TLP:WHITE

ATTAQUES PAR LE RANÇONGICIEL MESPINOZA/PYSA

TLP:WHITE

Sommaire

1 Contexte

L'ANSSI a récemment été informée d'attaques informatiques visant notamment des collectivités territoriales françaises. Lors de ces attaques, des codes malveillants de type rançongiciel ont été utilisés, rendant certains fichiers inutilisables. L'origine de ces attaques est inconnue à ce jour, et des analyses sont actuellement en cours. Toutefois, les attaques par rançongiciels sont généralement conduites de manière opportuniste par des acteurs motivés par des objectifs lucratifs, et ce à l'encontre d'entités variées.

Le but de ce document est de décrire le mode opératoire utilisé lors de ces attaques et les indicateurs de compromission associés, puis de fournir des recommandations permettant de limiter l'impact de ce type d'incident.

2 Mode opératoire

La compromission présentée dans ce document a touché des systèmes d'information interconnectés, et semble utiliser principalement une variante d'un rançongiciel connu en source ouverte sous le nom de **Mespinoza**. Les éléments techniques exposés ci-après sont issus d'analyses en cours et sont susceptibles d'évoluer.

2.1 Le rançongiciel Mespinoza/Pysa

Le rançongiciel **Mespinoza** est utilisé depuis octobre 2018 au moins. Ses premières versions produisaient des fichiers chiffrés portant l'extension « `.locked` », commune à de nombreux rançongiciels. Depuis décembre 2019, une nouvelle version de **Mespinoza** est documentée en source ouverte, parfois appelée **Pysa** car elle produit des fichiers chiffrés portant l'extension « `.pysa` ».

2.1.1 Deux versions différentes

Le rançongiciel utilisé dans la présente attaque semble être une variante de **Pysa**. Deux versions en ont été découvertes lors des investigations :

- Un fichier exécutable nommé « `svchost.exe` ». Ce fichier était accompagné de plusieurs scripts *.bat* notamment chargés de copier l'exécutable dans le dossier « `C:\windows\temp` » (qui n'est pas l'emplacement légitime de l'hôte de service standard) et de l'exécuter.
- Une archive *Python* nommée « `17535.pyz` », contenant le code source *Python* du rançongiciel. La fonctionnalité de chiffrement s'appuie sur les bibliothèques *Python pyaes* et *rsa* [T1486].

Nom fichier	SHA-256	Taille
svchost.exe	4770A0447EBC83A36E590DA8D01FF4A418D58221C1F44D21F433AAF18FAD5A99	504.5 KB
17535.pyz	6661B5D6C8692BD64D2922D7CE4641E5DE86D70F5D8D10AB82E831A5D7005ACB	279590 octets

Le code *Python* contenu dans « `17535.pyz` » contient notamment la clé publique RSA utilisée pour le chiffrement, le message de demande de rançon et une variable permettant de choisir l'extension des fichiers chiffrés. En particulier, le condensat du fichier est susceptible de varier, ainsi que son nom qui semble choisi aléatoirement.

Plusieurs éléments permettent d'associer ces codes malveillants à la famille **Pysa**, à commencer par l'extension « `.pysa` » des fichiers chiffrés qu'ils produisent mais aussi leurs messages de demande de rançon.

2.1.2 Messages de demande de rançon

Les deux codes malveillants décrits ci-dessus créent un fichier de demande de rançon, sous la forme d'une fenêtre *pop-up* dans le premier cas et d'un fichier nommé « `RECOVER_YOUR_DATA.txt` » dans le second cas.

Ces demandes de rançon sont écrites dans un anglais approximatif. Bien que différentes, elles contiennent des chaînes de caractères identiques comme « `To get all your data back contact us:` ». L'une des deux propose également à la victime le déchiffrement gratuit de deux fichiers, en guise de bonne foi. Ces deux caractéristiques étaient également présentes dans des versions antérieures du rançongiciel **Pysa**.

Enfin, les messages de demande de rançon contiennent deux adresses de courriel ProtonMail qui semblent générées à partir de noms propres choisis au hasard.

Il est à noter que les deux messages de demande de rançon contiennent les mêmes adresses. De plus, des adresses de courriel similaires ont été utilisées dans des versions antérieures de **Pysa**.

2.1.3 Une troisième version ?

Sur l'un des systèmes d'information compromis, des fichiers chiffrés portant l'extension « `.newversion` » ont été découverts. Le code responsable de la création de ces fichiers n'a pas encore été identifié.

Toutefois, un message de demande de rançon nommé « `Readme.READ` » est présent et contient les mêmes adresses de courriel ProtonMail que précédemment. Il est donc probable que toutes ces attaques soient l'œuvre d'un même mode opératoire.

Puisque le code source *Python* de **Pysa** contient une variable permettant de choisir l'extension des fichiers chiffrés, il est également possible que les fichiers « `.newversion` » aient été générés par une autre instance de **Pysa**.

2.2 Tactiques, Techniques et Procédures

Plusieurs traces d'activité liées au mode opératoire ont été observées sur le système d'information compromis.

2.2.1 Vecteur d'infection, reconnaissance et latéralisation

Le vecteur d'infection initial est inconnu à ce jour, mais plusieurs événements survenus peu avant l'attaque pourraient être liés au mode opératoire et avoir permis l'accès initial ou la latéralisation.

- Des tentatives de connexion par force brute sur une console de supervision ont été observées, ainsi que sur plusieurs comptes Active Directory [T1110]. Par ailleurs, certains comptes d'administrateurs de domaine ont effectivement été compromis.
- L'exfiltration d'une base de données de mots de passe a eu lieu peu avant l'attaque [T1081].
- Des connexions RDP illégitimes ont eu lieu entre contrôleurs de domaine en utilisant un nom d'hôte inconnu potentiellement lié au mode opératoire [T1076].

Les scripts « `.bat` » utilisés par le mode opératoire révèlent une utilisation importante de l'outil d'administration à distance **PsExec** [T1035], ainsi que du langage de script PowerShell [T1086].

2.3 Furtivité et maintien sur le système d'information

L'un des scripts « `.bat` » mentionnés ci-dessus est chargé d'exécuter sur des machines du réseau un script PowerShell baptisé « `p.ps1` ». Ce script a plusieurs fonctionnalités, parmi lesquelles :

- L'arrêt des services antiviraux et de divers autres services et processus, ainsi que la désinstallation de Windows Defender [T1089].
- La suppression des points de restauration et des *Shadow Copy* [T1490].
- Une modification des fichiers *README* pour faciliter l'ouverture par double-clic.

- L'envoi d'un datagramme UDP contenant l'adresse MAC de la machine sur le port 7.

Il semble que ce script permette à la fois d'améliorer la furtivité du mode opératoire et de préparer l'exécution du rançongiciel. La dernière fonctionnalité suggère qu'un programme du mode opératoire pourrait être en écoute sur le port 7. Néanmoins, aucun programme de ce type n'a été découvert pour le moment.

Le mode opératoire semble également avoir utilisé son propre binaire correspondant à *powershell.exe*, renommé « `EnNoB-1229.exe` ». Il est possible que ce nom de fichier soit généré aléatoirement.

2.4 Possible utilisation d'Empire

Plusieurs agents de l'outil de post-exploitation **Empire** ont été découverts sur des contrôleurs de domaine des systèmes d'information compromis. Bien qu'aucun lien technique n'ait été établi avec l'utilisation du rançongiciel **Pysa**, il est probable que ces codes malveillants aient été utilisés par le même mode opératoire.

2.5 Commentaires

Le mode opératoire observé dans cette attaque semble compatible avec un acteur opportuniste motivé par un but lucratif.

Les techniques, tactiques et procédures utilisées sont classiques et n'ont pas montré à ce jour de techniques d'attaques particulièrement évoluées. Le mode opératoire a effectué quelques actions permettant d'éviter la détection par des solutions de sécurité, notamment en désactivant certaines d'entre elles. Toutefois, ces actions visent davantage à permettre l'exécution du rançongiciel qu'à effacer des traces, en témoigne la présence du code *Python* du rançongiciel sur l'une des machines.

Le rançongiciel **Pysa** est basé sur des bibliothèques *Python* publiques et son code spécifique est très court. Cependant, aucune faille n'a été trouvée dans l'implémentation du chiffrement et les algorithmes utilisés sont à l'état de l'art. Le mode opératoire a par ailleurs utilisé des outils de post-exploitation disponibles en source ouverte. Ces éléments sont cohérents avec le profil d'un acteur opportuniste mettant en œuvre des moyens adaptés à son objectif.

3 Recommandations

Les indicateurs de compromission exposés dans la section précédente peuvent être bloqués et recherchés sur un système d'information pour prévenir ou détecter une attaque similaire.

Plus généralement, dans le cadre d'une attaque par rançongiciel et afin d'empêcher la compromission complète du système d'information, les mesures d'hygiène et de sécurité classiques suivantes s'appliquent et peuvent être conduites en parallèle :

- **M1. Assurer une sauvegarde des données critiques** : bases de données métier, partages de fichiers réseaux, bases de données Exchange (attention : l'architecture par redondance "*backupless*" uniquement en ligne n'est pas suffisante contre les rançongiciels qui arrêtent les services liés à Exchange et chiffrent toutes leurs bases en même temps), forêts Active Directory, etc. Ces sauvegardes doivent être périodiquement exportées vers un **support inaccessible depuis le réseau** et leur restauration doit être **testée périodiquement** afin de s'assurer qu'elles soient utilisables en cas d'urgence. Cette mesure est la seule garantie de protection des données face à un rançongiciel qui chiffrerait les données en ligne par propagation réseau.
- **M2. Mener des campagnes de mises à jour, en commençant par les vulnérabilités exploitables à distance (RCE).** Si un inventaire logiciel du parc n'est pas disponible, donner la priorité aux mises à jour génériques des systèmes d'exploitation : MS08-067, MS14-068, MS17-010 ("EternalBlue" utilisée par le rançongiciel WannaCry), CVE-2019-0708 ("BlueKeep"), etc. Les contrôleurs de domaine et autres serveurs critiques doivent être mis à jour dès la publication de mises à jour de sécurité avec les correctifs de sécurité cumulatifs (*Monthly Rollup*);

- **M3. Restreindre, par filtrage réseau, l'accès à certains ports réseau les plus critiques sur les postes de travail** (notamment 135, 139, 445, 3389, 5585 etc.) aux seuls postes d'administration clairement identifiés, par exemple au moyen du pare-feu intégré de Windows. Les postes de travail ne doivent exposer aucun service applicatif et ne doivent pas avoir de raison de communiquer entre eux. Le même principe s'applique pour la surface exposée par les serveurs applicatifs et entre une majorité des serveurs. Les flux réseau ne devraient être ouverts que sur un principe de "liste blanche" documentant le besoin métier auquel répond chaque ouverture de flux. Si un tel inventaire n'existe pas déjà, il peut être commencé dès maintenant au moyen d'une écoute réseau passive (solutions fournissant des journaux NetFlow ou équivalents, ou simple règle de pare-feu en mode "audit") ;

- **M4. Migrer vers des moyens d'assistance à distance et d'administration sécurisés** protégeant les authentifiants de l'administrateur vis-à-vis du système à administrer (ce que ne garantit pas par défaut VNC). Par exemple, Microsoft Remote Assistance est intégré à Windows pour une assistance utilisateur interactive. Pour les besoins d'administration à distance :
  - Si une session interactive n'est pas nécessaire, privilégier l'utilisation des composants Microsoft Management Consoles (MMC) intégrés à Windows ou installables par commande PowerShell[1].
  - Si une session interactive est nécessaire, utiliser un compte administrateur local de la machine. Un seul compte administrateur local devrait être activé à tout instant sur chaque machine, et ce compte devrait avoir des authentifiants différents pour chaque machine (faute de quoi, la compromission d'une machine permet leur rejeu sur toutes les autres). Par exemple, la solution LAPS (Local Administrator Password Solution[2]) éditée par Microsoft permet de remplir ces objectifs, à condition de déléguer finement les droits d'accès au mot de passe administrateur local en respectant le principe du moindre privilège.

- **M5. Utiliser des comptes administrateurs Active Directory (AD) dédiés et nominatifs** pour garantir leur traçabilité ;

- **M6. Minimiser au maximum les comptes de service et les comptes utilisateurs membres des groupes d'administration de l'Active Directory** ("Administrateurs", "Admins du domaine", "Administrateurs de l'entreprise", "Administrateurs du schéma", "DNS Admins", "Opérateurs de comptes", "Opérateurs de serveurs", "Opérateurs de sauvegardes", et "Opérateurs d'impression"). Si un droit d'accès est nécessaire, effectuer une délégation par liste de contrôle d'accès et jamais par ajout dans un des groupes privilégiés. Une fois toutes les délégations effectuées, les comptes administrateurs AD ne doivent être nécessaires que dans des cas exceptionnels (voir le modèle d'administration en tiers[3]) ;

- **M7. Assigner au compte administrateur intégré (RID 500) un mot de passe complexe, stocké sous enveloppe papier, et utilisé uniquement en urgence ou dernier recours** ;

- **M8. Utiliser les comptes d'administration de l'Active Directory seulement depuis des postes dédiés sans usage bureautique (navigation, messagerie, etc.) et sans accès à Internet.** Ces postes doivent avoir un pare-feu local bloquant tout flux entrant, sans exception, et être les seuls systèmes depuis lesquels sont utilisés les comptes d'administration ;

- **M9. Assurer un archivage des journaux d'évènements du parc** (Windows EventLogs, syslogs d'équipements réseau et Unix, etc.) dans un puits de journaux assurant une rétention de plusieurs mois au minimum, accessible uniquement par les administrateurs en ayant le besoin. **Ces journaux seront nécessaires pour mener à bien les éventuelles actions de réponse à incident et de remédiation en cas de compromission.** Compte-tenu de leur volumétrie, il peut être utile de séparer les journaux d'authentification des contrôleurs de domaine des journaux des autres systèmes de parc.

[1] Get-WindowsCapability -Name '*RSAT*' -Online | Add-WindowsCapability -Online
[2] https://support.microsoft.com/fr-fr/help/3062591/microsoft-security-advisory-local-administrator-password-solution-laps
[3] https://docs.microsoft.com/fr-fr/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN