Incident de sécurité / Demande de rançon Nov. 2019

J.-M. Kubek, É. Carayol, `rssi-contact@listes.univ-jfc.fr`

4 décembre 2019

Courant novembre 2019 un E.C. du site d'Albi a été victime d'une tentative d'escroquerie par rançongiciel. Ce programme malveillant a rendu inaccessible les données stockées sur le poste de travail ainsi que celles déposées sur la clef USB que l'E.C. utilise habituellement pour transférer les fichiers de ce poste de travail vers sa machine personnelle.

En raison de contraintes liées au domaine de recherche, la machine compromise par cette tentative d'extorsion de fond n'est pas maintenue par la DSIUN.

Ce type d'attaque [1] est relativement rare sur les campus de l'INUC. Toutefois, à l'instar du celle du CHU de *Rouen* [2], ces attaques représentent un risque important de blocage, sur une longue période, de l'ensemble du système informatique de l'établissement.

L'objectif de la présente note est de participer à la décision relativement aux mesures qui devraient accompagner l'*exercice du droit à l'indépendance des enseignants-chercheurs dans le domaine du numérique* au regard *des risques que cette indépendance peut entraîner sur le fonctionnement de l'établissement*.

Note typographique : Les liens cliquables intra-document sont en bleu, les liens hors document sont en vert.

Table des matières

Abbreviations

ANSSI Agence nationale de sécurité des systèmes d'information.

CHU Centre hospitalier universitaire.

DSIUN Direction du système d'information et des usages du numériques, service en charge du numérique à l'INUC.

E.C. enseignant-chercheur.

INUC Institut national universitaire J.-F. Champollion.

O.S. Système d'exploitation (*en*: Operating system).

USB (*en* : Universal serial bus) norme de communication entre ordinateurs ou périphériques.

rançongiciel Logiciel rançonneur (*en*: Ransomware).

1. Cf document intitulé « Logiciels rançonneurs : menaces, risques et contrôles» de mai 2017 par J.-M. Kubek et É. Carayol sur nuxeo
2. Voir par exemple `cet article du Monde`

Présentation du cas

Déroulement

1. À son domicile[3], en voulant transférer des fichiers de travail sur son ordinateur personnel, l'E.C. constate que les fichiers sur la clef USB sont chiffrés ;
2. le lendemain, sur site, il constate que les fichiers de données sur son poste de travail fixe sont aussi chiffrés ;
3. il notifie le service en charge du numérique (DSIUN) de l'incident.
4. la DSIUN[4] confirme le problème ainsi que l'impossibilité de décrypter les fichiers de données.
5. la DSIUN soumet les fichiers du poste de travail à l'anti-virus institutionnel (`kaspersky`). Le résultat de cette analyse apparaît à la figure 1 page 5 ;
6. notification[5] aux services de sécurité du ministère de la compromission en cours ;
7. le poste de travail est restitué à l'E.C. avec la recommandation de ne pas le reconnecter au réseau de l'établissement ;
8. le poste de travail est confié à un prestataire[6] avec pour mission de reinitialiser (reformater) le disque dur puis de réinstaller l'O.S.

3. Constatation de l'incident

4. Prise en charge DSIUN

5. Notification ministère

6. Nettoyage du poste de travail

Constats connexes

1. Le système d'exploitation a été modifié[7] environ une semaine avant l'incident ;
2. un certain nombre de programmes utilitaires ont été réinstallés par l'E.C. à la suite de la modification de l'O.S.
3. l'anti-virus installé sur la machine (`Windows Defender`) a été désactivé par l'E.C. afin qu'il puisse installer l'`environnement d'exécution java`[8] ;
4. les fichiers chiffrés sur la clef USB semblent avoir été modifiés entre 12h et 14h le jour de la constatation de l'incident.

7. Cette opération a consisté à installer `windows 10` à la place de `windows 7`. Elle a été réalisée par le prestataire extérieur.

8. L'installation de cet environnement d'exécution est requis pour permettre l'utilisation d'une application institutionnelle (application budgétaire ou financière).

Contexte

— l'E.C. réalise des travaux de recherche dans un domaine où les applications gratuites fourmillent : simulations, comparaisons de données, ... Les installations / désinstallations de programmes sont donc fréquentes.

— Les premiers rançongiciels sont apparus il y une demi décade, depuis cette date, ils se diffusent massivement par vagues, de manière irrégulière ;

— ANSSI a confirmé récemment qu'une vague de diffusion[9]. est en cours depuis mi octobre 2019 ;

9. Toutefois, le rançongiciel décrit dans le communiqué de l'ANSSI n'est pas celui qui a provoqué l'incident décrit ici

— les vecteurs de compromission des rançongiciels sont similaires à ceux d'autres logiciels malveillants :
  — *compromission par courrier électronique* au travers de campagne d'envois en masse où les utilisateurs sont invités à ouvrir un fichier compromis ;
  — *compromission par installation de programmes compromis* par ailleurs : le logiciel malveillant est ajouté lors de l'installation d'un logiciel tiers sur la machine ;
  — *compromission du système d'exploitation de la machine* : le logiciel malveillant est ajouté dès la mise en service de la machine par installation d'une version compromise du système d'exploitation ;
— lorsqu'une machine est compromise par un logiciel malveillant (en particulier un rançongiciel) elle est aussi compromise par de *nombreux autres logiciels malveillants* ;
— un logiciel malveillant peut-être *dormant* : il y a alors un délai entre l'installation de ce logiciel et la date de son déclenchement effectif (ici, la date où il chiffre les fichiers) ;
— les actions d'un logiciel malveillant sont parfois *déclenchées ou commandées de l'extérieur* ;

Analyse

L'analyse du cas et de ses impacts potentiels s'avère difficile pour les raisons suivantes :

— l'établissement ne dispose pas de système métrologique permettant de détecter ou d'évaluer (*pot de miel*) les tentatives de propagation d'un virus au sein de ses réseaux locaux ;
— le dispositif de stockage – uniquement le (ou les) disque(s) dur(s), pas la clef USB qui contient toujours les fichiers chiffrés – de l'ordinateur a été reformaté par le prestataire extérieur, ce qui rend impossible son analyse *post-mortem*.

Il est possible que la victime de la tentative d'escroquerie ait installé des logiciels à partir de sites internet secondaires. Dans ce cas, les logiciels installés *pourraient* avoir été équipés de manière à permettre l'installation du rançongiciel.

Le dépôt utilisé par le prestataire externe pour l'installation de `windows 10` *pourrait* avoir été lui même compromis. Dans ce cas, l'instance `windows 10` installée par ce prestataire *pourrait* avoir elle-même été équipée d'une forme dormante du rançongiciel ou d'un autre logiciel malveillant qui *pourrait* avoir ensuite post-installé le rançongiciel.

Enfin, le logiciel malveillant *pourrait* avoir été installé à la suite de la réception d'un courrier électronique. Toutefois, selon l'antivirus institutionnel, la version locale de la boîte de message [10] ne contenait pas de fichier compromis.

10. La boîte institutionnelle de la victime n'a pas été scannée en raison de sa localisation distante sur les serveurs de la COMUE.

Impacts

Impacts directs

Les fichiers de données utilisés par l'E.C. sont soit inutilisables soit perdus puisqu'ils sont soit chiffrés de manière irréversible, soit effacés à la suite du reformatage réalisé par le prestataire externe.

Les conséquence de cette perte en nombre de donnée sont limitées en raison de l'existence d'une sauvegarde récente [11] du disque dur de la victime. Elles consistent principalement en dégradation des conditions de travail de la victime : augmentation du stress et de la charge de travail pour rattraper les données perdues.

11. Une sauvegarde avait été réalisé avant installation de la nouvelle version de `Windows`

Ces conséquences peuvent éventuellement s'appliquer au sein de l'équipe de recherche de la victime en fonction des travaux en cours de manière collaborative au sein de cette équipe.

Impacts légaux éventuels

Les personnes concernées ne peuvent pas exercer leurs droits légaux si les fichiers inaccessibles contenaient des données à caractère personnel.

Autres impacts éventuels

Le passage de l'anti-virus institutionnel a mis en évidence l'existence de plusieurs logiciels malveillants.

Certains de ces logiciels peuvent être la source d'incidents ou désagréments bénins (barres de navigation de publicité dans `firefox`) mais d'autres programmes détectés sur ce poste de travail sont délibérément nocifs :

— Logiciel d'*interception d'activités* [12] : espionnage des frappes de touches clavier, réalisation de copies d'écran, espionnage des programmes lancés sur le poste de travail.

12. Cf page 6 en annexe

— *Chevaux de Troie* [13] permettant l'installation de nouveaux malwares

13. Cf page 6 en annexe

— *Portes dérobée*s [14] se connectant à des serveurs de contrôle commande extérieurs

14. Cf page 7 en annexe

Certains de ces logiciels sont installés depuis plusieurs mois, ce qui *pourrait* indiquer que l'anti-virus non institutionnel utilisé sur le poste de travail de la victime n'était pas opérationnel ou qu'il fonctionnait en mode dégradé.

Synthèse – Recommandations

L'établissement offre à certains utilisateurs la possibilité de gérer de manière indépendante leurs postes de travail. Ces utilisateurs ont alors la possibilité de réaliser cette gestion de manière autonome ou en faisant appel à un prestataire extérieur.

Informations aux utilisateurs

Ces utilisateurs devraient être avertis du danger que constitue l'installation non contrôlée de logiciel : les sources secondaires de logiciels doivent être considérées avec circonspection.

> Les logiciels disponibles aux travers de ces sources secondaires sont susceptibles d'être accompagnés par une quantité non négligeable de logiciels malveillants.

L'anti-virus utilisé pour ces postes de travail autogérés devraient être identiques aux anti-virus institutionnels et leur configuration initiale, conforme à celle utilisée sur les sites de l'établissement, ne devrait pas pouvoir être modifiée.

Risque de dysfonctionnement des activités INUC

L'installation puis l'absence de détection de la présence d'un rançongiciel est particulièrement risquée. En effet ces logiciels sont souvent accompagnés par un programme qui leur permet de se propager à grande vitesse, au travers du réseau local, sur les ordinateurs d'une organisation.

La propagation massive d'un rançongiciel *pourrait* donc entraîner des problèmes importants de dysfonctionnement pour une organisation comme l'INUC dont le fonctionnement repose largement sur l'utilisation de l'outil informatique.

FIGURE 1: Résultat du scan DSIUN du poste de travail compromis : copie d'écran

Annexe : incidents récents

— Université de Corse : mai 2019 Article Corse Matin du 30 mai 2019

— Université de Bretagne Occidentale : Incident en cours

Annexe : Principales classes de programmes malicieux

Cet annexe schématise le fonctionnement des principales classes de logiciels malveillants mentionnés dans cette note. Ces classes sont les suivantes :

— les *intercepteurs de données* [15] – cf page 6 – sont utilisés pour remonter des données du poste de travail vers un site externe.

— Les *chevaux de Troie* – cf page 6 – sont utilisés pour installer d'autres logiciels malveillants ;

— Les *portes dérobées* – cf page 7 – permettent à des programmes ou utilisateurs extérieurs de se connecter à la machine infectées ;

— les *rançongiciels* – cf page 8 – permettent de réaliser des extorsions de fond ou de renseignements.

L'expression *vecteur de compromission* utilisée dans cet annexe désigne le moyen utilisé pour installer puis activer un logiciel malveillant (*virus*) sur un matériel informatique. Ce vecteur peut-être la messagerie internet, l'installation d'un logiciel non vérifié ou encore une clef USB infectée utilisée sans attention préalable sur le matériel.

15. Les données interceptées peuvent être des séquences de touches saisies par l'utilisateur du poste de travail (on parle alors de *keylogger*), des copies d'écran ou tout autre donnée présente sur le disque dur ou la mémoire de l'ordinateur infecté.
Les données interceptées sont remontées vers le site externe peuvent ensuite être traitées *a posteriori* afin d'en retirer des informations pertinentes (numéros de carte de paiement, mots de passes, ...).

Intercepteurs de données

L'expression *intercepteurs de données* qualifie les logiciels qui sont capables d'intercepter des données du poste de travail puis de les déposer sur un site distant. La figure 2 schématise le séquencement des actions relatives à l'infection d'un poste de travail par un logiciel d'interception.

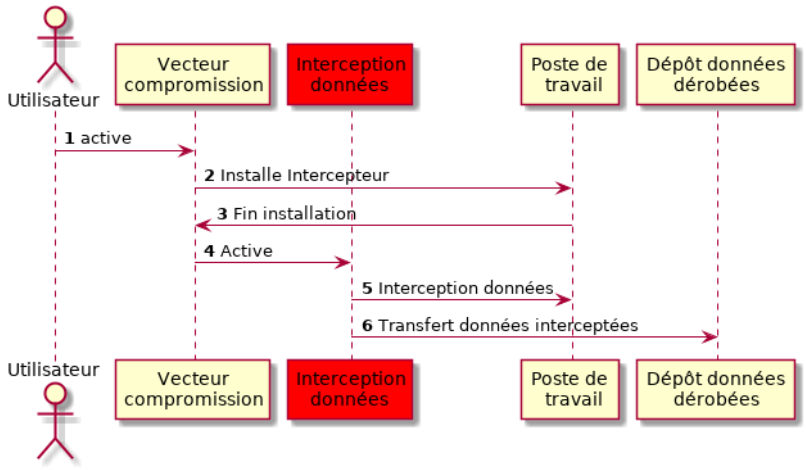

FIGURE 2: Fonctionnement schématique d'un intercepteur de données.

1. l'utilisateur active le vecteur de compromission qui sera utilisé pour installer la porte dérobée ;
2. le vecteur de compromission installe l'intercepteur ;
3. le poste de travail signale la fin de l'installation ;
4. le vecteur de compromission active l'intercepteur ;
5. l'intercepteur se met en écoute des communications entre les composants du poste de travail ;
6. l'intercepteur transfère, sans les interpréter, les données vers un dépôt externe ;

Cheval de Troie

L'expression *cheval de Troie* qualifie les logiciels dont la fonction est de télécharger d'autres logiciels malveillants.

La motivation principale de ce type de programme est de permettre l'installation d'un programme initial de taille minimale dont la mission sera ensuite d'installer un ou plusieurs autres programmes de tailles plus importantes.

Le diagramme de la figure 3 schématise le séquencement des actions relatives à l'infection d'un poste de travail par un cheval de Troie.

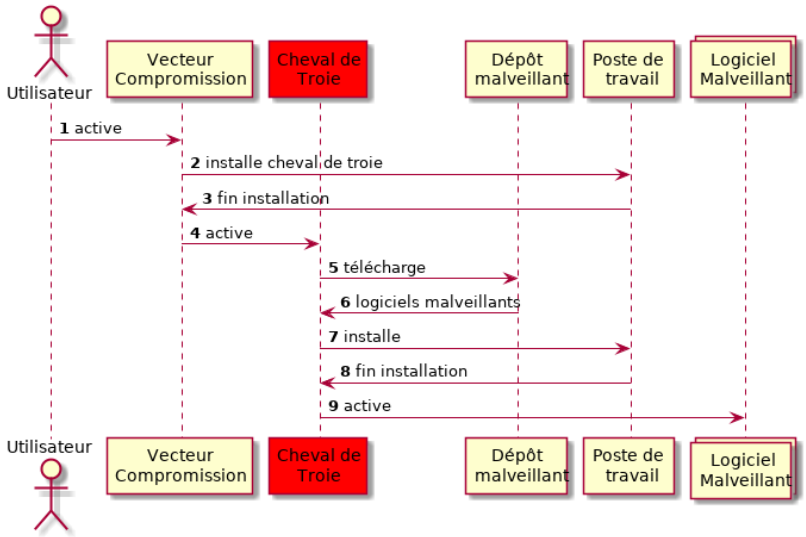

FIGURE 3: Fonctionnement schématique d'un cheval de Troie.

1. l'utilisateur active le vecteur de compromission qui sera utilisé pour installer le cheval de Troie.
2. le vecteur de compromission installe le cheval de Troie
3. le poste de travail signale la fin de l'installation
4. le vecteur de compromission active le cheval de troie
5. le cheval de Troie contacte le site internet contenant les autres logiciels malveillants à télécharger

7 le cheval de Troie installe les logiciels malveillants

6. le cheval de troie active les logiciels malveillants supplémentaires

Portes dérobées

L'expression *porte dérobée* qualifie les logiciels dont les actions peuvent être pilotées à distance

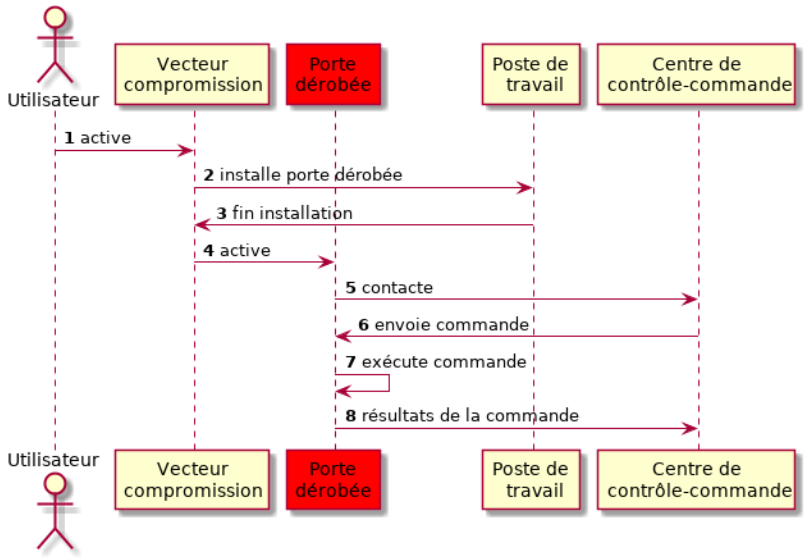

FIGURE 4: Fonctionnement schématique d'une porte dérobée.

1. l'utilisateur active le vecteur de compromission qui sera utilisé pour installer la porte dérobée ;
2. le vecteur de compromission installe la porte dérobée ;
3. le poste de travail signale la fin de l'installation ;
4. le vecteur de compromission active la porte dérobée ;
5. le cheval de troie contacte le site internet de contrôle commande pour lui signaler sa disponibilité ;
6. le site de contrôle commande demande à la porte dérobée d'exécuter une commande ;
7. la porte dérobée exécute la commande demandée ;
8. la porte dérobée signale la fin d'exécution et remonte les résultats de cette commande au site de contrôle commande ;

Le diagramme de la figure 4 schématise le séquencement des actions relatives à l'infection d'un poste de travail par une porte

dérobée.

La motivation principale de ce type de programme réside d'une part dans la flexibilité [16] qu'ils permettent et d'autre part dans les possibilités accrues d'attaque [17] que permettent une quantité importante de machines compromises.

16. Par rapport à une configuration *cheval de Troie* la flexibilité d'une *porte dérobée* permet par exemple de diversifier les programmes malveillants téléchargés sur la machine compromise.
17. L'ensemble des machines compromises qui se connectent à un même centre de contrôle commande peut être utilisée pour mener des attaques à grande échelle vers un site tiers : cas des *botnets* utilisés pour empêcher le fonctionnement d'un site web ou de l'ensemble des communications d'une entrprise par exemple.

Rançongiciel

Les expressions *rançongiciel*, *Ransomware* ou *cryptolocker* sont utilisées pour qualifier les programmes qui, une fois activés sur un matériel informatique, interdisent l'accès aux données stockées sur ce matériel.

La figure 5 schématise le mode de fonctionnement de ce type de logiciel.

Ce type de logiciel malveillant permet de réaliser des tentatives massives d'extorsion de fonds mais aussi des tentatives d'extorsion d'information dans le cas d'une attaque plus ciblée.

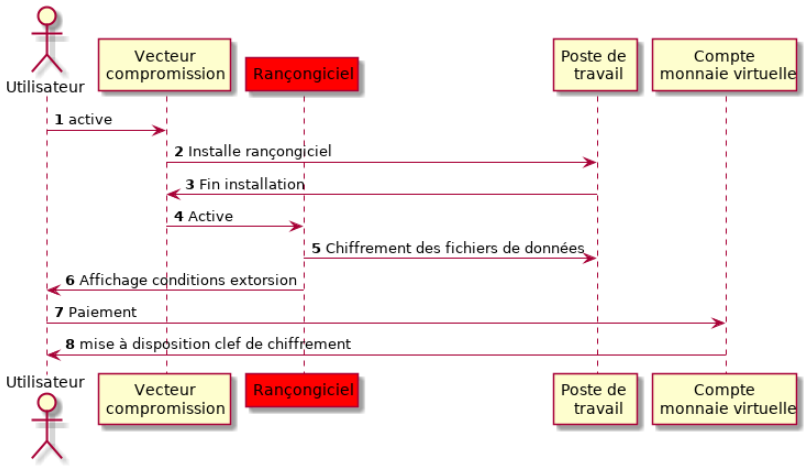

FIGURE 5: Fonctionnement schématique d'un rançongiciel.

1. l'utilisateur active le vecteur de compromission qui sera utilisé pour installer le rançongiciel ;
2. le vecteur de compromission installe le rançongiciel ;
3. le poste de travail signale la fin de l'installation ;
4. le vecteur de compromission active le rançongiciel ;
5. le rançongiciel chiffre les fichiers de données du poste de travail ;
6. le rançongiciel fournit à l'utilisateur les conditions de l'extorsion (restauration des fichiers dans leur état initial) ;
7. l'utilisateur met à disposition le montant demandé au compte de monnaie virtuelle indiqué ;
8. L'utilisateur reçoit la clef de déchiffrement ;