Vous pouvez rechercher dans ce fichier les occurences de *Anydesk* et vérifier la valeur du champ *AuthenticodeSignerThumbprint* :

— Si la valeur est égale à *9cd1ddb78ed05282353b20cdfe8fa0a4fb6c1ece*, le binaire AnyDesk n'est pas celui mis à jour. Il est conseillé de le supprimer ou de le remplacer par la dernière version.
— Si la valeur est égale à *646f52926e01221c981490c8107c2f771679743a*, le binaire AnyDesk est bien celui mis à jour.

ANSSI/SDO
Version 1.0- 2024-02-05

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr